Jussi-Pekka Karisaari

KESKISUOMALAISTEN MIKROKOKOISTEN TILITOIMISTOJEN KYBERTURVALLISUUSKOMPETENSSI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Karisaari, Jussi-Pekka
Keskisuomalaisten mikrokokoisten tilitoimistojen kyberturvallisuuskompetenssi
Jyväskylä: Jyväskylän yliopisto, 2022, 89 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Moilanen, Panu

Digitalisaatio on tehnyt tietojärjestelmistä ja IT-laitteista yhä yleisempiä työkaluja pienten yritysten liiketoiminnassa. Erityisesti älylaitteiden lukumäärän kasvu on edesauttanut tätä kehitystä. Tämä asettaa kuitenkin yritykset ja organisaatiot kyberturvallisuuden kannalta vaikeaan tilanteeseen, sillä IT:n ja internetistä riippuvaisten ratkaisujen yleistyminen tuo mukanaan lukuisia yritystoiminnalle mahdollisesti vaarallisia kyberriskejä. Sekä ulkoiset että sisäiset uhat altistavat yritykset hakkeroinnille ja kyberrikollisuudelle. Riskien hallinnointiin ja minimointiin täytyy investoida aikaa ja muita resursseja, mutta pienillä yrityksillä ei valitettavasti ole kuin rajallisesti resursseja ohjattavaksi kyberturvallisuuteen. Tilitoimistot, erityisesti mikrokokoiset sellaiset, ovat työnkuvansa johdosta erityisen riskialttiissa asemassa. Tämä tutkimus ottaa siksi tarkastelun kohteeksi keskisuomalaiset mikrokokoiset tilitoimistot. Yritysten haastatteluilla ja näistä saatavilla vastauksilla analysoidaan näiden yritysten kyberturvallisuusosaamista ja varautumisen tasoa ja pohditaan, onko näiden suhteen merkittävästi parantamisen varaa.

Asiasanat: kyberturvallisuus, kompetenssi, kyberstrategia, tilitoimistot, mikrokokoiset yritykset, pk-yritykset

ABSTRACT

Karisaari, Jussi-Pekka
Cyber security competence of micro-sized accounting firms in Central Finland
Jyväskylä: University of Jyväskylä, 2022, 89 pp.
Information Systems, Master's Thesis
Supervisor(s): Moilanen, Panu

Growing digitalization has made information systems and IT equipment increasingly common tools among SMEs. The increase of smart devices in particular has helped this development. However, this puts companies and organizations in a difficult position in terms of cyber security, as the proliferation of IT and Internet-dependent solutions brings with it numerous cyber risks that are potentially dangerous to business operations. Both external and internal threats expose companies to hacking and cybercrime. Time and other resources need to be invested in managing and minimizing risks, but unfortunately small businesses have only limited resources available to focus on cybersecurity. Accounting firms, especially micro sized ones, are in a particularly high-risk position due to what their job entails. This study therefore examines micro sized accounting firms in Central Finland. I will analyze the cyber security expertise and the level of preparedness of these companies through interviews and findings from earlier studies and consider whether there is room for significant improvement in these respects.

Keywords: cyber security, competence, cyber strategy, accounting firms, microenterprises, SMEs

KUVIOT

SISÄLLYS

1 JOHDANTO

Kyberturvallisuus on käsitteenä hyvin laaja. Tämä juontaa jo siitä, että termi kyber on itsessään jotakuinkin ylenpalttinen, kattaen käytännössä kaiken IT:hen liittyvän internetistä tietokoneisiin ja tietoverkkoihin, yleistäen koko digitaalisen bittien maailman (Limnéll ym., 2014, 29). Kyberturvallisuus on lisäksi vahvasti läsnä kaikessa nykyajan toiminnassa, sillä elämme maailmassa, jossa tietokoneilla on ratkaiseva merkitys arjessa, töissä ja vapaa-ajalla. Tällaisessa ympäristössä turvallisuuden takaaminen, olkoon kyseessä sitten tiedon, laitteiden tai henkilön turvallisuus, on ensiarvoisen tärkeää.

Kyberturvallisuudesta on tullut vuosien varrella yhä merkittävämpi termi. Digitalisaation ja IT:n käyttöönoton yleistymisen myötä kaikki yhteiskunnan osa-alueet ovat tiiviisti kytköksissä tietoverkkoihin, ja ennen kaikkea liikeelämä on omaksunut uutta teknologiaa. Kaikenlaisesta tietoturvaan liittyvästä on tullut äärimmäisen tärkeä osa yritystoimintaa, sillä tietotekniikalla ylläpidetään äärimmäisissä tapauksissa koko organisaation olemassaoloa, kaikkea varallisuutta ja korvaamatonta informaatiota.

Voidakseen järjestää kyberturvallisen toimintaympäristön yrityksen täytyy tehdä selonteko käytössään olevista resursseista, tunnistaa organisaatiota uhkaavat riskit ja uhat ja suunnitella kyberstrategia, jolla saavutetaan ennalta määritellyt tavoitteet (Mandritsa ym., 2018). Tämän toteuttamiseen ja lopputulokseen vaikuttavat monet seikat, erityisesti yrityksen koko ja ennalta omaksuttu tietämys.

1.1 Pien- ja mikroyritykset

Pienyrityksellä viitataan alle 50 hengen henkilöstön omaavaan organisaatioon, jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa (Tilastokeskus). Ne vastaavat lähes 99 % koko Suomen yrityskannasta ja yli kolmanneksen kaikkien yritysten yhteen lasketusta kokonaisliikevaihdosta

(Yrittäjät, 2019). Niillä on siis merkittävä rooli kansantalouden kehityksen kannalta.

Pienyritykset elävät kyberturvallisuuden suhteen suuren murroksen aikaa. Edellä mainittu digitalisaation vuosikymmeniä jatkunut yleistyminen on aiheuttanut sen, että monet ICT-alan ulkopuolella toimivat yritykset ovat aktiivisesti osana kyberympäristöjä tietojärjestelmien käyttöönoton takia. Näin kybertoimijoiden määrä kasvaa, samaten liiketoiminnan puitteissa liikkuva pääoma.

Mikroyritykset – henkilökunnan koko alle 10 henkeä (Tilastokeskus) – jakavat monelta osin samoja piirteitä ja ovat siksi varsin samanlaisessa asemassa kuin pienyritykset, mutta pienemmän kokonsa johdosta näillä on odotetusti pienemmät resurssit käytettävissään (Osborn & Simpson, 2015, 248). Tämä voi olla kyberturvallisuuden kehittämisen näkökulmasta joko uhka tai asiaintilaa helpottava seikka. Tätä asetelmaa tullaan tässä tutkimuksessa avaamaan tarkemmin.

