Tietoturva järjestöissä

Ammattikorkeakoulun opinnäytetyö
Tieto- ja viestintätekniikka, insinööri (AMK)
kevät 2022
Riikka Helminen

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka, insinööri (AMK) Tiivistelmä
Tekijä Riikka Helminen Vuosi 2022
Työn nimi Tietoturva järjestöissä
Ohjaaja Marko Grönfors

Opinnäytetyön tarkoituksena oli tuottaa tietoa järjestöjen tietoturvan tasosta sekä tutkia vaikuttavatko järjestön käytössä olevat resurssit, kuten järjestön koko tai vuoden toimintabudjetti, tietoturvan tasoon. Tämän selvittämiseksi laadittiin kyselylomake, jonka avulla kerättiin 88 vastaajan suuruinen aineisto. Vastaajat edustivat hyvin erilaisia järjestösektorin toimijoita. Aineisto analysoitiin määrällisiä tutkimusmenetelmiä hyödyntäen.

Opinnäytetyön tietoperustaan sisältyy perustietoa järjestöistä, niiden resursseista sekä tietoa aiemmin tehdyistä selvityksistä ja tutkimuksista. Lisäksi tietoperustaan kuuluu tietoa tietoturvasta, kyberuhkista ja niiltä suojautumisesta.

Järjestön koko, eli montako palkattua työntekijää järjestössä on, korreloi useamman kysymyksen kohdalla enemmän kuin järjestön toimintabudjetin suuruus. Mitä enemmän järjestöllä on henkilökuntaa, sitä todennäköisemmin tietoturva-asioista on huolehdittu paremmin. Järjestöillä on halua ottaa tietoturva paremmin toiminnassaan huomioon, mutta rajalliset resurssit ja osaaminen eivät tue tätä parhaalla mahdollisella tavalla.

Avainsanat Järjestöt, kyberuhkat, tietoturva
Sivut 39 sivua ja liitteitä 3 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and communication technology Abstract
Author Riikka Helminen Year 2022
Subject Information security on nonprofit organizations
Supervisors Marko Grönfors

The purpose of this thesis was to provide information on the level of information security on nonprofit organizations and to study whether the resources available, such as the size of the nonprofit organization or the annual operating budget, affect the level of information security. A questionnaire was prepared and used to collect data from 88 respondents. Respondents represented a wide variety of actors in the nonprofit sector. The data were analyzed using quantitative research methods.

The knowledge base of the thesis includes basic information about nonprofit organizations, their resources and information about previous surveys and research. In addition, the knowledge base includes information on information security, cyber threats and protection against them.

The size of the nonprofit organization, in other words how many employees there are in the organization, correlates to more issues than the size of the organization’s operating budget. The more staff an organization has, the more likely security issues are better taken care of. Organizations want to take security better into account in their operations, but limited resources and expertise do not support this in the best possible way.

Keywords Cyber threats, information security, nonprofit organizations
Pages 39 pages and appendices 3 pages

Sisällys

Liitteet

1 Johdanto

Suomessa on lähes 107 000 rekisteröityä yhdistystä, jotka toteuttavat tärkeää toimintaa julkisen ja yksityisen sektorin rinnalla (PRH, 2021 -a). Suomalaisista yli 75 prosenttia kuuluu vähintään yhteen yhdistykseen (Jousilahti, 2019). Suomesta löytyy yhdistys lähes jokaiseen tarkoitukseen, maanpuolustuksesta mato-ongintaan.

Yhdistykset toimivat pääsääntöisesti suhteellisen pienillä resursseilla ja keskittyvät toimintansa toteuttamiseen. Yhdistyksissä on keskimäärin kolme palkattua työntekijää, joten ICT-asiat saattavat olla vain pieni osa yhden työntekijän jo muutenkin laajaa työnkuvaa.

Lähes kaikilla yhdistyksillä on jonkinlainen jäsenrekisteri, joka sisältää vähintään jäsentensä yhteystietoja. Näiden lisäksi yhdistyksillä saattaa olla myös jäsentensä ja lahjoittajiensa maksutietoja, joten yhdistyksillä saattaa olla mahdollisia hyökkääjiä kiinnostavia tietoja. Tietoturvan avulla pyritään varmistamaan järjestön tietojen luottamuksellisuus, eheys ja käytettävyys.

Opinnäytetyö on toteuttamistavaltaan määrällinen tutkimus. Kyselylomakkeen avulla kerättiin aineisto, joka analysoitiin kvantitatiivisia menetelmiä käyttäen. Kyselyyn vastasi 88 hyvin erilaista järjestöä. Kyselyn teemat valikoituivat tutustumalla tietoturvan osa-alueisiin ja kyberuhilta suojautumiseen. Kyselyssä otettiin huomioon vastaajajoukon osaamistaso ja mitkä kyberuhilta suojautumisen keinot ovat mahdollisia järjestöissä.

Tavoitteena oli tuottaa tietoa järjestöjen tietoturvan tasosta. Opinnäytetyön tutkimuskysymyksiksi muodostuivat seuraavat kysymykset:

1. Miten tietoturvan osa-alueet eli tiedon luottamuksellisuus, eheys ja käytettävyys on huomioitu järjestöjen toiminnassa?

2. Vaikuttaako yhdistyksen resurssit, kuten yhdistyksen toimintabudjetti ja henkilöstön määrä, tietoturvan tasoon?

2 Tutkimuksen tietoperusta

Opinnäytetyön tietoperusta sisältää tietoa järjestöistä, niiden resursseista ja järjestöjen digitalisaatiosta. Tietoperustaan sisältyy myös perusteita tietoturvasta, kyberuhista ja kyberuhilta suojautumisesta.

2.1 Mikä on järjestö?

Yhdistyslain ensimmäisen pykälän mukaan yhdistyksen saa perustaa aatteellisen tarkoituksen yhteistä toteuttamista varten (Yhdistyslaki 26.5.1989/503 § 1). Tilastokeskuksen käsitemääritelmän mukaan aatteellisen yhdistyksen muodostaa vähintään kolmen yksityishenkilön, yhteisön tai säätiön sopimuksella perustama yhdistys, joka on rekisteröity Patentti- ja rekisterihallituksen ylläpitämään yhdistysrekisteriin. Mikäli aatteellisen yhdistyksen säännöissä tai jos se muuten liittyy tarkoituksen toteuttamiseen, voi yhdistys harjoittaa elinkeinoa tai muuta ansiotoimintaa. (Tilastokeskus, n.d.)

Suomi on yhdistysten luvattu maa. Rekisteröityjä yhdistyksiä oli Suomessa vuoden 2019 lopussa lähes 107 000 (PRH, 2021 -a). Joka vuosi rekisteröidään noin 2 000 uutta yhdistystä (PRH, 2021 -b). Suomalaisista kolme neljäsosaa kuuluu johonkin yhdistykseen ja kahteen tai useampaan yhdistykseen kuuluu yli puolet suomalaisista (Jousilahti, 2019). Näiden tietojen pohjalta voimme olettaa, että yhdistyksillä on paljon muun muassa jäsentensä henkilötietoja, joiden turvaaminen on tärkeää.

Yhdistys- ja järjestö-sanoja käytetään pitkälti toistensa synonyymeinä. Järjestöllä tarkoitetaan usein yleisemmin kansalaisyhteiskunnan toimijoita, kun taas yhdistys on enemmän hallinnollinen termi. Monesti puhutaan järjestökentästä, jota ohjaa yhdistyslaki. (Vaikute.net, n.d.) Tässä opinnäytetyössä käytetään järjestö-sanaa.

Yhdistysten toiminta on muuttunut 2000-luvulle tultaessa entistä lähemmäs yksityisen sektorin toimintaperiaatteita, kun 1990-luvulla toiminta oli enemmän vapaaehtoisiin pohjautuvaa ja toimintaa rahoitettiin jäsenmaksuilla. Palkkatyön lisääntyminen onkin yksi merkittävimmistä muutoksista yhdistyssektorilla. Valtio on myös kannustanut yhdistyksiä fuusioitumaan ja keskittämään toimintaansa. (Jousilahti, 2019)

2.2 Tietoa järjestöjen resursseista

SOSTE Suomen sosiaali ja terveys ry julkaisee ajantasaista tutkimustietoa suomalaisesta sosiaali- ja terveysjärjestökentästä. Vuoden 2016 kyselyyn vastasi 1031 paikallisjärjestöä ja valtakunnallisten sosiaali- ja terveysjärjestöjen johtajista vastasi 98 järjestöä. Tuloksista käy ilmi, että 22 prosentissa yhdistyksistä on palkattua henkilökuntaa ja keskimäärin henkilöstöä on kolme työntekijää per yhdistys. (Peltosalmi ym., 2016, 42)

Oikeusministeriö kartoitti vuonna 2020 ”Järjestöjen rooli ja osallisuus julkisen hallinnon valmistelu- ja päätöksentekoprosesseissa” -kyselyssä muun muassa palkatun henkilöstön määrää järjestöissä. Kyselyyn vastasi 211 järjestöä eri puolilta Suomea. Suurimmassa osassa vastanneista järjestöistä oli alle viisi palkattua henkilöä ja 27 prosentissa ei ollut ollenkaan palkattua henkilöstöä. Palkatun henkilöstön määrän voidaan olettaa vaikuttavan siihen, miten ammattimaista järjestön toiminta on. (Saarinen, 2020, s. 5)

Oikeusministeriön kyselyn mukaan yhteiskunnallinen suhtautuminen järjestöjä kohtaan on parantunut viime vuosien aikana, mutta avustusten ja rahoituksen saaminen on yleisesti vaikeutunut ja vähentynyt.

Vastaajista yli puolet ilmoitti järjestön vuosittaisten toimintakulujen olevan yli 100 000 euroa. Palkatun henkilökunnan määrä korreloi vahvasti vuosikulujen kanssa. Järjestöissä, joissa ei ole palkattua henkilöstöä, vuosikulut ovat lähes kaikilla alle 10 000 euroa. Vastaajajärjestöt kokivat, että heidän tulisi yhä enemmän tuottaa yhteiskunnallisesti merkittäviä palveluita, mutta ne tulisi tuottaa vapaaehtoistyöllä. (Saarinen, 2020, ss. 2–17)

Lisäksi Veikkauksen pelituotot, joilla järjestöjen toimintaa on rahoitettu, ovat vähentyneet merkittävästi pelihaittojen vähentämiseen pyrkivien muutosten ja koronapandemian vuoksi. Hallitus on päättänyt korvata Veikkauksen edunsaajien menetykset täysimääräisesti vuonna 2021 ja 2022, mutta vuodelle 2023 on sovittu leikkauksia. Valtiovarainministeriö on arvioinut, että järjestöjen saamat avustukset laskisivat yli sadalla miljoonalla eurolla. (Hakahuhta & Koivisto, 2021)

Edellä mainituista seikoista voidaan päätellä, että suomalaiset yhdistykset toimivat varsin niukoilla resursseilla. Yhdistykset keskittyvät toiminnan tarkoituksensa toteuttamiseen, jolloin pienistä resursseista ei riitä juuri muuhun ylimääräiseen. Tällaisissa tilanteissa yhdistyksillä ei välttämättä ole henkilöstöä työskentelemään tieto- ja viestintätekniikan parissa, eikä tämän kokonaisuuden vastuita ole välttämättä nimetty kenellekään.

2.3 Tietoja järjestöjen digitalisaatiosta ja tietoturvasta

Suomessa on tutkittu hyvin vähän järjestöjen tietoturvan tasoa. Suomessa on kuitenkin useamman vuoden ajan tehty Järjestödigi-kartoitus, jonka tarkoituksena on kerätä tietoa yhdistysten digitalisaation, digiosaamisen ja viestinnän tilasta sekä samalla antaa uusia oivalluksia järjestöjen toimijoille edellä mainituista teemoista, nostaa esiin todellisia esimerkkejä ja pitää yllä keskustelua digitalisaation ja osaamisen merkityksestä järjestösektorilla (Järjestödigi-kartoitus 2019, 2019, s. 3).