1.2 Tilitoimistot

Tilitoimistot ovat yrityksiä, joiden toimialaa on muiden yritysten, organisaatioiden ja yksityishenkilöiden kirjanpito ja talouden hallinto. Työn luonteen vuoksi kyseisen alan toimijat käsittelevät päivittäin asiakkaidensa yksityiseksi tai arkaluontoiseksi miellettävää materiaalia, mikä vaatii paitsi luottamusta, myös käsitystä tietoturvasta. Pk-yritykset ovat omaksuneet digitalisaation ja sähköisen taloushallinnon jokseenkin vahvasti osaksi toimintatapojaan, vaikka kehittämisen varaa löytyy (Yrittäjät, 2020). Täten on syytä olettaa, että tilitoimistot taloushallinnon ammattilaisina ovat omaksuneet tämän kehityksen. Tilitoimistot voisivat siksikin olla varsin houkuttelevia kohteita kyberrikollisille, ja muutkin tietoturvaan kohdistuvat uhat ovat erittäin huomionarvoisia.

1.3 Miksi mikrokokoiset tilitoimistot?

Kuten edellä mainittu, tilitoimistot ovat asemansa vuoksi houkuttelevia kohteita rikollisille ja erityisen haavoittuvaisia digitaalisessa ympäristössä toteutuville uhkakuville. Mitä pienempi yritys on kyseessä, sitä suurempi on todennäköisyys joutua kyberrikollisuuden tai muun kyberuhkan uhriksi (Osborn & Simpson, 2015, 247). Ainakin teoriassa näin voisi olettaa, käytännön tasolla tutkimus pyrkii selvittämään, onko asia näin.

1.4 Kompetenssi

Kompetenssi eli pätevyys viittaa kykyyn/osaamiseen määriteltyjen tehtävien parissa, erityisesti yksilötasolla. Se pureutuu terminä myös käytökselliseen puoleen; ei pelkästään opittuun tietoon, vaan havainnointiin ja mukautumiseen (Barrie & Pace, 1997, 336-337).

Kompetenssilla tässä tutkimuksessa haetaan erityisesti tutkittavan alan oman viiteosaamisen ulkopuolisia taitoja: oletusarvoisesti mikrokokoisten tilitoimistojen työntekijöiltä ei voi odottaa täydellistä asiantuntemusta kyberturvallisuuden saloihin tai IT:n teknisesti vaativimpiin seikkoihin. Siksi juuri näihin seikkoihin paneudutaan.

1.5 Raportin tavoite ja tutkimuskysymykset

Tämän tutkielman tarkoitus on tarkastella tilitoimistoja kyberturvallisuuden valossa ja ennen kaikkea selvittää, millaiset lähtökohdat mikrokokoisilla tilitoimistoilla on tietoturvan suhteen. Kyberturvallisuutta käsitteenä avataan myös tarkemmin.

Tutkimuskysymykset ovat siis seuraavat:

- Mitä on kyberturvallisuus ja kyberturvallisuussuunnitelma ja mitä ne pitävät sisällään?
- Millä tavalla mikrokokoiset tilitoimistot huolehtivat yrityksensä ja asiakkaidensa tietoturvasta?
- Onko mikrokokoisilla tilitoimistoilla joitain huomioitavia erityispiirteitä kyberturvan ja sen kehittämisen suhteen?

2 KYBERTURVALLISUUS

Kyberturvallisuus on monipuolinen termi, koska sillä voidaan viitata muun muassa kyberympäristöjen tai -laitteiden turvallisuuteen, henkilöiden tietoturvaosaamiseen tai tiedon. Monelle tutumpi termi tietoturva ei riitä käsittämään kaikkea nykyisen kyberturvallisuuden ilmiöitä, koska informaatioteknologian kehittyessä ja laajetessa termi on tullut käsittämään enenevissä määrin paitsi tietoa ja sen turvaamista, myös ihmisiä itseään. (von Solms & van Niekerk, 2013, 101.) Ihmisten rooli kyberturvallisuudessa on siksi merkittävä, koska yhä useampi diginatiivi[1] uppoutuu webympäristöihin arkisten asioiden puitteissa ja tulee siten altistuneeksi verkon vaikutuksille, sekä hyvässä että pahassa.

Turvallisuus ei myöskään ole sanana yksiulotteinen, merkiten vain havainnoitavaa, fyysisten tekijöiden luomaa takuuta siitä, ettei mitään pahaa tapahdu. Turvallisuus on yhtä paljon tunnetta, standardeja ja opittuja malleja (Limnéll ym., 2014, 34).

Tämä luku tarkastelee kyberturvallisuutta sekä yleisellä tasolla että korostaen pk-yritysten kannalta tärkeitä seikkoja. Yleisimmät termit ja käytännöt määritellään ja selitetään lyhyesti.

2.1 Kyberturvallisuuden elementit

Kyberturvallisuus ei ole mikään irrallinen konsepti, joka täydellisesti määrittää tietoturvan säännöt tai asettaa täydelliset raamit, joita pitää noudattaa. Se muodostuu lukuisista tekijöistä, niin ihmislähtöisistä kuin teknisistä asioista.

2.1.1 Laitteet, ohjelmat ja järjestelmät: tekninen elementti

Tiedon turvaamisen perspektiivistä tiedonkäsittelyyn käytettävät laitteet ovat kyberturvallisuuden keskiössä. Näillä laitteilla, kuten tietokoneilla, tableteilla ja älypuhelimilla dataa luodaan, lähetetään ja vastaanotetaan. Ne toimivat globaa-

[1] Digitaalisen maailman keskuuteen syntynyt ja/tai sen parissa sujuvasti toimiva henkilö

lin tiedonvälityksen ”postilaatikkoina” internetin toimiessa kuriiripalveluna, ja ovat siten äärimmäisen olennaisia digitaalisen maailman ylläpitämisessä. On siis selvää, että niiden rooli kyberturvallisuudessa on tärkeä, sekä suojelemisen kohteena kuin alustanakin.

Jain ja Pal (2017, 791) luettelevat merkittävimmät (tekniset) puitteet tai ympäristöt, jotka lukeutuvat kyberturvallisuuden piiriin:

1. **Sovellusturvallisuus**, eli laitteisiin asennettujen ohjelmien käyttö sekä niiden suojaaminen ulkoisilta uhkilta;
2. **Tietoturvallisuus**, kattoterminä digitaalisen ja ei-digitaalisen datan turvalliseen prosessointiin ja tähän liittyviin strategioihin;
3. **Sähköpostiturvallisuus**, tämän ollessa yksi yleisimmistä kanavista tietomurroille;
4. **Mobiililaitteiden turvallisuus**, näiden lukumäärän kasvaessa nopeasti mobiililaitteisiin kohdistuu paljon uhkatekijöitä;
5. **Verkkoturvallisuus**, eli internetin ja tietoverkkojen käytön turvallisuus;
6. **Langaton turvallisuus**, eli (usein vähemmän suojattujen) langattomien verkkoyhteyksien turvalliseen käyttöön liittyvät toimenpiteet.

2.1.2 Käyttäjät eli ihmiselementti

Laitteet, ohjelmat ja muu IT:n tekninen puoli muodostavat vain yhden osan kyberturvallisuuden kokonaisuudesta. Käyttäjät eli ihmiset ovat merkittävä elementti, viime kädessä jopa tärkein osa kyberturvallisuutta. Ilman ihmiskäyttäjää IT-järjestelmät ovat pääsääntöisesti pelkkiä toimettomia ohjelmia, yksinkertaisenkin tiedonkäsittelyn aloittamiseen tarvitaan ihminen. Vielä emme elä maailmassa, jossa tekoäly kykenisi suorittamaan tehokkaasti ja turvallisesti digitaalisen ympäristön työtehtäviä sekä käsittelemään ja suojaamaan dataa.