Järjestödigi-kartoitukseen osallistuneista 67 % vastasi, että heillä on jäsenrekisteriä varten oma ohjelma. Osa vastaajista kertoi käyttävänsä jäsentietojen ylläpitoon esimerkiksi jaettua Google Drive -tiedostoa. (Järjestödigi-kartoitus 2019, 2019, s. 9)

Järjestöt kokevat digitalisaatiota hidastaviksi tekijöiksi henkilöstöresurssien ja taloudellisten resurssien puutteen, asenteet sekä osaamisen. Hidastavat tekijät vaihtelivat järjestön koon sekä esimerkiksi kohderyhmän iän mukaan. Yli puolet vastaajista koki, että tietoturvaosaaminen on hallinnassa, mutta kuitenkin 34 prosenttia vastaajista koki, että tietoturvaan ja tietosuojaan liittyvää osaamista tarvitaan lisää. (Järjestödigi-kartoitus 2019, 2019, ss. 14–23)

OK-opintokeskuksen Osaajat järjestötyössä -selvityksessä nousee esiin, että erityisesti tietotekniikan nopea kehitys vaatisi järjestön mielestä aikaa perehtymiseen. Järjestöjen jatkuva kehittämispaine ja uuden oppimisen tarve kuormittavat järjestötoimijoita. (Ristolainen, 2015, s. 38) Selvityksestä tulee myös ilmi, että vastaajien mielestä järjestötyö raahaa vuosia kehityksestä jäljessä ja että se tulee kehittymään erityisesti viestinnän ja tietotekniikan puolella (Ristolainen, 2015, s. 49).

Iso-Britanniassa on neljänä vuotena toteutettu The Charity Digital Skills Report, jossa on mitattu järjestösektorin digitaalisia taitoja. Kyselyyn on vastannut vuonna 2019 429 järjestöä eri puolilla Iso-Britanniaa. Kyselyyn on vastannut erilaisissa rooleissa työskenteleviä henkilöitä ja eri kokoisista järjestöistä.

The Charity Digital Skills Report 2020 mukaan yhdellä viidestä järjestöstä on huonot taidot monissa digitaalisen osaamisen aiheissa, mikä sisältää muun muassa käyttäjien tarpeet, datan ja analytiikan ja tietoturvan. Vastaajista 76 prosenttia koki järjestönsä tietoturvataidot huonoiksi tai kohtalaisiksi. Vain 18 prosenttia koki taidot hyviksi. Vuonna 2019 vastaava luku oli 54 %. (Amar, 2020, s. 17)

51 prosentilla vastanneista järjestöistä ei ole digitaalista strategiaa. Tulosten mukaan suurilla järjestöillä, joiden vuosibudjetti oli yli miljoona puntaa, ovat siinä tilanteessa, että digitaalisuus on vahvasti osa kaikkea työtä. (Amar, 2020, s. 16)

Järjestöt kokivat, että rahoituksen puute, henkilöstön osaamisen taso ja organisaation itsevarmuuden puute ovat suurimpia estäviä tekijöitä, jotta järjestö voisi hyödyntää digitaalisia ratkaisuja parhaalla mahdollisella tavalla. 66 prosenttia järjestöistä vastasi, että heidän hallituksensa jäsenten digitaaliset taidot ovat huonot tai niissä on kehittämisen varaa. (Amar, 2020, s. 22–28)

2.4 Tietoturva

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on määrittänyt, että käytännössä kyberturvallisuus -termillä tarkoitetaan organisaatioiden ja yhteiskunnan digitalisoitumisen aiheuttamia uudenlaisia turvallisuushaasteita. Sillä voidaan tarkoittaa niitä toimenpiteitä, joilla organisaatiot pyrkivät suojaamaan toiminnassaan tarvittavia järjestelmiä, laitteita ja tietoliikenneyhteyksiä kyberuhkilta. Kyberuhkat taas tarkoittavat organisaatiolle haitallisia tapahtumia, jotka vaikuttavat sen toimintaan, sen tietoihin ja pahimmillaan liiketoiminnan jatkuvuuteen. (Traficom, 2020a, s. 4)

Kyberturvallisuuskeskus on määritellyt tietoturva-termin hallinnollisiksi ja teknisiksi toimiksi, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain oikeutettujen henkilöiden saatavilla. Eheys tarkoittaa sitä, että tietoja voi muuttaa vain oikeutetut henkilöt ja käytettävyys sitä, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen henkilöiden käytettävissä. (Tietoturva, 2019)

2.5 Kyberuhkia

Mahdollisia kyberuhkia ovat muun muassa tietojenkalastelu, haittaohjelmat ja palvelunestohyökkäykset. Tietojenkalastelun tavoitteena on saada haltuun kirjautumistietoja tai muita tärkeitä tietoja, kuten luottokorttitietoja. Rikolliset voivat huijata käyttäjän vierailemaan huijaussivustollaan, joka on pyritty tekemään mahdollisimman paljon aidon palvelun sisäänkirjautumissivun kaltaiseksi. Jos käyttäjä ei huomaa eroa, hän syöttää kirjautumistietonsa huijaussivulle ja tiedot päätyvät rikollisten käsiin. (Traficom, 2020a, ss. 4–6)

Monesti näiden tietojen avulla pyritään pääsemään käsiksi esimerkiksi laskutustietoihin. Näiden tietojen pohjalta pystytään luomaan valelaskuja, joissa hyödynnetään oikean laskun tietoja ja kontekstia. Saatujen kirjautumistietojen avulla voidaan lähettää myös lisää tietojenkalasteluviestejä uhrin yhteystiedoille. Anastetuilla käyttäjätunnuksilla on myös mahdollista vakoilla yrityssalaisuuksia ja onnistunut tietojenkalasteluyritys voi aiheuttaa maine- ja sääntelyriskejä. Viime vuosina tietojenkalastelua on tapahtunut paljon Microsoftin Microsoft 365 -ympäristössä. (Traficom, 2020a, ss. 4–6)

Haittaohjelmilla tarkoitetaan tietokoneohjelmia, joista aiheutuu ei-toivottavia tapahtumia tietojärjestelmissä tai sen osissa. Monesti haittaohjelmat leviävät sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivujen ja haavoittuvien palvelinten kautta. Ympäri maailmaa on yleistynyt ilmiö, Big Game Hunting, jossa rikollinen valitsee kohteiksi houkuttelevia ja rahakkaita organisaatioita. Hyökkäyksen aikana rikollinen pyrkii tunkeutumaan organisaation järjestelmiin ja levittäytyy organisaation verkkoon. Tämän jälkeen hyökkääjä käynnistää organisaation tietojärjestelmien tiedot salaavan kiristyshaittaohjelman, jonka tarkoituksena on hidastaa, haitata tai lamauttaa organisaation toimintaa. Sen jälkeen hyökkääjä kiristää lunnaita salauksen purkamiseksi. (Traficom, 2020a, s. 7)

Suomalaiset yhdistykset eivät todennäköisesti ole haittaohjelmien ja kiristysten keskeisintä kohderyhmää rajallisten budjettiensa vuoksi ja toimintansa luonteen vuoksi. Yhdistyksiin on viime vuosina kohdistunut lähinnä tietomurtoja tai tietojenkalastelua, joissa on pyritty anastamaan jäsenten tai palveluiden käyttäjien tietoja. Yhdistyksillä on paljon tietoja jäsenrekistereissään sekä myös esimerkiksi lahjoitusten maksutietoja, mitkä saattavat kiinnostaa hyökkääjiä.

Esimerkiksi Ylemmät toimihenkilöt YTN ry joutui vuonna 2020 tietomurron kohteeksi. Tietomurto kohdistui YTN:n työntekijän sähköpostiin, josta hyökkääjä lähetti tietojenkalasteluviestejä, joilla yritettiin kalastella käyttäjätunnuksia ja salasanoja. (YTN, 2020) Kehitysvammaliiton Papunet-verkkopalveluun kohdistui myös tietomurto, jossa hyökkääjä sai haltuunsa käyttäjien sähköpostiosoitteita ja palvelussa käytettyjä salasanoja (Kehitysvammaliitto ry, 2021).

Maailmalla suuriin järjestöihin on kohdistunut myös hyökkäyksiä haittaohjelmilla ja kiristämistä. Uuden-Seelannin suurimpaan vapaaehtoisia välittävään yhdistykseen kohdistui haittaohjelmahyökkäys, jossa salattiin yhdistyksen tärkeitä tietoja sen tietojärjestelmissä. Philadelphia Food Bankiin kohdistui vuonna 2020 miljoonan dollarin lunnashaittaohjelmahyökkäys juuri, kun 5,6 miljoonaa amerikkalaista oli ruoka-avun tarpeessa koronapandemian takia. (CyberPeace Institute, 2021)

Toinen yleinen hyökkäys on johtajahuijaus, jossa hyödynnetään tietojenkalastelua ja identiteettivarkautta ja näiden avulla yritetään saada yhdistys tekemään tilisiirtoja. Näiden avulla on anastettu Yhdysvaltojen Pelastakaa Lapsilta miljoona dollaria vuonna 2018 ja Roots of Peacelta 1,3 miljoonaa dollaria vuonna 2020. (CyberPeace Institute, 2021)

Microsoftin Digital Defense -raportin mukaan valtiollisista kyberhyökkäyksistä 31 prosenttia kohdistui yhdistyksiin ja ajatushautomoihin. Microsoftin huomaamista valtiollisista

kyberhyökkäyksistä 58 prosenttia tuli Venäjältä. (Microsoft, 2021, ss. 52–53) Suomalaisiin yhdistyksiin ei todennäköisesti kohdistu suurta riskiä valtiollisten kyberhyökkäysten toimesta, mutta yhdistysten taustalla vaikuttavat aatteet saattavat provosoida ja motivoida hyökkääjiä ja näin lisätä riskiä joutua kyberrikoksen uhriksi.

2.6 Kyberuhkilta suojautuminen

Kyberuhkilta on mahdollista suojautua monilla eri keinoilla. Osiossa esitellään kyselyyn osaksi otettuja kyberuhkilta suojautumisen keinoja. Osa teemoista painottuu henkilöstön osaamiseen ja tietouteen, osa tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen.

Kyberturvallisuuskeskuksen Pienyritysten kyberturvallisuusopas nostaa esiin yhtenä teemana henkilöstön kouluttamisen, jotta heillä on tarvittava osaaminen tietoturvalliseen toimimiseen työssään. Oppaassa kehotetaan myös tekemään suunnitelma tietoturvapoikkeamien hallitsemiseksi. (Traficom, 2020b, s. 16) Muun muassa tietojenkalastelu on huomattavasti hankalampaa, jos henkilöstö on tiedostavaa tietoturvan suhteen ja suhtautuvat epäilevästi erilaisiin tietopyyntöihin. Monet haittaohjelmat myös leviävät sähköpostiviestien linkkien tai liitteiden avulla, joten jos henkilöstö jättää ne avaamatta ja lataamatta, jää haittaohjelmakin asentumatta.

Organisaatioiden olisi hyvä tehdä riskikartoitus kyberturvallisuuteen liittyen. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa yritysten hallituksille työkaluja ja tukea kyberturvallisuuden edistämiseen, mutta opasta voivat hyödyntää kaikenkokoiset organisaatiot. Opas kehottaa kartoittamaan organisaation tilanteen, eli mitkä järjestelmät ovat yhteydessä toisiinsa, kenellä on pääsy mihinkin tietoihin, kuka omistaa verkon tai palvelun sekä määrittää mitkä tietoteknisen ympäristön osat ovat tärkeimpiä. (Traficom, 2020a, s. 10)

Edellä mainitussa oppaassa kehotetaan pohtimaan mikä organisaatiota voisi uhata. Miksi hyökkääjä olisi kiinnostunut juuri kyseisestä organisaatiosta? Mitkä uhat ovat merkityksellisiä organisaatiolle ja miksi? Samalla arvioidaan uhkien mahdolliset vaikutukset ja todennäköisyys sille, että uhat kohdistuvat organisaatioon. (Traficom, 2020a, s. 20)

Organisaatioiden kannattaa laatia tietoturvaohjeet henkilöstölleen. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas korostaa koulutetun ja valppaan henkilökunnan merkitystä turvallisuuspoikkeamien havaitsemisessa. Organisaatiolle on tärkeää, että henkilöstö raportoi havaitsemistaan kyberuhkista ja poikkeamista. Näiden käsittelyyn täytyy olla selkeät prosessit. Henkilökunnan täytyy kokea olevansa kannustettuja raportoimaan ja tietää miten ja kenelle poikkeamista voi kertoa ja. (Traficom, 2020a, s. 26)

Monimenetelmäisellä tunnistautumiselle (Multifactor authentication, MFA) tarkoitetaan sitä, että käyttäjän identiteetti todennetaan useampaa eri tunnistautumistapaa käyttämällä. Käyttäjätunnuksen ja salasanan lisäksi vaaditaan esimerkiksi tekstiviestitse saapuva koodi tai puhelimen sovelluksessa pitää hyväksyä kirjautuminen. (Traficom, 2021) Microsoftin Digital Defense -raportin yksi tärkeimmistä suosituksista on MFA:n käyttöönottaminen. MFA pysäyttää kirjautumistietoihin perustuvat hyökkäykset, kun hyökkääjällä ei ole pääsyä sisäänkirjautumiseen vaadittavaan lisävahvistukseen. (Microsoft, 2021, s. 125)

Käyttö- ja pääsyoikeuksien hallinta on merkittävä keino lisätä turvallisuutta. Organisaatioiden tulisi pohtia kenellä on tarvetta millekin tiedoille ja keille pääsyoikeudet halutaan myöntää. Vähimmän oikeuden periaatteella tarkoitetaan sitä, että työntekijällä on pääsy tietoon, jota hän työnsä tekemiseksi tarvitsee. Pääsy työtehtävien kannalta tarpeettomiin tietoihin rajoitetaan. Pääsyoikeuksien rajaamisella pystytään rajaamaan myös mahdollisia tietovuotoja ja vahinkoja. Tällöin vääriin käsiin päätyneellä tilillä ei pystytä aiheuttamaan niin suurta haittaa.

Käyttöoikeudet tulee myös muistaa poistaa lopettaneilta henkilöiltä. (Traficom, 2020b, s. 14)

Laitteiden ja järjestelmien päivittäminen on tietomurroilta suojautumisen kannalta erittäin tärkeää. Ohjelmistopäivitykset sisältävät usein haavoittuvuuksien korjauksia, minkä vuoksi ne on tärkeää asentaa mahdollisimman pian niiden julkaisun jälkeen. Hyökkääjät usein hyödyntävät järjestelmien haavoittuvuuksia, jonka takia haavoittuvuuksia sisältävillä järjestelmillä on suurempi riski joutua tietomurron kohteeksi. (Traficom, 2021) Microsoftin Digital Defense -raportti suosittaa virustorjunnan asentamista ja käyttöönottoa torjumaan haittaohjelmahyökkäyksiä (2021, s. 124).

Kiintolevyt on syytä salata, jotta kiintolevyjen sisältämiin tiedostoihin ei pääse käsiksi esimerkiksi siirtämällä kiintolevy toiseen laitteeseen (PK-yrityksen kyberturvallisuuden kehittäminen, 2013, s. 23). Myös Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä suosittaa salaamaan kaikkien työasemien kovalevyt hyvällä salaustuotteella (VAHTI 2/2015, 2015, s. 18).

Organisaation tärkeimmistä tiedoista on hyvä ottaa säännöllisesti varmuuskopiot ja ne on tärkeää säilyttää erillään suojattavista järjestelmistä, jotta esimerkiksi haittaohjelmat eivät tee varmuuskopioista käyttökelvottomia. Varmuuskopiot pitää pystyä palauttamaan, joten tietojen palauttamista on syytä testata säännöllisesti. (Traficom, 2021)

Lokitiedot keräävät tietoa siitä, mitä, miksi ja milloin jotakin tapahtui. Kyberturvallisuuskeskuksen mukaan riittävän hyvä loki sisältää tiedon siitä, milloin tapahtuma tehtiin, kuka teki, mitä teki ja onnistuttiinko teossa vai ei. (Traficom, 2020c)

Pilvipalvelut ovat viimeisen vuosikymmenen aikana yleistyneet osana yksityishenkilöiden, yhteisöjen ja yritysten tavallista tietojenkäsittelyä. Niiden valtteja ovat kustannustehokkuus, helppokäyttöisyys ja kyky

vastata erilaisiin tarpeisiin. Organisaatioiden on kuitenkin hyvä pohtia mitä tietoja käsitellään, ovatko tiedot luottamuksellisia, pitääkö tietoihin päästä käsiksi myös tilanteissa, joissa Internet-yhteys ei toimi. (Traficom, 2019, ss. 3-4)

Pilvipalveluiden yleistymisen vuoksi omien paikallisten palvelinten käyttö on vähentynyt viime vuosina. Oman palvelin vaatii alkuun muun muassa investointeja laitteisiin, asennukseen, ohjelmistoihin, varmuuskopiointeihin ja niin edelleen. Lisäksi oman palvelimen ylläpitäminen vaatii joko sisäistä tai ulkoista IT-henkilöstöä tukea, ylläpitoa ja tietoturvaa varten. (Diamond, 2020)

VPN-yhteys eli virtuaalinen erillisverkko (virtual private network) mahdollistaa organisaation verkon käyttämisen turvallisesti esimerkiksi etätöissä. Tämä mahdollistaa esimerkiksi paikallisten palvelinten käyttämisen myös muualla kuin vain organisaation toimipisteessä.

3 Aineisto ja tutkimusmenetelmät

Osiossa esitellään tutkimusprosessia ja tutkimuskysymykset sekä tietoa kyselylomakkeen laadinnasta, tutkimusmenetelmistä ja aineiston keräämisestä.

3.1 Tutkimusprosessi

Tutkimusprosessi käynnistyi tutustumalla tietoturvaan ja jo ennestään tehtyihin selvityksiin kolmannen sektorin toimijoista. Opinnäytetyön toteuttaja työskentelee järjestöjen parissa ja tukee heitä digitalisaatioon liittyvissä haasteissa, mikä alun perin johdatti aiheen pariin.

Prosessi käynnistyi keväällä 2020 tapaamalla Microsoftin Suomen ja Ruotsin yhteiskuntasuhdejohtajan sekä Microsoftin Digital Crime Unitin Euroopan, Lähi-idän ja Afrikan tiimin johtajan, joiden kanssa keskusteltiin

järjestöjen digitalisaation haasteista ja etenkin tietoturva-aspekti nousi keskustelussa esiin. Kolmannen sektorin toimijoilla tietoturvaan liittyvät haasteet ovat monesti samankaltaisia kuin pienillä ja keskisuurilla yrityksillä, joilla ei ole suurta henkilöresurssia käytössään. He kannustivat rajaamaan aiheen tietoturvaan painottuvaksi.

Tutkimusmenetelmäksi valikoitui määrällinen kyselytutkimus, koska opinnäytetyön tarkoituksena oli selvittää järjestöjen tietoturvan tilaa. Määrällisen tutkimuksen avulla saadaan yleensä tietoa olemassa olevasta tilanteesta, mutta sen avulla ei pystytä selvittämään asioiden syitä. Internet-pohjainen kysely on helppo toteuttaa, sen tulokset ovat käytettävissä reaaliajassa ja tiedot ovat helposti siirrettävissä tilasto- ja taulukkolaskennan ohjelmiin. (Heikkilä, 2014)

Kyselylomake laadittiin kesällä 2020 ja kysely toteutettiin syksyllä 2020. Kysely ehdittiin juuri julkaista ennen suurta Vastaamo-tietomurtoa. Kyseinen tietomurto nosti tietoturva-aiheen pinnalle, mikä varmasti osaltaan nosti vastaajamäärää. Opinnäytetyöprosessi jäi tauolle perhevapaiden vuoksi vuoden 2020 lopussa ja opinnäytetyö viimeisteltiin vuoden 2022 alussa.

3.2 Tutkimuskysymykset

Opinnäytetyölle määritellyt tutkimuskysymykset ovat:

- Miten tietoturva on huomioitu järjestöjen toiminnassa?
- Vaikuttavatko järjestön toimintabudjetti ja henkilöstön määrä tietoturvan tasoon?

3.3 Kyselylomakkeen laadinta ja tutkimusmenetelmät

Ennen kyselylomakkeen laadintaa perehdyttiin tietoturvan osa-alueisiin ja kartoitettiin millä kysymyksillä saataisiin mahdollisimman hyvin arvioitua, miten tietoturva on otettu yhdistysten toiminnassa huomioon.

Kyselylomaketta tehdessä on varmistettava vastaajan kiinnostus kyselyn aihepiiriä kohtaan, jotta hän on motivoitunut vastaamaan kyselyyn. Jokaisen kysymyksen kohdalla on varmistettava mitä kysymys mittaa, onko se täsmällinen, onko kysymyksessä turhia sanoja tai vastaajaa johdattelevia sanoja ja onhan yhdessä kysymyksessä varmasti kysytty vain yksi asia. (Vilkka, 2007, s. 64–65)

Kyselyn laatimisessa otettiin huomioon myös vastaajajoukko ja heidän tieto- ja taitotasonsa tietoturvaan liittyen, joten kysymykset piti saada mahdollisimman helposti ymmärrettäviksi. Tämän vuoksi monessa kysymyksessä oli mukana lisätietoja antava teksti tai esimerkki.

Muuttuja ovat mitattavia asioita, joista määrällisessä tutkimuksessa halutaan tietoa. Muuttujat voivat saada erilaisia arvoja. Strukturoidussa kyselyssä vastausvaihtoehdot on vakioitu. (Vilkka, 2007, ss. 14–15) Kyselylomakkeesta tehtiin pääosin strukturoidun, eli vastaajalle vastausvaihtoehdot olivat valmiiksi määriteltyjä.

Suurin osa kysymyksistä oli kyllä/ei -kysymyksiä, eli käytössä oli dikotominen asteikko, jota on yleensä hyvä pyrkiä välttämään, mutta joissakin tilanteissa on luontevinta vastata ”kyllä” tai ”ei” (Vehkalahti, 2019, s. 39). Nämä kysymykset kartoittivat sitä, onko jokin tietoturvaratkaisu vastaajan järjestössä käytössä vai ei.

Taustamuuttujia koskevissa kysymyksissä oli myös yksi avoin kysymys, joihin vastaajat pystyivät vastaamaan ainoastaan numeerisesti IT-henkilöstön määrän. Kyselyn loppuun lisäsin kolme avointa kysymystä

täydentämään vastauksia ja antamaan lisätietoa järjestöjen tilanteista ja ajatuksista.

Aineistosta analysoitiin miten muuttujien saamat erilaiset arvot, eli havainnot, ovat lukumäärällisesti esiintyneet. Eli millaisia frekvenssijakaumia muuttujat ovat saaneet. Frekvenssi ilmoittaa muuttujan havaintojen lukumäärän aineistossa (Vilkka, 2007, s. 123).

Lisäksi tarkasteltiin muuttujien välistä korrelaatiota. Korrelaatio ilmoittaa kahden jatkuvan muuttujan lineaarista yhteyttä. Pearsonin korrelaatiokerroin on yksi eniten käytetyistä tunnusluvuista kahden muuttujan välisen yhteisvaihtelun tarkasteluun. Pearsonin korrelaatiokerroin voi saada arvoja ainoastaan välillä -1 ja 1. -1 kertoo täydellisestä negatiivisesta korrelaatiosta, eli kun toisen muuttujan arvot kasvat, niin toisen muuttujan arvot pienenevät samassa suhteessa. 1 kertoo täydellisestä positiivisesta korrelaatiosta, eli molemmat muuttujat kasvavat samassa suhteessa. (Kestilä-Kekkonen, n.d.)

Kyselylomakkeen alkuun sijoittuivat taustamuuttujia, kuten tyyppiä, kokoa ja budjettia, kartoittavat kysymykset. Näiden kysymysten jälkeen lomakkeessa olivat vuorossa organisaation sisäistä organisointia käsittelevät kysymykset, kuten IT-henkilöstön määrää, IT-palveluiden ulkoistamista ja vastuuhenkilön nimeämistä koskevat kysymykset.

Seuraavaksi lomakkeessa kysyttiin suojautumiseen liittyviä kysymyksiä, joilla kartoitettiin virustorjuntaa, laitteiden ja järjestelmien säännöllistä päivittymistä ja kiintolevyjen salausta.