Toisaalta ihminen on useimmiten se kyberturvallisuuden ketjun heikoin osa juuri siksi, että ihminen on kykenevä tekemään inhimillisiä virheitä (Nobles, 2018, 72). Täten resilienssistä muodostuu tärkeä tekijä pohdittaessa ihmisen roolia kyberstrategian osana (Kleij & Leukfeldt, 2019). Näitä seikkoja käsitellään tarkemmin haavoittuvuuksia ja resilienssiä käsittelevissä luvuissa.

2.2 Kyberturvallisuussuunnitelma

Kyberturvallisuuden käytänteillä ja menettelytavoilla pyritään tiedostamaan ja määrittelemään yleiset säännöt tietoturvan toteuttamiseksi (Bayuk ym., 2012, 4-5). Kuitenkin ilman selkeää tietoa yrityksen päämääristä, keinoista ja käytettävissä olevista resursseista voi turvallisuuden ylläpitäminen suuntautua pahimmillaan väärille raiteille. Siksi kyberturvallisuus tarvitsee takaajakseen laa-

ditun ja toimivan suunnitelman, jolla määritellään tarkasti kyberturvallisuuden implementointi kulloisessakin toimintaympäristössä.

Hyvin toteutettu kyberturvallisuussuunnitelma ottaa huomioon kaikki tekijät ja toimijat, jotka potentiaalisesti vaikuttavat tietoturvaan joko negatiivisesti tai positiivisesti (Mandritsa ym., 2018). Suunnitelmallinen toiminta edellyttää tietoturvatarkastuksen toteuttamista organisaation sisällä sekä yhteisen turvallisuussäännöstön laatimista (Iguer ym., 2014). Selkeän päämäärän sekä realististen ja ymmärrettävien toimintatapojen ja -suunnitelmien kehittely, kirjaaminen ja opettaminen avaavat organisaatiolle mahdollisuuden käsitellä kyberympäristöä ja sen lainalaisuuksia ja uhkia oikeaoppisesti.

Riskien ja uhkien arvioiminen (englanniksi risk assessment) on ensiarvoisen tärkeää suunnitelman toiminnan kannalta (Damenu & Balakrishna, 2015, 371). Ilman ymmärrystä siitä, mitkä tekijät tai toimijat voivat aiheuttaa vahinkoa organisaatiolle ja sen toiminnalle, ei voida kehittää toimivaa suunnitelmaa ongelmien torjumiseksi tai ratkaisemiseksi. Tätä prosessia kuvataan tarkemmin myöhemmin, samaten yleisimpiä riskejä ja uhkia.

2.2.1 Kyberstrategia

Kyberturvallisuussuunnitelmaa voisi kuvailla tavoitteeksi kehittää selkeitä käytännön toimenpiteitä tietoturvan ylläpitämiseksi. Se siis poikkeaa hieman kyberturvallisuusstrategiasta, mikä on toinen yleisesti käytetty termi. Tällä viitataan usein pitkäjänteiseen suunnitelmaan, jolla taataan organisaation tai valtion sekä sen sisällä toimivien tahojen esteettömyys kyberympäristöissä ja niiden piirissä, joskin erityisesti valtioiden kesken on hieman eroja siinä, miten kyberstrategia tulkitaan ja toteutetaan (Min ym., 2015). Esimerkiksi Suomen kyberturvallisuusstrategia (Turvallisuuskomitea, 2019) korostaa että ”kyberturvallisuuden varautuminen edellyttää yhteiskunnan eri toimijoiden, julkishallinnon ja elinkeinoelämän välistä yhteistyötä ja osaamisen vahvistamista eri sektoreilla”. Täten Suomella on olemassa ohjenuora, jonka varaan rakentaa varsinaisia toimintasuunnitelmia.

Edellä kuvaillun kaltaiset turvallisuusstrategiat ovat sisällöltään hyvin kattavia ja suuripiirteisiä, vaikuttaen tuhansien tai jopa miljoonien toimijoiden arkeen. Yritysten – erityisesti pienyritysten – näkökulmasta moinen skaala voi vaikuttaa varsin ylimalkaiselta. Hakusanoilla ”cyber strategy” saadaankin tuloksena lähinnä tutkimuksia ja artikkeleita kansallisista kyberturvallisuusstrategioista. Kaikki yritykset ja organisaatiot kuitenkin noudattavat jonkinlaista strategiaa toiminnassaan, olkoon kyse liiketoimintastrategiasta tms. Kyberin huomioiminen tässä kokonaiskuvassa on vain yksi osa suurta kokonaisuutta, mutta äärimmäisen tärkeä sellainen. Suunnitelma sanana on myös mahdollisesti helpompi sisäistää kuin abstrakti strategia. Siksi tässä tutkimuksessa sanoja kybersuunnitelma ja kyberstrategia käytetään samanlaisessa kontekstissa.

2.2.2 Sisäinen turvallisuustarkastus

Toimivan kyberturvallisuussuunnitelman tärkeimpänä kulmakivenä voidaan pitää organisaation merkittävimpien tietoturvahaavoittuvuuksien kartoittamista. Turvallisuustarkastuksella (security audit) tavoitellaan objektiivista arviointia yrityksen toiminnasta kyberympäristössä, sen käytössä olevista järjestelmistä ja prosesseista sekä riskitietoisuutta ennalta määriteltyjen standardien puitteissa (Sabillon ym., 2017, 253-254). Tällainen sisäinen tarkastus antaa siis viitteellisen kuvan vallitsevasta tilanteesta. Tällä ei kuitenkaan välttämättä pureuduta potentiaalisiin uhkatekijöihin tarkemmin, ellei samassa yhteydessä toteuteta haavoittuvuuksien arviointia. Tuota prosessia kuvataan tarkemmin jäljempänä.

2.3 Resilienssi

Turvallisuuskomitean (2018, 14) määritys termille resilienssi (myös kriisinkestävyys/kriisinsietoisuus) ilmaistaan seuraavasti: ”yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä”. Toisin sanoen kyberturvallisuuden puitteissa tällä haetaan erityisesti kykyä valmistautua ja varautua kyberhyökkäyksien aiheuttamiin ongelmiin (Linkov & Kott, 2019, 2). Resilienssillä on täten suuri merkitys tutkittaessa kyberturvallisuuskompetenssia, ja tätä tullaan tarkastelemaan kokonaisvaltaisesti tilitoimistojen kohdalla.

Kriisinkestävyyttää voidaan Kleijin ja Leukfeldtin (2019, 19) mukaan edistää korostamalla neljää kykyä:

- kyky ennakoida mahdollisia ongelmatilanteita tai muutoksia;
- kyky valvoa järjestelmää ja tunnistaa siinä esiintyviä muuttujia;
- kyky reagoida nopeasti muutoksiin oikein keinoin;
- kyky oppia tapahtuneesta kriisitilanteesta ja tehdä soveliaita muutoksia järjestelmiin ja toimintatapoihin vastaisen varalle.