Tiedon luottamuksellisuuteen liittyivät käyttöoikeustasojen määrittelyä, käyttäjätilien elinkaarta ja ja kaksivaiheista tunnistautumista kartoittavat kysymykset. Tietojen eheyteen puolestaan liittyivät lokitietojen tallentumiseen, varmuuskopioiden säännöllisyyteen ja varmuuskopioiden palauttamisen testaamiseen liittyvät kysymykset. Tietojen saatavuutta

kartoittivat pilvipalvelujen käyttöön, paikallisten palvelinten ja VPN-yhteyden käyttöön liittyvät kysymykset.

Kyselyn loppuun sijoittuivat kolme avointa kysymystä, joissa kysyttiin suurinta tietoturvapuutetta organisaatiossa, mikä koetaan hyvin tehdyksi asiaksi tietoturvaan liittyen sekä viimeisenä vapaa sana, jossa sai jättää kommentteja kyselystä. Näiden avointen kysymysten vastaukset tarkasteltiin teemoittelun avulla. Teemoittelu on kvalitatiivisen analyysin menetelmä, jossa tutkittavasta aineistosta pyritään löytämään keskeisiä aihepiirejä eli teemoja (Saaranen-Kauppinen & Puusniekka, 2006).

3.4 Aineiston kerääminen

Kysely päädyttiin toteuttamaan Google Formsin avulla sen helppokäyttöisyyden vuoksi ja kyselyä jaettiin TechSoup Suomen uutiskirjeessä ja Facebook-sivulla sekä erilaisissa järjestöjen Facebook-ryhmissä.

Näissä kaikissa kanavissa oli lyhyt tekstimuotoinen saatekirje. Saatteessa tulee antaa riittävästi tietoa tutkimuksesta, koska vastaajan motivointi vastaamiseen alkaa saatekirjeestä (Vilkka, 2007, s. 65).

Saatekirjeessä perusteltiin kyselyn tärkeyttä muun muassa tarjoamalla tietoa suomalaisesta järjestökentästä, siitä miten paljon järjestöillä on suojeltavia tietoja ja miten pienillä resursseilla järjestöt toimivat sekä toteamalla, ettei Suomessa ole tehty järjestöjen tietoturva-asioita kartoittavia kyselyitä.

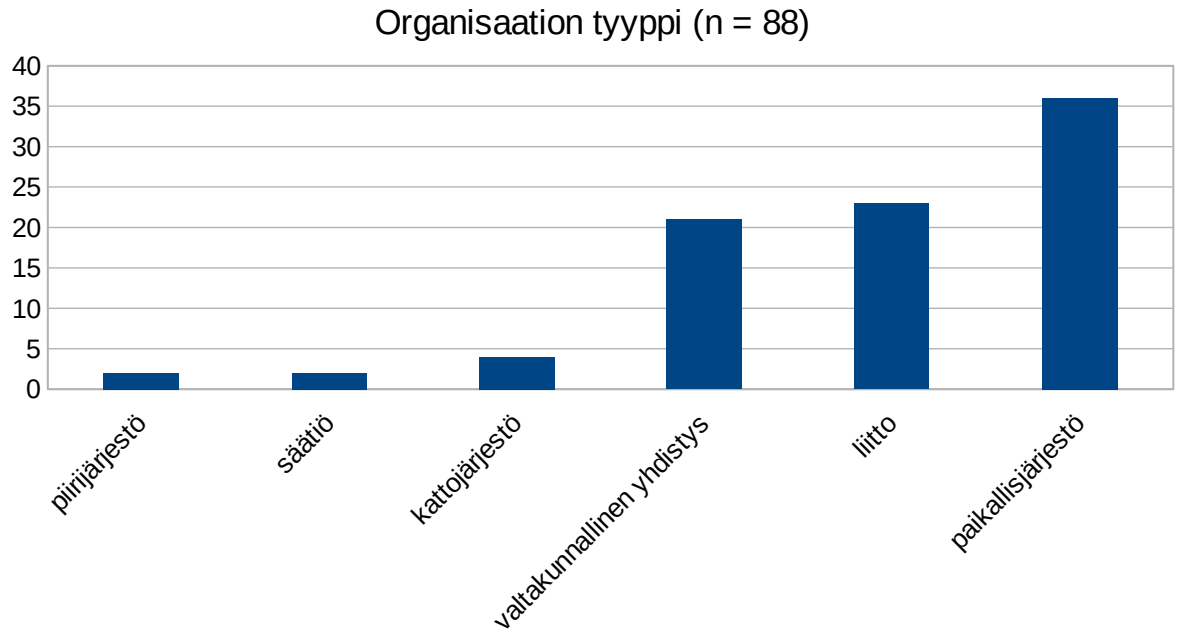
4 Tulokset

Kyselyyn vastasi 88 erityyppistä kolmannen sektorin toimijaa. Tavoitteena oli saada 60 vastausta, joten vastaajien määrä yllätti positiivisesti.

4.1 Taustamuuttujat

Kuvassa 1 esitellään vastaajaorganisaatioiden tyypit. Vastaajaorganisaatioista kaksi oli piirijärjestöjä, kaksi säätiöitä, neljä kattojärjestöä, 21 valtakunnallista järjestöä, 23 liittoa ja 36 paikallisjärjestöä.

Kuva 1: Organisaation tyyppi



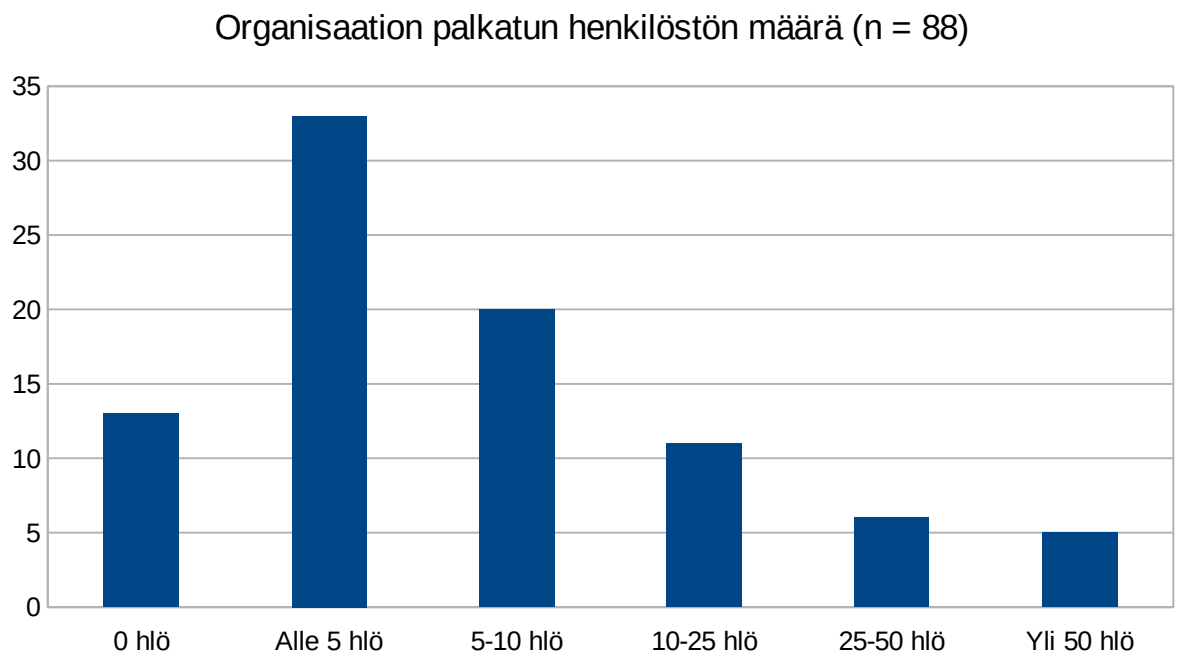
Paikallisjärjestöt toimivat nimensä mukaisesti paikallisella tasolla, kuten esimerkiksi Parolan Eräveikot ry, joka puolestaan kuuluu Hämeen Partiopiiriin, joka on piirijärjestö. Hämeen Partiopiiri taas toimii Suomen Partiolaisiin, joka on liitto.

Valtakunnallisen järjestön toiminta-alaa on koko Suomi ja se voi toimia itsenäisesti tai se voi koota alleen useita saman alan järjestöjä. Kattojärjestö kokoaa alleen aina saman aihepiirin järjestöjä.

Säätiö on yksi kolmannen sektorin toimija järjestöjen ohella. Säätiön suurin ero järjestöihin on se, että perustettavalla säätiöllä on oltava peruspääomaa 50 000 euroa ja sen varainhoidon on oltava suunnitelmallista (Säätiölaki 24.4.2015/487 § 3–5).

Kyselyyn vastanneet organisaatiot olivat suurimmaksi osaksi melko pieniä, kuten kuva 2 tuo esiin. 13 organisaatioissa ei ollut ollenkaan palkattua henkilöstöä, 33 organisaatioissa oli alle 5 henkilöä, 20 organisaatiossa oli 5–10 henkilöä, 11 organisaatiossa oli 10–25 henkilöä, 6 organisaatiossa 25–50 henkilöä ja viidessä organisaatiossa oli yli 50 palkattua henkilöä. Eli 75 prosentissa vastanneista organisaatioista oli 0–10 palkattua työntekijää.

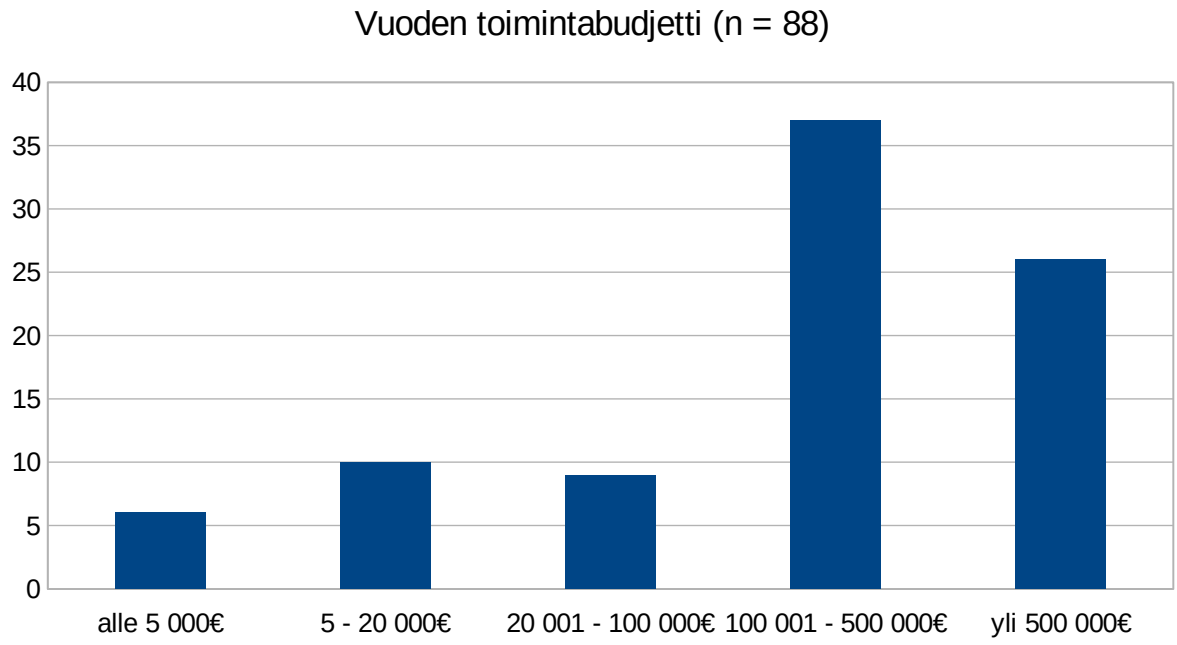
Kuva 2: Organisaation palkatun henkilöstön määrä



Ilman palkattua henkilöstöä toimivista kolmestatoista organisaatioista 12 oli paikallisjärjestöä ja yksi valtakunnallinen järjestö. Yksikään paikallisyhdistys ei työllistänyt yli 50 henkilöä. Muutoin organisaatioiden tyyppi ei vaikuttanut organisaation palkatun henkilöstön määrään.

Vuoden toimintabudjetti oli kuudessa organisaatioissa alle 5 000 euroa, 10 organisaatiossa 5–20 000 euroa, yhdeksässä organisaatiossa 20 001–100 000 euroa, 37 organisaatiossa 101 000–500 000 euroa ja 26 organisaatiossa yli 500 000 euroa (kuva 3). Eli noin 72 prosentissa vastaajaorganisaatioista vuoden toimintabudjetti oli yli 101 000 euroa.

Kuva 3: Vuoden toimintabudjetti



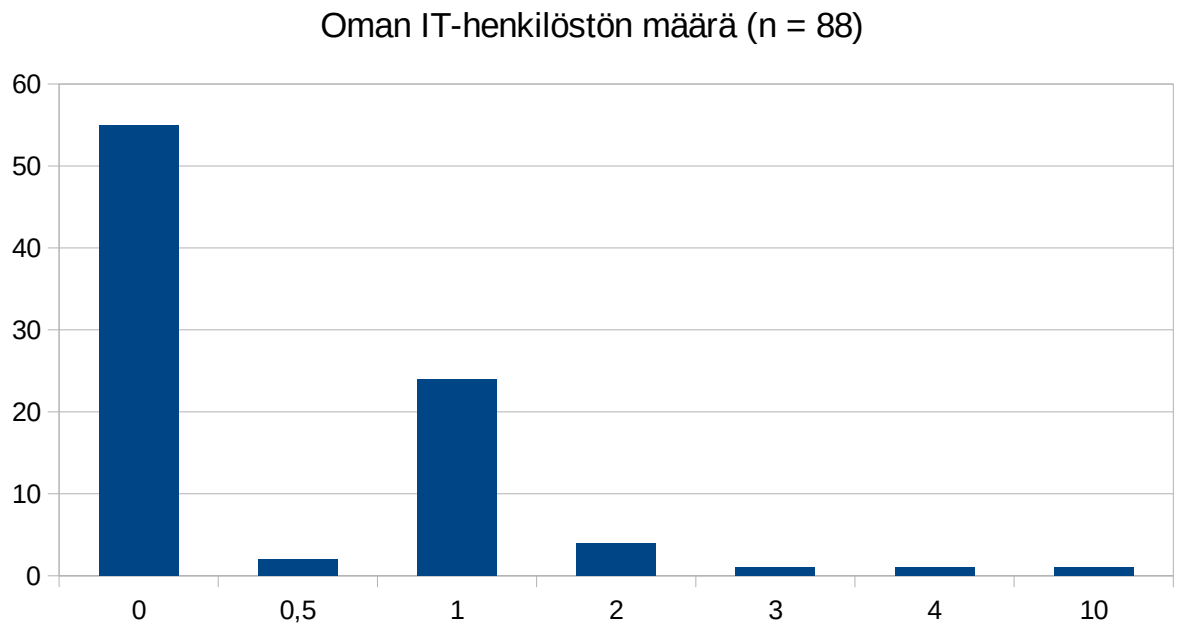
Kuudesta alle 5 000 euron budjetilla toimivista organisaatioista 5 oli paikallisyhdistyksiä ja yksi valtakunnallinen yhdistys. Muutoin vastaajaorganisaatioiden tyyppi ei vaikuttanut organisaation vuoden toimintabudjetin suuruuteen.

Organisaation koon ja vuoden toimintabudjetin välinen korrelaatiokerroin on 0,45, eli näiden kahden välinen yhteys on kohtalainen.

4.2 Sisäinen organisointi

Vastaajaorganisaatiot olivat keskimäärin suhteellisen pieniä, mistä pystyi jo olettamaan, ettei organisaatioissa ole juurikaan omaa IT-henkilöstöä (kuva 4). 55 organisaatiota vastasi, ettei heillä ole ollenkaan omaa IT-henkilöstöä, kahdessa oli 0,5 henkilöä, 24 organisaatiossa yksi henkilö, neljässä kaksi henkilöä, yhdessä kolme, yhdessä neljä ja yhdessä organisaatiossa oli 10 omaa IT-henkilöä töissä.

Kuva 4: Oman IT-henkilöstön määrä



Toimintabudjetin ja IT-henkilöstön määrän välinen korrelaatiokerroin oli 0,11, joten budjetilla ei ole vaikutusta it-henkilöstön määrään. Organisaation koon ja IT-henkilöstön määrän välinen korrelaatiokerroin oli puolestaan 0,45, eli näiden välillä on jonkinlainen yhteys.

Jakauma sen suhteen, onko organisaatio ulkoistanut IT-palvelunsa kokonaan tai osittain, oli melko tasainen. 42 organisaatiota ei ollut ulkoistanut ja 46 organisaatiota oli ulkoistanut IT-palvelunsa kokonaan tai osittain.

Organisaatioissa, jotka olivat ulkoistaneet IT-palvelunsa, vain 12 oli omaa palkattua IT-henkilöstöä (keskimäärin 0,26 henkilöä). Kun taas organisaatioissa, jotka eivät olleet ulkoistaneet IT-palveluitansa, 21:ssä oli omaa palkattua IT-henkilöstöä (keskimäärin 0,83 henkilöä).

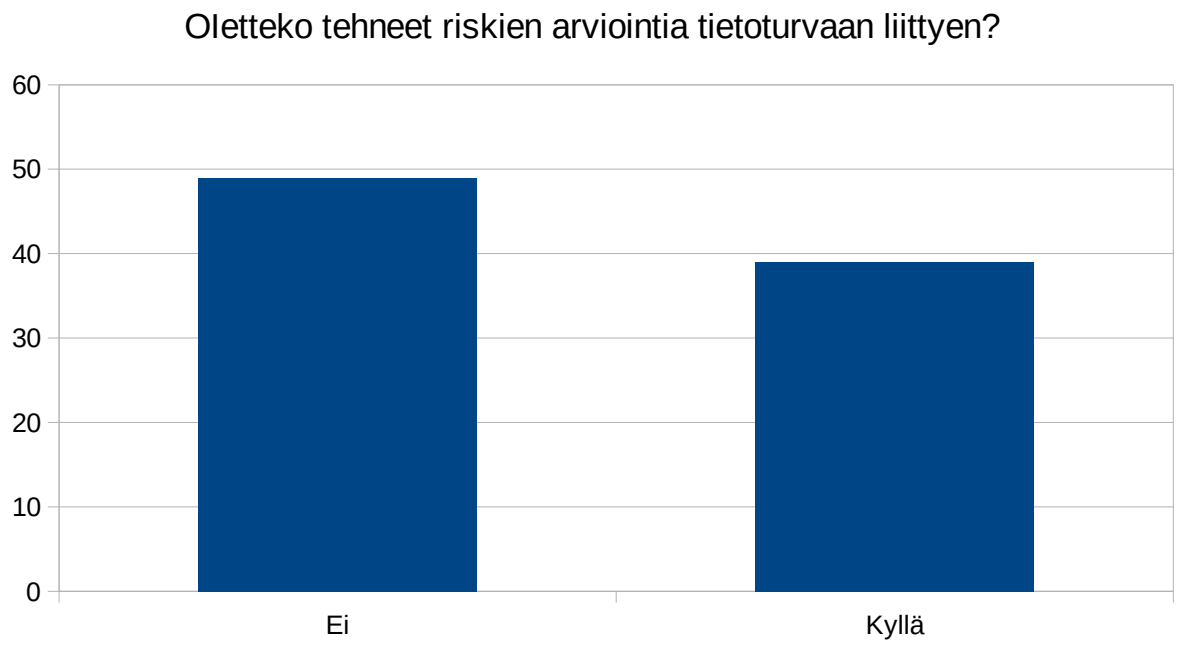
53 vastaajaorganisaatiota ilmoitti, että heillä on nimetty tietoturvasta vastaava henkilö. Kun taas 35 organisaatiossa ei ollut nimetty tietoturvasta vastaavaa henkilöä.

35 organisaatiota, joissa ei oltu nimetty tietoturvasta vastaavaa henkilöä, olivat pieniä organisaatioita. Kuudessa ei ollut ollenkaan palkattua henkilökuntaa, 19 organisaatiossa alle 5, seitsemässä organisaatiossa 5–10 palkattua henkilöä ja vain kahdessa 10–25 palkattua henkilöä.

53 organisaatiossa, jotka kertoivat nimenneensä tietoturvasta vastaavan henkilön, oli enemmän palkattua henkilökuntaa. Organisaation koon ja että tietoturva on nimetty jonkun vastuulle välinen korrelaatiokerroin on 0,37, eli korrelaatio on kohtalainen.

49 organisaatiossa ei oltu tehty riskienarviointia tietoturvaan liittyen (kuva 5). Organisaatiot, joissa riskienarviointi oli tehty, oli keskimäärin enemmän palkattua henkilökuntaa kuin organisaatioilla, joissa riskienarviointia ei oltu tehty. Järjestön koon ja riskienarvioinnin välinen korrelaatiokerroin oli 0,41 eli kohtalainen.

Kuva 5: Oletteko tehneet riskien arviointia tietoturvaan liittyen?



Reilu enemmistö eli 67 prosenttia organisaatioista ilmoitti, etteivät he ole laatineet tietoturvaohjeita henkilökunnalleen, hallitukselleen tai vapaaehtoisilleen. Organisaatioissa, joissa ohjeistus oli laadittu, oli enemmän henkilökuntaa kuin organisaatioissa, joissa ohjeistusta ei oltu laadittu. Järjestön koon ja tietoturvaohjeiden laatimisen välinen korrelaatiokerroin on 0,37, eli korrelaatio on kohtalainen.

Noin puolet vastaajaorganisaatioista, eli 43 organisaatiota, koulutti henkilökuntaansa tietoturvaan liittyen esimerkiksi osana perehdytysprosessia tai muita sisäisiä koulutuksia. 45 organisaatiota ilmoitti, etteivät he kouluttaneet henkilöstöään tietoturvaan liittyen.

91 prosentissa niistä organisaatioista, jotka ilmoittivat kouluttavansa henkilökuntaansa tietoturvaan liittyen, vuosibudjetti oli yli 100 000 euroa. Organisaatioissa, joissa koulutuksia ei järjestetty, vuosibudjetti oli yli 100 000 euroa vain 53 prosentissa vastaajista. Tämän kysymyksen kohdalla sekä budjetin että koon korrelaatio henkilöstön kouluttamiseen liittyen oli

molempien kohdalla kohtalainen. Organisaation budjetin ja kouluttamisen välinen korrelaatiokerroin on 0,45 ja organisaation koon ja kouluttamisen välinen korrelaatiokerroin on 0,43.