2.4 Riskienhallinta

Riskienhallinta on riskien tiedostamista ja organisaation toiminnan kontrollointia siten, että potentiaalisilta ongelmilta ja vahingoilta vältytään (Limnéll ym., 2014, 109). Olennaisesti kyberriskien hallinnalla tavoitellaan myös riskien lieventämistä hyväksyttävälle tasolle, sillä oletusarvoisesti kaikkia riskejä ei voida täysin poistaa (Eling ym., 2021). Tehokas valmistautuminen tarkoittaa siten mahdollisen aiheutuneen vahingon nopeaa korjaamista kulloinkin sopivalla metodilla.

Hyvin laadittu kyberturvallisuussuunnitelma tai muut organisaation sisäiset, kontrolloidut ohjenuorat ja toimintasäännöt ovat olennainen osa toimivaa riskienhallintaa, sillä se auttaa organisaatiota ennakoimaan ja tunnistamaan riskitekijät hyvissä ajoin (Hopkin, 2018, 3). Suunnitelma vaatii kuitenkin toimiakseen täydellisesti henkilökunnan ehdottoman ymmärryksen yhteisistä pelisäännöistä, mikä kysyy tarkkaa opetusta ja valvontaa.

Kyberriskienhallinnan vaiheissa toistuu hyvin samoja piirteitä kuin organisaation ja kyberin käyttäjien resilienssiä kohottaessa. Näihin vaiheisiin kuuluvat erityisesti riskien tunnistaminen, riskien analysoiminen, riskien hoitaminen sekä riskien seuranta ja tapahtuneen vaaratilanteen arviointi (Eling ym., 2021, 96).

Riskien tunnistamisella pyritään sekä positiivisten että negatiivisten riskien tunnistamiseen ja erityisesti yrityksen toimintaa haittaavien seikkojen erittelyyn (Stine ym., 2020, 8). Tietojärjestelmien osalta nämä voidaan kategorisoida tiedon luottamuksellisuuteen, saatavuuteen tai eheyteen kohdistuviin riskeihin (Eling ym., 2021, 99).

Riskien analysointi tarkoittaa riskin toteutumisen todennäköisyyden ja seurausten arviointia (Stine ym., 2020, 8). Eling ym. (2021, 104) nostavat kyberin kannalta erityiseksi piirteeksi kyberhyökkäysten vaikutusten nopean leviämisen. Riskien kaukokatseinen analysointi voi olla siis hyvinkin haasteellista.

Riskien hoito on prosessi, jossa soveliasta vastatoimenpidettä soveltaen riskin aiheuttamaan potentiaaliseen vahinkoon vastataan. Tämä saavutetaan välttämällä vaikeasti ratkaistavia riskejä kokonaan, lieventämällä riskien aiheuttamaa vahinkoa siedettävälle tasolle tai siirtämällä riskin seuraukset vakuutuksen piiriin ja hyväksymällä jäljelle jääneet riskit mikäli niistä ei ole taloudellisesti merkittävää haittaa (Stine ym., 2020, 31; Eling ym., 2021).

Riskien seurannalla arvioidaan tapahtuneiden riskien aiheuttamia seurauksia, joka johtaa mahdollisiin riskinhallinnan toimenpiteiden muutoksiin. Näin vastaavanlaisen tilanteen sattuessa kohdalle käytössä on tehokkaammat vastareaktiot. Prosessi on parhaimmillaan jatkuvaa, koska kyberturvallisuuden olosuhteet ja teknologia elävät jatkuvaa muutosta. (Stine ym., 2020, 35.)

2.5 Haavoittuvuudet

Haavoittuvuudella tarkoitetaan johonkin asiaan – niin konkreettiseen kuin abstraktiin käsitteeseen – liittyvää tekijää, joka saattaa altistaa kyseisen asian jollekin negatiiviselle seuraukselle. Tietotekniikassa haavoittuvuuksilla siis viitataan pääasiassa tietojärjestelmissä ja laitteissa piileviin ongelmatekijöihin, joskin kyberturvallisuuden viitekehyksessä aihe on laajempi, kuten jäljempänä käydään läpi. (Kizza, 2013, 89)

2.5.1 Laitteet ja järjestelmät

Organisaation käytössä olevat tietotekniset laitteet, verkot ja tietojärjestelmät muodostavat selkeän kyberturvallisuuteen liittyvän haavoittuvuuden. Näiden kautta haittaohjelmat pääsääntöisesti leviävät, ja ne toimivat portteina vakoilulle ja kyberrikollisille. Tämän takia laitteiston ja järjestelmien turvallisuus on äärimmäisen tärkeä askel toimivaan tietoturvaan.

Vanhat tai päivittämättömät järjestelmät eivät aina omaa uusimpia haittaohjelmien ja hakkerointiyritysten torjuntaan liittyviä käytäntöjä ja suojauksia, minkä takia haittaohjelmat pääsevät niihin verraten helposti sisään. Esimerkiksi Demir ym. (2021, 88) tekevät tutkimuksessaan huolestuttavan havainnon, että jopa 95 prosentissa internetin verkkosivuista käytetään vanhentuneita/haavoittuvia ohjelmistoja ja ne ovat täten hyvin haavoittuvaisia.

Myös yleisessä käytössä olevat tietokoneet ja niiden käyttöjärjestelmät vaativat turvallista toimintaa varten säännöllistä päivittämistä. Microsoft Windows XP-käyttöjärjestelmän tuki päättyi 8.4.2014 (Microsoft), mikä aiheutti huolta välittömästä hakkerointien aallosta suojaamattomia Windows-koneita kohtaan ja tästä vaarasta yhtiö itse varoitti. Monet ennakoidut haavoittuvuudet korjattiin Microsoftin toimesta joko etu- tai jälkikäteen, mutta vaara oli silti todellinen. Nykyään maailmalta löytyy vielä tietokoneita, jotka käyttävät tätä jo pitkälti vanhentunutta järjestelmää (Toulas, 2021).

Laitteiden tai järjestelmien ei tarvitse olla edes vanhentuneita, jotta ne tarjoaisivat vapaamman pääsyn tietomurtoihin. Monissa tapauksissa nämä on jätetty täysin avoimiksi tai käytetyt suojaukset ovat liian heppoisia (Fernandez de Arroyabe & Fernandez de Arroyabe, 2021, 16). Tämä voi johtua käyttäjien halusta helpottaa asiointia laitteiden tai järjestelmien kanssa välttämällä helposti unohtuvien salasanojen käyttöä tai nopeuttamalla kirjautumista. Valitettavasti juuri tällainen toiminta tarjoaa hakkereille vapaat kädet murtautua olemattomilla suojauksilla varustettuihin järjestelmiin. Käyttäjän on siis mahdollisesti tehtävä vaikea valinta ehdottoman helppokäyttöisyyden tai toimivan kyberturvan väliltä.