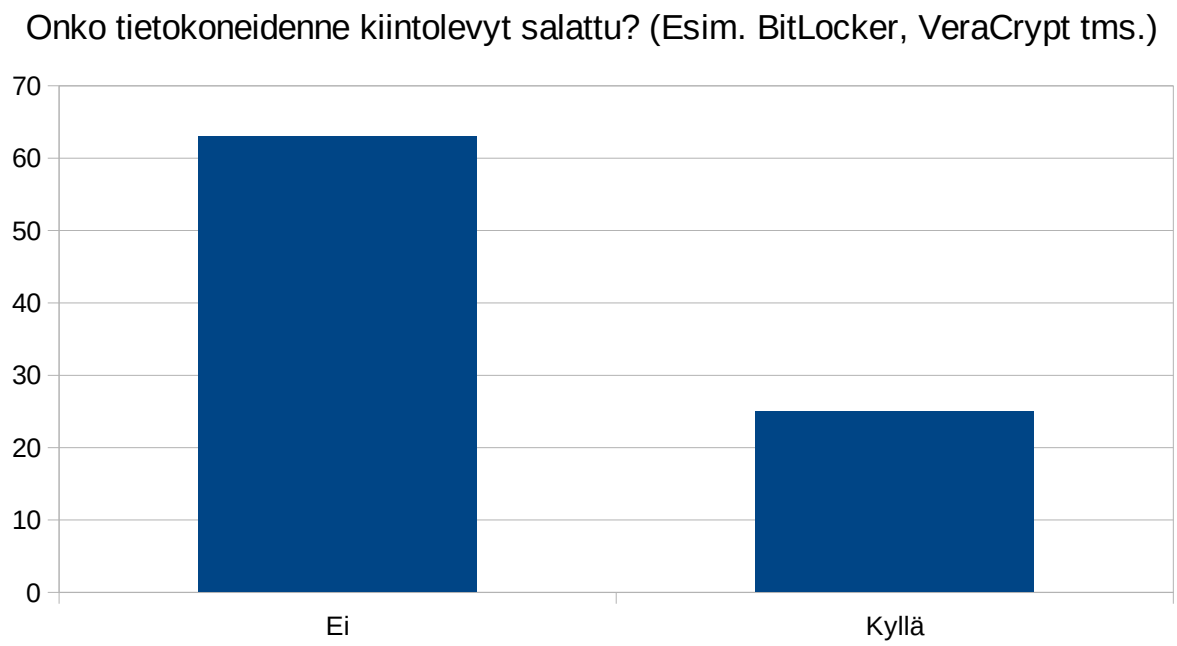
4.3 Laitteiden suojaaminen

Lähes kaikilla vastaajaorganisaatioilla, eli 82 organisaatiossa, oli tietokoneissaan käytössä virustorjunta. Ainoastaan kuusi organisaatiota ilmoitti, ettei heillä ole virustorjuntaa käytössään. Tämän kysymyksen kohdalla esimerkiksi organisaation koko tai vuosibudjetti ei vaikuttanut siihen onko virustorjunta käytössä vai ei.

81 vastaajaorganisaatiota 88 organisaatiosta vastasi, että heidän laitteensa ja järjestelmänsä päivittyvät säännöllisesti. Vain seitsemän organisaatiota vastasi, etteivät heidän laitteensa ja järjestelmänsä päivity säännöllisesti. Tässäkään kysymyksessä organisaation koko tai vuosibudjetti ei selittänyt vastauksia.

63 eli selkeä enemmistö vastaajaorganisaatioista ei ole salannut tietokoneidensa kiintolevyjä (kuva 6). 25 organisaatiota ilmoitti, että kiintolevyt on salattu. Organisaation koolla ja kiintolevyjen salaamisella on kohtalainen yhteys, kun näiden välinen korrelaatiokerroin oli 0,35.

Kuva 6: Onko tietokoneidenne kiintolevyt salattu? (Esim. BitLocker, VeraCrypt tms.)



4.4 Tietojen saatavuus

92 prosentilla vastaajaorganisaatioista oli pilvipalveluja käytössä, eli vain 8 prosenttia vastaajista eivät olleet siirtyneet käyttämään pilvipalveluja. Nämä ei-vastanneet olivat kaikki pieniä organisaatioita, joissa oli alle viisi työntekijää.

Lähes kaikki kyselyyn vastanneet organisaatiot olivat siirtyneet käyttämään pilvipalveluja ja vain 17 vastasi, että heillä on käytössä omia paikallisia palvelimia. Näillä kaikilla oli kuitenkin myös pilvipalvelut käytössä omien palvelinten rinnalla, vuosibudjetti oli 95 prosentilla yli 100 000 euroa ja keskimäärin enemmän omaa IT-henkilökuntaa (1,4 henkilöä) kuin organisaatioissa, joissa ei ollut paikallisia palvelimia käytössä (0,3 henkilöä).

Vastaajista 23 ilmoitti, ettei heillä ole VPN-yhteydelle tarvetta. 44 ilmoitti, ettei heillä ole VPN-yhteyttä ja 21 kertoi, että heillä on VPN-yhteys

käytössä. Mielenkiintoista on, että kaikilla 17 organisaatiolla, joilla on omia palvelimia käytössä, ei ole käytössä VPN-yhteyttä. Ja esimerkiksi kolme organisaatiota, jotka kertovat heillä olevan omia paikallisia palvelimia, ilmoitti ettei heillä ole tarvetta VPN-yhteydelle.

4.5 Tiedon luottamuksellisuus

76 organisaatiota vastasi, että he ovat määritelleet erilaisia käyttöoikeustasoja järjestelmiinsä ja vain 12 ilmoitti, etteivät näitä ole määritelty. Nämä kaikki 12 organisaatiota olivat pieniä organisaatioita, kahdeksassa oli vain alle viisi työntekijää, kolmessa 5–10 työntekijää ja yhdessä ei ollut lainkaan palkattua työntekijää.

Kysymykseen siitä, onko organisaatiossa luotu selkeä ennalta määritelty elinkaari käyttäjätilien luomiseen, ylläpitoon ja poistamiseen, vastaukset jakautuivat lähes tasan. 47 organisaatiota kertoi, ettei heillä ole luotu elinkaarta ja 41 organisaatiota oli luonut elinkaaren käyttäjätileihin liittyen.

Yllättävää oli, että vain 36 organisaatiolla oli käytössä kaksivaiheinen tunnistautuminen järjestelmiin kirjauduttaessa (kuva 7). Eli vain noin 40 prosentilla organisaatiosta oli käytössä kaksivaiheinen tunnistautuminen. Lähes kaikilla organisaatioilla oli kuitenkin esimerkiksi pilvipalvelut käytössä ja kaksivaiheinen tunnistautuminen löytyy nykyään kaikista tarjolla olevista palveluista.

Kuva 7: Onko teillä käytössä kaksivaiheinen tunnistautuminen?

Organisaatioista, joissa kaksivaiheinen tunnistautuminen käytössä, 50 prosentilla vuosibudjetti oli yli 500 000 euroa, kun taas kysymykseen ei-vastanneilla vain noin 15 prosentilla vuosibudjetti oli yli puoli miljoonaa euroa. Järjestön koon ja kaksivaiheisen tunnistautumisen käyttämisen välinen korrelaatiokerroin oli 0,36, eli kohtalainen.

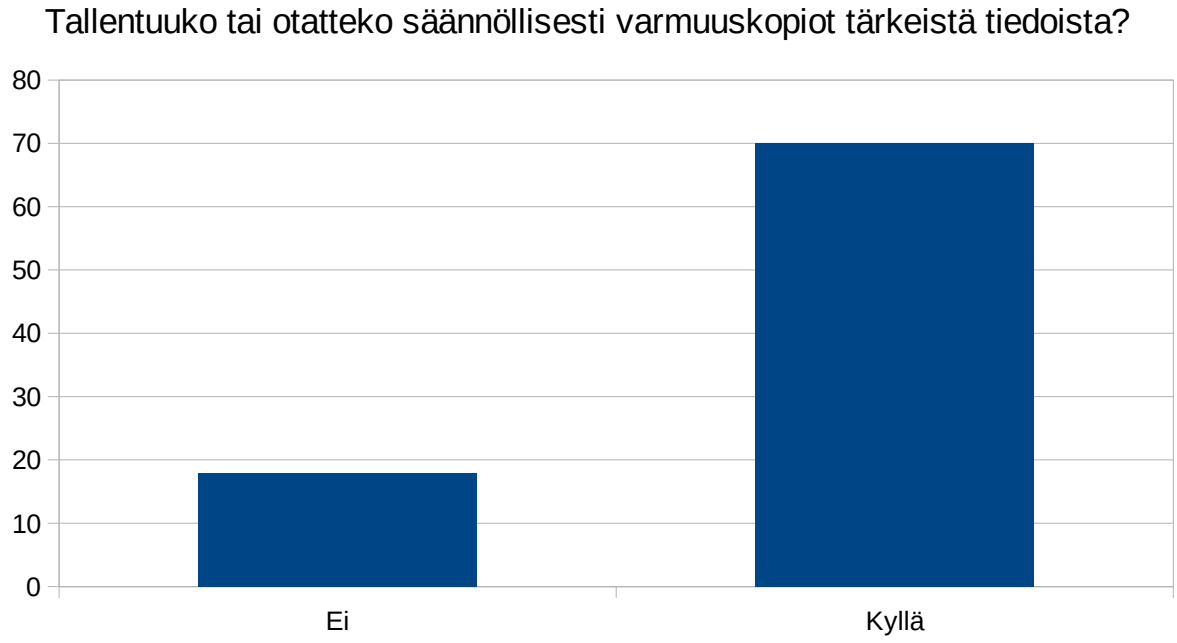
4.6 Tiedon eheys

Kysymykseen ”Onko teillä käytössä keskitetty lokitietojen tallennus-, hallinta- ja käsittelyjärjestelmä järjestelmissänne?” vastaukset jakautuivat tasan puoliksi. 44 organisaatiota vastasi kyllä ja 44 organisaatiota vastasi ei. Vastausten ja budjetin tai organisaation koon välillä ei ollut korrelaatiota.

Hieman yllättävästi jopa 70 vastaajaorganisaatiota 80:stä ilmoittaa, että heillä tallentuu säännöllisesti varmuuskopiot tärkeistä tiedoista (kuva 8). Vain 18 organisaatiossa tätä ei tapahdu. Organisaatiot, joissa ei

varmuuskopioita tallenneta säännöllisesti, ovat keskimäärin henkilöstöltään ja budjetiltaan pienempiä kuin ne, joissa varmuuskopiot tallentuvat.

Kuva 8: Tallentuuko tai otatteko säännöllisesti varmuuskopiot tärkeistä tiedoista?



Kuitenkaan kovin moni organisaatio ei ole testannut varmuuskopioiden palauttamista, mistä olisi hyötyä etenkin kriisitilanteissa. Vain 27 organisaatiota ilmoitti testanneensa palauttamista ja 61 organisaatiota ei ole testannut palauttamista. Organisaation vuosibudjetilla tai henkilöstön määrällä ei ollut yhteyttä varmuuskopioiden palauttamisen testaamiseen.

4.7 Avoimet vastaukset

Kysymykseen ”Mikä on mielestänne suurin tietoturvapuute organisaatiossanne” vastasi yllättäen jopa 64 vastaajaa 88:sta. 16 vastauksessa korostui resurssien puute, niin ajan, rahan kuin välineiden osalta.

”Olemme yhdistys joka tarjoaa IT-palveluita yhdistyksille; haaste on saada tukemamme yhdistykset myöntämään hieman aikaa esim. aiheen koulutukselle ja neuvonnalle. Tietoturva nähdään "turhakkeena", tietosuoja "hidasteena".”

Monissa vastauksissa tuotiin esiin osaamisen puutetta, mikä osaltaan on myös yksi käytössä oleva resurssi. 28 vastauksessa korostui henkilöstön osaaminen sekä se, ettei henkilöstöä ole pystytty kouluttamaan riittävästi.

”Ihmiset ovat iso riski, koska turvallisia käyttötapoja ei aina haluta käyttää, "koska niin ei ole tehty ennenkään". Esim. niin yksinkertainen, kuin koneen lukitseminen koneen ääreltä poistuttaessa, tuottaa joillekin ongelmaa…”

”tiedon puute henkilöstöllä koko aiheesta, eikä ole rakenteita, jotka tukisi tietoturvan edistämistä”

Kuusi organisaatiota toi esiin, että heidän suurin tietoturvapuutteensa on tietoturvaohjeiden, risikikartoitusten ja erilaisten suunnitelmien puuttuminen.

Neljän organisaation mukaan henkilökunnan ja vapaaehtoisten suuri vaihtuvuus aiheuttaa ongelmia. Vaihtuvuuden koetaan vaikuttavan muun muassa tietojen siirtoon sekä tietojen luottamuksellisuuteen, kun käyttöoikeuksia voi jäädä roikkumaan.

12 vastauksessa tuotiin esiin enemmän teknisiä puutteita, kuten monimenetelmäisen tunnistautumisen, varmuuskopioiden ja niiden palauttamisen, virustorjunnan, salasanaohjelmien sekä salatun sähköpostin puuttumista.

”2-vaiheinen tunnistus ei kaikilla käytössä koska jokaisella työntekijällä ei ole työpuhelinta. ”

Kysymykseen siitä, mitkä asiat on tehty organisaatiossa hyvin, tuli 58 hyvin moninaista vastausta. 11 vastauksesta tuli ilmi jollakin tavalla tietosuoja, henkilötietojen käsittely ja se, ettei tarpeettomia tietoja kerätä. Yleisen tietosuoja-asetuksen voimaantulo keväällä 2018 on todennäköisesti vaikuttanut paljon siihen, että organisaatiot kiinnittävät paljon huomiota henkilötietojen käsittelyyn.