2.5.2 Käyttäjien haavoittuvuudet

Kyberturvallisuus on vain yhtä tehokas kuin siitä vastuussa oleva käyttäjä. Siksi organisaation henkilöstön on oltava vähintään jollain tasolla perillä käytettävissä olevista tietojärjestelmistä, laitteista ja käytänteistä.

Yleinen ymmärtämättömyys tietotekniikasta on ensimmäinen askel kohti potentiaalista kybervahinkoa. Mikäli käyttäjä ei tiedä käyttämästään tekniikasta muuta kuin sen mitä tämä tarvitsee työnsä tekemiseen eikä omien kontaktien keskuudessa ole jotakuta, joka osaisi neuvoa ongelmatilanteissa, ongelmat kasautuvat helposti. Samaten välinpitämättömyys järjestelmien suojausta kohtaan kostautuu helposti mahdollisen kyberhyökkäyksen osuessa omalle kohdalle, erityisesti jos moinen asenne johtaa riskien vähättelyyn (Hadlington, 2017, 12).

Ihmiset ovat myös yksilöllisiä ja tekevät asioita – myös IT:n parissa – eri tavalla, eivät konemaisesti yhtä universaalia tapaa noudattaen (Hall, 2016, 9). Omaksuttuja tapoja ja käytösmalleja syntyy arjessa ja töissä helposti erilaisia. Monet tällaisista voivat olla hyvinkin kyberturvallisuuden käytänteiden vastaisia.

Organisaatiossa voi ilmetä joukoittain tällaisia virheellisiä tai haitallisia toimintatapoja, jotka altistavat tietojärjestelmät, laitteet tai verkot kyberuhkille. Jos näitä ei tiedosteta tai niihin ei mahdollisesti puututa (edelleen joko tietämättömyydestä tai välinpitämättömyydestä johtuen), moisista toimista tulee helposti rutiinia, josta voi olla vaikea irtautua (Hall, 2016, 10). Siksi kyberalttiit prosessit on paikallistettava nopeasti ja näiden varalle rakennettava toimiva kybersuunnitelma.

2.5.3 Haavoittuvuuksien arviointi

Jotta kyberuhkia vastaan voidaan tehokkaasti puolustautua, täytyy siksi olla hyvissä ajoin tiedossa, mitkä ovat merkittävimmät syyt tietoturvaan kohdistuville uhkakuville ja potentiaalisimmat väylät ulkoa tai sisältä toteutuville vahingoille/hyökkäyksille. Tätä toimenpidettä varten on kehitetty haavoittuvuusarviointi (Shinde & Ardhapurkar, 2016). Tämä tarkoittaa organisaation sisällä toteutettavaa katselmusta, jonka yhteydessä tarkastetaan organisaation tietyn osa-alueen tai koko yrityksen toiminnan kyberturvatehokkuutta ja kykyä hahmottaa potentiaalisia tietoturvariskejä. Tarkastus kohdistuu laajimmillaan sekä henkilökuntaan että organisaation käyttämään teknologiaan, laitteisiin ja verkkoihin. Löydetyt haavoittuvuudet kirjataan ylös ja yleensä listataan niiden vakavuuden mukaan. Samassa yhteydessä voidaan myös toteuttaa nk. penetraatiotestausta, jolla simuloidaan kyberhyökkäys ja selvitetään järjestelmän kyky torjua ja kestää ulkoa tulevia uhkia (Shinde & Ardhapurkar, 2016, 3).

Tarkastuksen hyötynä saadaan parhaimmillaan selkeä tilannekuva siitä, mitkä tekijät tai kohteet ovat organisaation potentiaalisesti pahimpia tietoturvaaukkoja (MacDonald ym., 2013). Organisaation johdon ja henkilökunnan tietoisuuden lisääntyminen ilmenneistä ongelmista on myös ehdoton hyöty. Kun koko henkilökunta saa eteensä listan kyberturvallisuushaavoittuvuuksista, toimii se usein selkeänä herätyksenä sekä johdolle että työntekijöille parantaa tietoturvan tasoa.

2.6 Riskit ja uhat

Riskien ja uhkien tiedostaminen ja arvioiminen vaatii kyseisten termien täydellistä ymmärtämistä. Limnéll ym. (2014, 105) huomauttavat, että nämä sanat sekoitetaan usein keskenään, vaikka ne omaavat varsin samankaltaiset merkitykset. Riskillä terminä tarkoitetaan potentiaalista negatiivista seurausta jollekin

tapahtumalle, uhalla vuorostaan varsinaista vaaratilanteen aiheuttavaa toimintaa.

Tietoturvaan liittyvät uhat ovat ilmiöitä ja potentiaalisia haavoittuvuuksia tai muita ongelmatekijöitä, jotka voivat vaarantaa organisaation kyberturvallisuuden. Näitä kyberuhkia on monenlaisia riippuen toimijasta, kohteesta ja päämäärästä. Näihin voidaan sisällyttää ulkopuolelta kohdistuvat, harkitusti toteutetut hyökkäykset joko rikollisten, hakkereiden, vakoilijoiden tai terroristien toimesta, sekä organisaation sisältä nousevat uhat. Nämä uhat muodostavat organisaatiolle tai yksilölle potentiaalisia riskejä, jotka täytyy tunnistaa ja torjua mieluiten ennaltaehkäisevästi. Toisaalta on olemassa täysin ihmisistä riippumattomia tekijöitä, jotka aiheuttavat ongelmia IT-järjestelmille. (Lehto ym., 2015, 8-9.)

2.6.1 Kyberrikollisuus

Kyberrikollisuus eli digitaalisissa ympäristöissä toteutuva rikollinen toiminta on yksi digitalisaation merkittävimmistä uhkista (Kizza, 2013, 108). Nykypäivänä käytännössä kaikki yritysten, organisaatioiden ja valtioiden kuten myös useimpien yksittäisten ihmisten taloudellinen pääoma kulkee elektronisen raha- ja tiedonvälityksen puitteissa. Samaten luottamuksellinen kommunikointi hoidetaan pääasiassa sähköpostitse tai muutoin verkon kautta tavalla, joka on altis datan sieppaamiselle tai häirinnälle. Kyberrikollisuudella kuten rikollisuudella yleensä tavoitellaan pääasiassa rahallista hyötyä, mistä johtuen yritykset ovat usein kyberrikollisuuden kohteena (Lowe, 2014, 12).

Rikollisuuden kannalta edellä kuvaillun kaltainen digitaalinen kehitys on ollut todellinen onnenpotku. Laajat tietoverkot ja tehostuneet kommunikointiteknologiat ovat tarjonneet IT-taitoisille rikollisille keinoja tavoittaa käytännössä lukemattomia uhreja pienellä vaivalla (Yar & Steinmetz, 2019, 14). Siksikin ajan tasalla pysyminen on rikollisuuden kanssa kamppaileville tahoille erittäin tärkeää.

Kyberrikollisuuden käyttämät metodit vaihtelevat, joskin useimmilla pyritään keräämään arvokasta tietoa, kuten käyttäjätietoja, salasanoja, sähköpostiosoitteita tai spesifejä dokumentteja. Virukset, troijalaiset, madot ja vakoiluohjelmat ovat tuttuja termejä kyberhyökkäyksistä puhuttaessa, ja näitä haittaohjelmia käytetään maailmalla päivittäin läpäisemään lukuisien tietojärjestelmien ja laitteiden turvatoimet. (Yar & Steinmetz, 2019.) Nämä leviävät nopeasti käyttäjän selatessa epäilyttäviä linkkejä sisältäviä verkkosivustoja tai avatessa roskapostia. Hyökkäyksen kohteeksi joutunut saastutettu järjestelmä tarjoaa rikollisille vapaan kentän tietojen/tiedostojen varastamiseen tai hävittämiseen. Pahimmassa tapauksessa yksittäinen laite tai kokonainen tietojärjestelmä pystytään kaappaamaan ja näin organisaation toimintaa voidaan haitata aktiivisesti sisältä käsin, ulkopuolisen hakkerin toimesta. (Sikorski & Honig, 2012, 231-232.)

Täysin havaitsematta jäänyt kyberhyökkäys voi aiheuttaa vahinkoa päivien, viikkojen tai kuukausien ajan ennen kuin hyökkääjän toimet paljastuvat – jos paljastuvat. Mikäli hakkerin luoma takaportti järjestelmään jää korjaamatta,

voidaan kyseistä järjestelmää käyttää kyberrikollisuuden välineenä hyvinkin pitkään. (Lowe, 2014, 12)

Kaikki kyberrikollisuudeksi luokiteltava ei ole suoraa kohdennettua hakkerointia, sillä monet rikolliset turvautuvat hienovaraisempiin metodeihin. Phishing eli verkkourkinta pyrkii ”kalastelemaan” kohdeorganisaatiolta arvokasta tietoa esimerkiksi massoittain levitettävien huijausviestien tai tekaistujen verkkosivujen sisältämien, klikkauksesta aktivoituvien vakoiluohjelmien avulla (Akhgar ym., 2014, 156-157). Myös vakuuttavan oloiset tai luotettavilta vaikuttavilta tahoilta saapuvat lomakkeet, joissa pyydetään henkilötietojen täyttämistä tekaistun ongelman korjaamista varten voivat välittää arkaluonteisen yksityistiedon rikollisten haltuun (Sangani & Vijayakumar, 2012, 60). Kekseliäät rikolliset ottavat jopa suoraan yhteyttä kohteeseensa tekeytymällä organisaation esimieheksi tai yhteistyöyrityksen edustajaksi ja pyytämällä pahaaavistamattomalta uhrilta luottamuksellisia tietoja tekosyyhyn vedoten. Tähän ei tarvita muuta kuin riittävän uskottavan näköinen sähköpostiosoite – joskin mahdollisesti aiemmin hakkeroimalla saavutetuista käyttäjätiedoista on suuri apu rikolliselle – ja hyväuskoisuutta vastaanottajalta. (Krombholz ym., 2015, 115.) Näin saadaan kierrettyä tietojärjestelmät ja niiden turvallisuustoimet lähes kokonaan. Tällaista ihmisiin kohdistuvaa, huijaamisen ja vakuuttelun keinoin toteutettua luottamuksellisen tiedon varastamista kutsutaan sosiaaliseksi manipuloinniksi (Conteh & Schmick, 2016, 32).

2.6.2 Kybervakoilu

Vakoilulla pyritään saamaan käsiksi arvokasta tietoa, mikä on erityisesti yritysmaailmassa erityisen vaarallinen uhka. Tämän puitteissa toteutetut tietomurrot ovat verraten hienovaraisempia kuin kyberrikollisten aiheuttama vahinko. Edellisissä tilanteissa haetaan useimmiten selkeää taloudellista hyötyä, vakoilun keskittyessä tiedonkeruuseen (Wangen, 2015). Vakoojan tarkoituksena on ilmestyä huomaamattomasti ja kadota tarvitsemiansa tietojen kanssa ilman merkkejä vahingonteosta. Tällaisen kyberhyökkäyksen toteuduttua tietojärjestelmät ja tiedostot voivat näyttää päällepäin koskemattomilta ja (taloudelliset) resurssit saattavat olla edelleen turvattuja, mutta vahinko on ehtinyt tapahtua esimerkiksi kopioitujen asiakas- ja liiketietojen merkeissä vakoojan pyyhkiessä kaikki jäljet hakkeroinnista (Wangen, 2015, 206-207).

Kybervakoilu on myös yksi kybersodankäynnin muodoista, ja suuri osa vakoilutoiminnasta kohdistuu valtiollisiin toimijoihin, kuten sotilaskohteisiin, hallintoon tai infrastruktuuriin (Kizza, 2013, 81). Mikäli kohteena ovat liiketoimintaa harjoittavat tahot, tekijöinä voi olla paitsi omaa etuaan tavoittelevat kärsivälliset kyberrikolliset, myös vieraan valtion palveluksessa olevat hakkerit, jotka etsivät liikesalaisuuksia oman maansa liiketoiminnan pönkittämiseksi. Näissä tapauksissa pk-yritykset harvoin joutuvat uhreiksi, suurten ja vaikutusvaltaisten organisaatioiden ollessa houkuttelevampia vakoilun kohteita.

2.6.3 Organisaation sisältä kumpuavat uhat

Kaikki tietoturvaan kohdistuvat vaaratilanteet eivät synny ulkoisista uhkatekijöistä, hakkereiden tai muiden pahantahtoisten toimijoiden aiheuttamana. On aina olemassa mahdollisuus, että kyberuhka on lähtöisin organisaation sisältä, yhden tai useamman työntekijän aiheuttamana. Tahallisessa mielessä toteutettu, sisäpiiriläisen aiheuttama taloudellinen vahinko on yhtä ongelmallista kuin ulkopuolisten hakkereiden toteuttamat hyökkäykset, ja sikäli vaarallisempi ja arvaamattomampi uhkakuva. Sillä harva organisaatio osaa odottaa hyökkäystä oman työntekijäkunnan piiristä, ja vieläpä sellaiselta henkilöltä, joka tuntee tietoturvajärjestelyt ja osaa siten peittää jälkensä. (Kizza, 2013, 79-80)

Toisaalta kaikki uhkakuvat eivät juonna tarkoituksenmukaisesta pahanteosta. Ihminen on valitettavan altis tekemään virheitä. Yksittäinenkin vahingossa aiheutettu virhe organisaation tietojärjestelmään, mikä jättää portin avoimeksi hakkereille tai internetissä leviäville haittaohjelmille, voi pahimmillaan johtaa hyvin suuriin vaikeuksiin. (Kleij & Leukfeldt, 2019, 17)

Esimerkiksi eräs yleisimmistä organisaation sisällä tapahtuvista potentiaalisista virheistä on oman laitteen tuominen työpaikalle ja sen liittäminen yhteiseen verkkoon. Varsin yleinen käytäntö varsinkin, jos yritys haluaa säästää rahaa ja tuoda joustavuutta työpaikalle (Olalere ym., 2015, 2). Kontrolloimaton ylimääräisten laitteiden käyttäminen voi kuitenkin pahimmillaan johtaa yrityksen tietojen varastamiseen tai haittaohjelmien leviämiseen näiden mahdollisesti huonosti suojattujen laitteiden kautta (Olalere ym., 2015, 3-4).