”Jäsenrekisterin suhteen on selkeä käsittelytapa ja -tiheys, erityisesti eronneiden suhteen ei "hillota" aiheettomasti kenenkään tietoja.”

Yhdeksän vastaajaa kertoi, että pilvipalveluiden käyttöön siirtyminen on parantanut heidän organisaationsa tietoturvaa. Vastaajat kokivat, että tärkeiden tietojen tallentaminen pilveen parantaa niiden saatavuutta ja säilymistä. Lisäksi tuotiin esiin pilvipalveluihin sisältäviä tietoturvaratkaisuja, kuten monimenetelmäistä tunnistautumista ja sähköpostiliitteiden ja linkkien automaattista tarkistusta.

Kahdeksan vastaajaa toi esiin, että organisaatio on onnistunut ulkoistamaan IT-palveluitansa hyvälle kumppanille.

”Palvelun ulkoistaminen luotettavalle kumppanille, joka on tarvittaessa auttanut ja hoitanut tietoturvaan liittyvät haasteet ripeästi. Infra (sisäverkot, pilvipalvelut, virustorjunta jne.) on ajantasalla.”

Erilaisia tietoturvaratkaisuja mainittiin kahdeksassa vastauksessa. Näitä ratkaisuja olivat muun muassa lähiverkon turvallisuus, palomuuri, ohjelmistojen ja palvelinten päivittäminen, varmuuskopiointi, työasemien tietoturva ja ohjelmistojen suojaukset ja salaukset.

Neljä vastaajaa koki, ettei mitään ole tehty hyvin tietoturvaan liittyen tai että siihen ei ole ollut mahdollisuuksia.

Vapaa sana -kenttään tuli 25 vastausta. Osassa vastaukissa täydennettiin aiempia vastauksia, kuten kerrottiin, että osa järjestelmistä kirjoittaa lokia ja osa ei.

Kolmessa vastauksessa tuotiin esiin järjestöille suunnattuja pilvipalveluja, joita Microsoft ja Google tarjoavat ilmaiseksi tai alennetuilla hinnoilla järjestöille. Näiden koettiin parantavan järjestöjen tietoturvaa.

Vastauksissa tuotiin myös esiin se, etteivät kaikki IT-palveluidentarjoajat ymmärrä järjestöjen erityispiirteitä. Lisäksi tuotiin esiin pienten järjestöjen haasteena sitä, että on niin paljon sellaista mihin tulisi itse perehtyä ja tehdä, kun ei ole mahdollisuutta ostaa ulkopuolelta. Koetaan, että on vaikea ostaa ulkopuolelta, kun ei tiedetä mikä on tarpeellista ja pelätään, että ostetaan turhia palveluita.

”Sattuipas Riikalle ajankohtainen aihe - tai sitten oli hienosti ja ketterästi reagoitu!

Pienillä toimijoilla on aina tämä pulma, on niin paljon kaikkea sellaista, mihin pitäisi itse perehtyä ja hoitaa, koska ei ole varaa ostaa tätä ulkopuolelta. Tätä on vaikea ostaa ulkopuoliselta, koska emme puhu samaa kieltä palveluntarjoajien kanssa emmekä voi arvioida, mikä on tarpeellista meidän kohdallamme vai myydäänkö meille sinkoa banaanikärpäsen lahtaamiseen. –

Olisipa hienoa, jos tämän kartoituksen tuloksia jatkojalostettaisiin konkreettiseksi työkaluksi!”

Yhdessä palautteessa toivottiin kyselyn pohjalta tehtyä tarkistuslistaa. Kyselyn runko ja lyhyet lisätiedot kustakin kysymyksestä julkaistiin osoitteessa: https://techsoup.fi/content/pieni-tarkistuslista-tietoturvaan-liittyen

”Todella hyvä ja herättävä kysely. Saisiko tämän pohjalta jonkun "tarkista ainakin nämä tietoturva-asiat" -vinkkilistan? :)”

5 Yhteenveto ja pohdinta

Tietoturva järjestöissä -kyselyyn vastanneet organisaatiot edustavat hyvin erilaisia järjestöjä. Suurin osa vastaajaorganisaatioista on suhteellisen pieniä. 75 prosentissa vastaajajärjestöistä on 0–10 palkattua työntekijää, mikä on melko hyvin linjassa aiemmin tehtyjen järjestökartoitusten kanssa. Oikeusministeriön kartoitukseen vastanneista organisaatioista suurimmassa osassa oli alle viisi työntekijää (Saarinen, 2020, s. 5). SOSTEn kyselyyn vastanneissa organisaatioissa oli keskimäärin kolme työntekijää (Peltosalmi ym., 2016, 42).

72 prosentissa vastaajaorganisaatioista vuosibudjetti on yli 101 000 euroa, mikä vastaa hyvin Oikeusministeriön kartoituksen tuloksia. Kyseiseen kyselyyn vastanneista yli puolet ilmoitti järjestön vuosittaisten toimintakulujen olevan yli 100 000 euroa (Saarinen, 2020, s 10).

Kyselyä markkinoitiin sosiaalisessa mediassa ja järjestöjä ICT-asioissa tukevan järjestötoimijan Internet-sivuilla, joten todennäköisesti kyselyyn vastanneet järjestöt ovat keskimääräistä enemmän digitalisaatiosta kiinnostuneita. Kysely tuskin tavoitti esimerkiksi pienimpiä eläkeläisyhdistyksiä, mikä varmasti osaltaan vaikuttaa kyselyn tuloksiin.

Järjestön koko, eli montako palkattua työntekijää järjestössä on, korreloi useamman kysymyksen kohdalla kuin järjestön toimintabudjetin suuruus. Mitä enemmän järjestöllä on henkilökuntaa, sitä todennäköisemmin tietoturva-asioista on huolehdittu paremmin.

Järjestöllä voi olla hyvinkin suuri toimintabudjetti, mutta palkattua henkilökuntaa voi olla suhteellisen vähän. Järjestön toiminnan laatu selittää suurilta osin järjestöjen toimintabudjetin suuruutta. Järjestö saattaa tuottaa paljon palveluita suoraan kohderyhmälleen ympäri

Suomea, esimerkiksi ostamalla ohjaajapalveluita ulkopuolelta, jolloin järjestössä itsessään saattaa olla hyvin vähän palkattua henkilökuntaa.

Järjestöt priorisoivat pienet resurssinsa järjestön toiminnan kannalta keskeisiin toimintoihin, eikä tietoturvaa välttämättä nähdä tällaisena. Pienissä järjestöissä ICT- ja tietoturva-asiat saattavat olla pieni osa esimerkiksi toimistosihteerin tai hallintojohtajan työtehtäviä. Tällöin esimerkiksi riskikartoitukset tietoturvaan liittyen saattavat jäädä tekemättä, koska ne eivät ole niin sanotusti pakollisia. Tietoturvaohjeiden laadintakin vaatii aikaa ja osaamista, jota läheskään kaikissa järjestöissä ei ole.

Kyselyn tulosten mukaan järjestöissä on huolehdittu hyvin virustorjunnasta sekä laitteiden ja järjestelmien päivittymisestä. Nämä ovat helppoja ja edullisia tietoturvatoimia, jotka eivät juurikaan vaadi aktiivista työtä. Virustorjunta toimii, kun se on asennettu ja monet järjestelmät ja laitteet päivittyvät lähes automaattisesti. Tietokoneiden kiintolevyjen salaaminen on varmastikin tuntemattomampaa järjestöille ja saattaa vaatia osaamista, jota heiltä ei löydy. Tämän vuoksi vähemmistö vastaajaorganisaatioista oli salannut kiintolevyt.

Lähes kaikki järjestöt olivat siirtyneet käyttämään pilvipalveluja. Microsoft Tech for Social Impact tarjoaa järjestöille ilmaiseksi Microsoft 365 Business Basicin ilmaiseksi 300 käyttäjälle ja Business Premiumin ilmaiseksi 10 käyttäjälle. Google Järjestöille -ohjelma puolestaan mahdollistaa Google Workspacen maksuttoman käytön järjestöille. Moni järjestö on tarttunut jompaankumpaan tarjoukseen. Molemmat pilvipalvelut sisältävät monia tietoturvatoimia, kuten monimenetelmäisen tunnistautumisen, mahdollisuuden määritellä erilaisia käyttöoikeustasoja, varmuuskopioita, sähköpostilinkkien ja liitteiden automaattista tunnistamista ja niin edelleen.

Paikallisia palvelimia oli vain 19 prosentilla vastaajista. Palvelimen ylläpitäminen vaatii osaamista ja resursseja, joten organisaatioissa, joissa oli omia palvelimia, oli myös enemmän IT-henkilöstöä.

Monessa järjestössä työskentelee palkatun henkilökunnan lisäksi vapaaehtoisia, jotka todennäköisesti käyttävät omia laitteitaan vapaaehtoistöissä. Tämä saattaa tuoda haasteita tietoturvaan liittyen. Esimerkiksi virustorjunta voi olla haastavaa saada vapaaehtoisten tietokoneille ja puhelimiin. Lähes kaikissa kyselyyn vastanneissa järjestöissä oli kuitenkin määritelty erilaisia käyttöoikeustasoja, joten vapaaehtoisilla tuskin on pääsyä arkaluontoisiin tai erityisen tärkeisiin tietoihin ja järjestelmiin.

86 prosenttia vastaajaorganisaatioista oli määritellyt erilaisia käyttöoikeustasoja järjestelmiinsä. Todennäköisesti yleinen tietosuoja-asetus on saanut järjestöt pohtimaan sitä, kenellä on tarvetta millekin tiedolle.

Yllättäen noin puolet vastaajista ei ollut kuitenkaan määritellyt elinkaarta käyttäjätileille. Jos organisaatiossa ei ole IT-henkilöstöä ja tunnuksia luo esimerkiksi toimistosihteeri, niin on mahdollista, ettei tunnusten sulkemiseen ole luotu prosessia. Monessa organisaatiossa on prosessi uuden työntekijän aloittamista varten, mutta yhtä tärkeää olisi luoda prosessi siihen, mitä tehdään, kun työntekijä tai vapaaehtoinen lopettaa.

Vaikka lähes kaikilla järjestöillä oli käytössä pilvipalvelut, ei niiden mahdollistama kaksivaiheinen tai monimenetelmäinen tunnistautuminen ollut käytössä kuin 40 prosentissa vastaajaorganisaatioista. Kysely on toteutettu syksyllä 2020, joten tilanne on saattanut muuttua kuluneen puolentoista vuoden aikana. Järjestöillä on usein myös käytössä esimerkiksi taloushallinnon ohjelmia, työajanseurantaa ja muita hallinnollisiin töihin vaadittavia järjestelmiä. On toivottavaa, että näistä löytyisi kaksivaiheinen tai monimenetelmäinen tunnistautuminen.

Yllättävää oli, että jopa puolet vastasi heillä olevan käytössä keskitetty lokitietojen tallennus-, hallinta- ja käsittelyjärjestelmä. Toisaalta järjestöjen käyttämistä Googlen että Microsoftin pilvipalveluista löytyy lokitietojen tallennusta ja monet taloushallinnon ohjelmat sekä jäsenrekisterit myös tallentavat lokia, ja esimerkiksi tietosuoja-asetus edellyttää henkilötietojen käsittelyn seuraamista ja valvontaa (Henkilötietojen käsittely yhdistystoiminnassa, 2019, s. 4).

80 prosentilla organisaatioista tallentuu säännöllisesti varmuuskopiot tärkeistä tiedoista, mutta vain 30 prosenttia on testannut varmuuskopioiden palauttamista. Varmuuskopioiden palauttamisen onnistuminen on ensiarvioisen tärkeää, koska toimimattomista varmuuskopioista ei ole hyötyä kenellekään. Mikäli niiden palauttamiseen menee paljon aikaa ja vaivaa, on niiden palauttamisen järkevyyttä myös harkittava.