Tällaisia vahingossa, puhdasta huolimattomuuttaan aiheutettuja tilanteita on vaikea ennakoida, koska virheitä voi sattua koska tahansa kenelle tahansa. Siksi tehokkaasti valvotun, toimivan kybersuunnitelman luominen ja ylläpitäminen on ensiarvoisen tärkeää.

2.6.4 Kyberterrorismi

Terrorismi yhdistetään helposti pelkästään asein toteutettaviin iskuihin. Internetin kautta tapahtuva terrorismi on kuitenkin yleistynyt selkeästi sitä mukaa, kun kyberhyökkäykseen soveltuva teknologia ja metodit ovat kehittyneet. Pahantahtoisen ideologisen agendan omaavien vihamielisten tahojen kannalta globaali verkko on korvaamattoman arvokas työkalu pelon, epävarmuuden ja materiaalisen tuhon levittämiseen. (Lehto ym., 2015, 12-13.)

Kyberterrorismin kohteeksi voi käytännössä joutua välillisesti kuka tahansa, sillä vaikka terroristit kohdistavat toimensa pääasiallisesti valtioiden viranomaistoimintaa, infrastruktuuria ja/tai julkisia organisaatioita vastaan, on yksilötasolla mahdollista joutua terroristisen hyökkäyksen kärsijäksi. Kriittistä infrastruktuuria vastaan kohdistettu isku vaarantaisi kokonaisen yhteiskunnan ja kaikkien sen toimijoiden arjen (von Solms & van Niekerk, 2013, 100).

2.6.5 Pilvi- ja mobiilipalveluiden turvallisuus

Digitalisaatio on tuonut mobiililaitteet vahvasti osaksi IT-pohjaista työntekoa, älypuhelinten toimiessa tehokkaina viestintävälineinä ja melkein tietokoneiden vastineina turvallisuustekijöitä (Harris & Patten, 2014). Pilvipalvelut vuorostaan ovat mullistaneet tiedonkäsittelyn- ja tallennuksen konsepteja vähentämällä riippuvuutta fyysisistä työympäristöistä ja tallennuslaitteista ja tarjoamalla mahdollisuuksia ketterään informaation jakoon (Damenu & Balakrishna, 2015). Monet pilvipalveluja tarjoavat sovellukset ovat myös saatavilla mobiililaitteisiin, joten näiden teknologioiden yhdistäminen on luonnollista ja tehokasta. Ei ole siis yllätys, että yritykset omaksuvat molemmat konseptit vahvasti osaksi liiketoimintaansa.

Monien muiden uusien teknologioiden tavoin sekä mobiili- että pilvipalvelut avaavat ovet mahdollisiin riskeihin. Tiedonjakokonseptina ne omaavat saman roolin kuin perinteisemmät työkalut ja työympäristöt, joten niitä uhkaavat samat tiedonkäsittelyn väärinkäyttöön liittyvät uhat. Mobiililaitteiden tietoturva ei läheskään aina saavuta muiden IT-laitteiden tasoa, ne ovat alttiita haittaohjelmille ja mobiilisovellusten laadunvalvonta vaihtelee (Harris & Patten, 2014). Pilvipalveluiden virtuaalinen luonne tekee niistä haavoittuvaisia ulkopuolisten tahojen tiedonkeruulle: kuka tahansa, jolla on palvelun käyttäjätunnukset hallussa, pääsee tallennettuun dataan käsiksi koska tahansa ja mistä tahansa (Patel ym., 2020, 759). Huolena on, että erityisesti pk-yritykset luopuvat omien tietojärjestelmien ja -verkkojen turvallisuuden hallinnoinnista kääntymällä enenevissä määrin mobiili- ja pilvipalveluiden ja näiden omiin järjestelyjen puoleen (Kurpjuhn, 2015).

2.6.6 Muut riskitekijät

IT-järjestelmien toimintaan voi vaikuttaa uhkia, joita ei voi pitää verkossa väijyvien pahantekijöiden tai huolimattoman henkilöstön aikaansaannoksina. On täten olemassa riskejä, joita voi olla mahdotonta ennustaa mutta joihin pitää yhtä kaikki varautua.

Onnettomuus- tai vahinkotilanteet, kuten tulipalo tai laitteiden särkyminen voivat aiheuttaa materiaalista vahinkoa, joka vuorostaan voi vaikuttaa suoraan tai välillisesti organisaation toimintaan. Ydintoimintojen keskeytyminen ja korvaamattoman tiedon pysyvä tai tilapäinen katoaminen vaikeuttaa liiketoimintaa ja saattaa asettaa kyberturvallisuuden alttiiksi. Myös ulkoinen vahinkotilanne, joka saattaa aiheuttaa esimerkiksi sähkökatkoksen voi johtaa tilapäiseen toimintojen keskeytymiseen ja epätietoisuuteen, ellei tällaiseen tilanteeseen ole olemassa varasuunnitelmaa. (Lehto ym., 2015, 8-9.)

”Perinteinen” rikollisuus on myös kyberturvallisuusuhka. Rikollinen, joka murtautuu organisaation tiloihin saattaa viedä mukanaan arvokasta dataa sisältäviä tai toiminnan kannalta kriittisiä laitteita, joiden korvaaminen voi olla kal-

lista tai datan suhteen kenties mahdotonta. Myös erityisesti mobiililaitteet ovat alttiita tällaiselle (Kizza, 2013, 438).

Vaikka organisaatiolla ei olisikaan kykyä suoralta kädeltä torjua jotakin edellä mainituista tilanteista, täytyy vahinkojen minimoimisen ja toimintakyvyn nopean palauttamisen oltava prioriteettina suunnitelmaa laadittaessa. Sokea luottamus siihen, ettei mitään tapahdu, ei auta ketään.

3 PIENTEN TILITOIMISTOJEN KYBERTURVAN ERITYISPIIRTEITÄ

Kuten edellä on todettu, pien- ja mikroyritykset ovat merkittävässä roolissa Suomen yritysmaailmassa, lähes 99% yrityksistä ollen tämän kokoluokan toimijoita ja työllistäen n. 45% yrityksissä työskentelevistä henkilöistä (Yrittäjät, 2019). Näin kyberturvallisuus on myös satojentuhansien työntekijöiden ja tuhansien työllistäjien kannalta oleellisessa roolissa.

Pienyrityksiä voidaan tarkastella monin osin samoista lähtökohdista kuin isompia organisaatioita. Sekä suurilla että pienillä yrityksillä on samanlaiset tarpeet kehittää liiketoimintarakenteita ja turvallisuustekijöitä (Harris & Patten, 2014, 100). Joskin henkilökunnan koko ja yleiset resurssikoot ovat luonnollisesti erottavia tekijöitä. Työtehtävissä ja -nimikkeissä on suurella varmuudella myös poikkeuksia: pienissä organisaatioissa tietyt henkilöt omaavat usein varsinaisen työnimikkeensä ulkopuolisia vastuualueita. Päämäärät ovat joka tapauksessa pitkälti samat.