Avoimista vastauksista nousi esiin järjestöjen tahtotila ottaa tietoturva paremmin huomioon toiminnassaan, mutta heidän nykyiset resurssinsa eivät tue tätä. Järjestö kaipaavat ulkopuolelta tukea tietoturva-asioihin, mutta toisaalta pelkäävät ostaa sitä tiedon puutteen vuoksi. Pelätään, että ostetaan liian suuria ja tarpeettomia palvelupaketteja, kun ei ymmärretä mikä on tarpeellista.

Järjestöille olisi hyvä tarjota tietoturvaan keskittyvää koulutusta esimerkiksi Digi- ja väestötietoviraston Digituki-palvelun ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen yhteistyönä. Järjestöt voisivat myös kaivata esimerkiksi valmiita malleja riskikartoitusten tai tietoturvaohjeiden laadintaan, joita he voisivat käyttää apuna oman järjestönsä tietoturvapohdinnoissa.

Lähteet

Amar, Z. (2020). *The Charity Digital Skills Report.* Skills Platform. https://www.skillsplatform.org/uploads/charity_digital_skills_report_2020.pdf

CyberPeace Institute. (14.7.2021). *The dark side of cyberspace: the threat to NGOs and nonprofits.* https://cyberpeaceinstitute.org/news/the-dark-side-of-cyberspace-the-threat-to-ngos-and-nonprofits/

Diamond, P. (25.9.2020). *Pilvitallennustila ja paikalliset palvelimet: yhdeksän muistettavaa asiaa.* Microsoft. https://www.microsoft.com/fi-fi/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers

Hakahuhta, A. & Koivisto, M. (21.10.2021). Ylen kysely: Enemmistö eduskuntaryhmistä katkaisisi kulttuurin, tieteen ja muiden järjestöjen kytköksen Veikkauksen tuottoihin. *Yle Uutiset.* https://yle.fi/uutiset/3-12153722

Heikkilä, T. (2014). *Kvantitatiivinen tutkimus.* Edita Publishing Oy. Helsinki. http://www.tilastollinentutkimus.fi/1.TUTKIMUSTUKI/KvantitatiivinenTutkimus.pdf

Henkilötietojen käsittely yhdistystoiminnassa. (2.8.2019). Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/documents/6927448/10594424/Henkil%C3%B6tietojen+k%C3%A4sittely+yhdistystoiminnassa/3f0e1e72-ec39-a103-4de9-df5a730ed226/Henkil%C3%B6tietojen+k%C3%A4sittely+yhdistystoiminnassa.pdf?t=1620635100143

Jousilahti, J. (16.12.2019). Kansalaisyhteiskunta on voimissaan, mutta erkaantuuko se kansasta? *Blogi: Tieto käyttöön!* https://tietokayttoon.fi/ajankohtaista/blogi/-/blogs/kansalaisyhteiskunta-on-voimissaan-mutta-erkaantuuko-se-kansasta-

Järjestödigi-kartoitus 2019. (13.12.2019). Avoine Oy, TIEKE Tietoyhteiskunnan kehittämiskeskus ry & Viestintä-Piritta Oy. https://bin.yhdistysavain.fi/1602444/oWL70OZ4w90gGr0WFb0B0SwUYG/J%C3%A4rjest%C3%B6digi-kartoitus%202019.pdf

Kehitysvammaliitto. (19.2.2021). *Tiedote tietomurrosta Papunet-verkkopalvelumme osaan PlaneettaX ja Joulukalenteri Joulupuumetsä* https://www.kehitysvammaliitto.fi/tiedote-tietomurrosta-papunet-verkkopalvelumme-osaan-planeettax-ja-joulukalenteri-joulupuumetsa/

Kestilä-Kekkonen, E. (n.d.) Kovarianssi ja korrelaatio. Teoksessa *Kvantitatiivisen tutkimuksen verkkokäsikirja*. Tampere: Yhteiskuntatieteellinen tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/korrelaatio/korrelaatio/

Microsoft. (2021). *Microsoft Digital Defense Report.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Peltosalmi, J., Eronen, A., Litmanen, T., Londén, P. & Ruuskanen, P. (2016). *Järjestöbarometri 2016.* SOSTE Suomen sosiaali- ja terveys ry. https://www.soste.fi/wp-content/uploads/2018/11/soste_jarjestobarometri_2016.pdf

PK-yrityksen kyberturvallisuuden kehittäminen. (2013). Huoltovarmuuskeskus. https://www.huoltovarmuuskeskus.fi/files/e3eea09b86919c8132f550a2e2df5e4734ca857c/2013_kyberturvallisuusopas_www.pdf

PRH. (7.12.2021, -a). *Yhdistysten ja uskonnollisten yhdyskuntien lukumäärät.* Patentti- ja rekisterihallitus. https://www.prh.fi/fi/yhdistysrekisteri/yhdistysrekisterintilastoja/lukumaaratyhdistysrekisterissajauskonnollistenyhdyskuntienrekisterissa.html

PRH. (7.12.2021, -b). *Rekisteröidyt uudet yhdistykset ja uskonnolliset yhdyskunnat.* Patentti- ja rekisterihallitus. https://www.prh.fi/fi/yhdistysrekisteri/yhdistysrekisterintilastoja/tilastoarekisteroidyistauusistayhdistyksistajauskonnollisistayhdyskunnista.html

Ristolainen, H. (2015). *Osaajat järjestötyössä – Järjestötyöntekijöiden näkemyksiä ammattiataidosta, työn hallinnasta ja tulevaisuudesta.* OK-opintokeskus. https://www.ok-sivis.fi/media/materiaalit-osio/selvitykset-ja-tutkimukset/osaajat-jarjestotyossa.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *Teemoittelu.* KvaliMOTV - Menetelmäopetuksen tietovaranto. Yhteiskuntatieteellinen tietoarkisto https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_4.html

Saarinen, L. (10.4.2020). *Järjestöjen rooli ja osallisuus julkisen hallinnon valmistelu- ja päätöksentekoprosesseissa.* Kansalaisyhteiskunnan neuvottelukunta. Haettu 10.9.2020 osoitteesta https://oikeusministerio.fi/documents/1410853/6299812/5.+J%C3%A4rjest%C3%B6jen+rooli+ja+osallisuus+julkisen+hallinnon+valmistelu-+ja+p%C3%A4%C3%A4t%C3%B6ksentekoprosesseissa.pdf/24f5ff91-444b-d151-183b-c0f2c3036df2/5.+J%C3%A4rjest%C3%B6jen+rooli+ja+osallisuus+julkisen+hallinnon+valmistelu-+ja+p%C3%A4%C3%A4t%C3%B6ksentekoprosesseissa.pdf?version=1.3&t=1611563243200

Säätiölaki 24.4.2015/487. https://www.finlex.fi/fi/laki/ajantasa/2015/20150487

Tietoturva. (9.7.2020). Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Tilastokeskus. (n.d.). *Käsitteet.* Haettu 27.8.2020 osoitteesta https://www.stat.fi/meta/kas/aatteellinen_yh.html

Traficom. (2019). O*hjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille.* Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf

Traficom. (2020a). *Kyberturvallisuus ja yrityksen hallituksen vastuu.* Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficom. (2020b). *Pienyritysten kyberturvallisuusopas.* Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Traficom. (21.7.2020c). *Näin keräät ja käytät lokitietoja.* Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. *https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja?toggle=Lokeja%20koskeva%20lains%C3%A4%C3%A4d%C3%A4nt%C3%B6*

Traficom. (26.7.2021). *Näin suojaudut tietomurroilta.* Liikenne- ja viestintävirasto Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Yhdistyslaki 26.5.1989/503. https://www.finlex.fi/fi/laki/ajantasa/1989/19890503

YTN. (27.8.2020). *Nimissämme lähtenyt kalasteluviestejä – tietomurto pysäytettiin nopeasti* https://ytn.fi/ajankohtaista/nimissamme-lahtenyt-kalasteluviesteja-tietomurto-pysaytettiin-nopeasti/

VAHTI 2/2015. (4.11.2015). *Ohje salauskäytännöistä.* Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Valtiovarainministeriö. https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_2_2015_pdf.pdf

Vaikute.net. (n.d.) Erilaisia järjestöjä. Nuva ry. Haettu 21.2.2022 osoitteesta http://vaikute.net/kansalaisyhteiskunta/erilaisia-jarjestoja/

Vehkalahti, K. (2019). *Kyselytutkimuksen mittarit ja menetelmät.* Helsingin yliopisto.https://helda.helsinki.fi/bitstream/handle/10138/305021/Kyselytutkimuksen-mittarit-ja-menetelmat-2019-Vehkalahti.pdf

Vilkka, H. (2007). *Tutki ja Mittaa – määrällisen tutkimuksen perusteet.* Tammi. http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-mittaa.pdf

Liite 1: Kyselylomake

Kysely

Taustatiedot

- Onko organisaationne
  - liitto
  - kattojärjestö
  - piirijärjestö
  - paikallisjärjestö
  - valtakunnallinen yhdistys
- Organisaation koko (palkatun henkilöstön määrä)
  - 0
  - < 5
  - 5-10
  - 10-25
  - 25-50
  - > 50
- Vuoden toimintabudjetti
  - alle 5 000€
  - 5 - 20 000€
  - 20 001 - 100 000€
  - 100 001 - 500 000€
  - yli 500 000€
- Oman it-henkilöstön määrä (lukumäärä)
- Oletteko ulkoistaneet IT-palvelunne kokonaan tai osittain (käyttäjähallinta, verkko, it-tuki yms.)?
  - Kyllä / Ei

- Onko teillä nimetty tietoturva jonkun henkilön vastuualueeksi?
    - Kyllä / Ei
- OIetteko tehneet riskien arviointia tietoturvaan liittyen (mitä suojeltavaa tietoa teillä on, millaisia uhkia teihin voisi kohdistua, mahdollinen hyökkääjä ja motiivit)
    - Kyllä / Ei
- Oletteko laatineet tietoturvaohjeet henkilökunnallenne?
    - Kyllä / EI
- Koulutatteko henkilökuntaanne tietoturvaan liittyen? (Esim. osana perehdytysprosessia tai muita sisäisiä koulutuksia)
    - Kyllä / Ei
- Onko työkoneissanne käytössä virustorjunta?
    - Kyllä / Ei
- Päivittyvätkö laitteenne ja järjestelmänne säännöllisesti?
    - Kyllä / Ei
    - Onko tietokoneiden kiintolevyt salattu? (Esim. BitLocker, VeraCrypt tms.)
        - Kyllä / Ei
- Onko teillä käytössä pilvipalveluja?
    - Kyllä / Ei
- Onko teillä käytössä omia paikallisia palvelimia?
    - Kyllä / Ei
- Onko teillä käytössä VPN-yhteys mikäli henkilöstöllä on tarve päästä sisäverkkoon tai palvelimille esim. kotoa?
    - Kyllä / Ei
    - Ei tarvetta päästä
- Oletteko määritelleet/jaotelleet erilaisia käyttöoikeustasoja järjestelmiinne? (Esim. kenellä on oikeus tarkastella jäsenten henkilötietoja, kenellä on oikeus tarkastella palkkatietoja taloudenhallintajärjestelmissä yms.)

    - Kyllä / Ei

- Onko teillä luotu selkeä ennalta määritelty elinkaari käyttäjätilien luomiseen, ylläpitoon ja poistamiseen? (Kuka vastaa luomisesta, millainen käyttöoikeustaso kuuluu millekin roolille yms.)

    - Kyllä / Ei

- Onko teillä käytössä kaksivaiheinen tunnistautuminen järjestelmiinne kirjautuessa? (Esim. tekstiviestivahvistus tai puhelimen sovelluksessa kirjautumisen hyväksyntä)

    - Kyllä / Ei

- Onko teillä käytössä keskitetty lokitietojen tallennus-, hallinta- ja käsittelyjärjestelmä järjestelmissänne? (Eli tallentuuko esim. tietoa siitä, kuka on muokannut tietoa ja muokkaustapahtuman aikaleiman)

    - Kyllä / Ei

- Tallentuuko tai otatteko säännöllisesti varmuuskopiot tärkeistä tiedoista?

    - Kyllä / Ei

- Oletteko testanneet varmuuskopioiden palauttamista?

    - Kyllä / Ei