Kyberturvallisuuden suhteen asia on monin tavoin poikkeuksellinen. Vaikka kyberturvallisuudella pyritään kaikissa organisaatioissa lopulta samaan lopputulokseen (datan, verkkojen ja laitteiden koskemattomuus sekä uhista aiheutuvan vahingon minimointi), on eri kokoisten yritysten tietoturvan toteuttamisessa käytännön tasolla mahdollisia eroavaisuuksia. Näitä pk-yritysten erityispiirteitä käsitellään tässä luvussa tarkemmin.

Pienyrityksen näkökulmasta kaikki aiemmassa luvussa käsitellyt kyberturvallisuuden käsitteet ovat ajankohtaisia ja tärkeitä. Riippumatta yrityksen alasta tämä on tavalla tai toisella osa digitaalista verkostoa, sillä tuskin on olemassa yritystä, joka ei työnsä puolesta joudu jossain määrin turvautumaan tietokoneisiin ja tietoverkkoihin. Kyberturvallisuuden tekninen elementti on siis huomioonotettava seikka.

Huomattava osa tilitoimistoista Suomessa on pien- tai mikroyrityksiä, keskimääräisen henkilöstömäärän ollessa noin 4 työntekijää (Kuvio 1). Tästä johtuen pienyrityksiin liittyvät kyberturvallisuusseikat ovat sovellettavissa tilitoimistoihin. Lisäksi tilitoimistojen rooli yritysten finanssiasioiden käsittelijänä

asettaa ne erityisen haasteelliseen asemaan. Jo tämä status tekee kyberturvallisuudesta huolehtimisesta näiden toimijoiden keskuudessa hyvin tärkeää.

Yritykset toimialoittain (yritysyksikkö) muuttujina Vuosi, Toimiala (TOL 2008) ja Tiedot

	Yritysten lukumäärä, yritykset	Henkilöstön lukumäärä (htv), yritykset
2020		
692 Laskentatoimi, kirjanpito ja tilintarkastus; veroneuvonta	4 725	18 035

KUVIO 1 Tilitoimistojen keskimääräinen henkilöstömäärä. (Tilastokeskus, 2020)

3.1 Tilitoimistojen asema digitaalisessa ekosysteemissä

Shojaifarin ja Järvisen (2021, 2) tutkimuksessa pk-yritykset kategorisoidaan neljään ryhmään sen perusteella, miten ne omaksuvat kyberturvallisuustoimenpiteet ja millaiset vaatimukset ne täyttävät:

1. aktiivisesti kyberturvallisuustoimenpiteitä tuottavat yritykset;
2. digitaalisella toimialla toimivat yritykset, joiden painopiste ei kuitenkaan ole kyberturvallisuusratkaisuissa;
3. tietotekniikasta riippuvaiset, loppukäyttäjän roolissa olevat yritykset, jotka käyttävät helposti omaksuttavia valmiita IT-ratkaisuja osana liiketoimintaansa;
4. startup-yritykset, joiden ehdoton huomio on omassa liiketoimintamallissa.

Näistä neljästä kategoriasta tilitoimistot täyttävät selkeimmin ryhmän 3 piirteet, niiden toimialan ollessa vahvasti sidoksissa digitalisaation tuomiin ratkaisuihin ja toimintatapoihin. Pääpainopisteen ollessa muussa kuin syvässä IT:n tuntemuksessa, ne jäänevät suuremmissa määrin loppukäyttäjän rooliin.

3.2 Pienyrityksen koko ja käytettävissä olevat resurssit

Yrityksen koko on merkittävä erottava tekijä kyberturvallisuuden laatimisessa, sillä suurempi organisaatio tarkoittaa yleensä poikkeuksetta isompaa määrää resursseja (Osborn & Simpson, 2015). Kun resursseja on alusta lähtien paljon käytettävissä, on odotettavissa, että osa tästä voidaan kanavoida organisaation kyberturvallisuuden rakentamiseen. Pienet yritykset eivät useinkaan ole yhtä onnekkaita, kyberturvallisuuden ollessa monille vain yksi vastuualue monista muista. Osaajien puuttuessa yritykset voivat joutua turvautumaan ystäviin tai perheenjäseniin hoitamaan tämän työn puolestaan (Berry & Berry, 2018, 2). Ääritapauksissa edes tämä ei ole mahdollista.

Kun resurssien, erityisesti ajan puute aiheuttaa edellä mainitun kaltaisia ongelmia, päädytään vääjäämättä tilanteeseen, jossa kyberturvallisuus jää selkeästi vähäisemmälle huomiolle yrityksen toiminnassa (Kurpjuhn, 2015). Erityi-

sesti yksityisyrittäjälle kyberturvallisuuteen perehtyminen ja sen henkilökohtainen ylläpitäminen tuo jo valmiiksi kiireiselle yrittäjälle lisää vastuuta. Kaikille tämä ei sovi, minkä takia moni saattaa jättää kyberturvallisuuden kokonaan huomiotta, tarkoituksellisesti tai huomaamattaan.

Soveliainta tällaisessa tilanteessa olisi etsiä apua ammattitaitoisilta osaajilta (Bhattacharya, 2011, 302). Toiminnan ulkoistaminen säästäisi yrityksen kyberturvallisuuden aiheuttamalta pähkäilyltä, mutta onko kaikilla pienyrityksillä varaa tai halua tällaiseen, on asia erikseen. Lisäksi sekin tuo mukanaan potentiaalisia riskejä, mikäli ulkoistaminen toteutetaan hätäisesti (Benz & Chatterjee, 2020).

3.3 Pienyrityksen kyberturvallisuussuunnitelma

Pienelle yritykselle kyberturvallisuuden suunnittelu ja toteuttaminen voi olla joko helppoa tai ylitsepääsemättömän vaikeaa tai jotain tältä väliltä. Resurssien vähäisyys sekä suojeltavan datan määrä voivat olla osaavalle tietoturva-asiantuntijalle helpotus. Pienen yrityksen asema auttaa tätä parhaimmillaan hyväksymään joustavasti uusia teknologioita, ylläpitämään yhteisiä pelisääntöjä ja sopeutumaan uusiin tilanteisiin (Harris & Patten, 2014, 100). Yrityksen suljettuun verkkoon kytkettyjen laitteiden pieni määrä puolestaan saattaisi mahdollistaa tiukemman valvonnan ja vaaratilanteessa ongelman nopean paikallistamisen ja vahingon minimoimisen.

Ongelmaksi asia muodostuu silloin, kun organisaatiolla ei löydy lainkaan tietämystä tai asiantuntemusta toimivan suunnitelman toteuttamiseen ja ylläpitämiseen. Pienillä yrityksillä tämä voi olla lähtökohtaisesti todennäköisempää, sillä pienyrityksen resurssit eivät välttämättä riitä tällaisen toiminnan jatkuvaan ylläpitoon taikka löydä yrityksensä sisältä tietotaitoa omaavaa tahoa. Myöskään kaikilla pienyrityksillä ei löydy syvällisempää ymmärrystä kyberympäristöjen hallinnasta, mikä voi johtaa toiminnan improvisointiin. Tämä vuorostaan kasvattaa virheellisten toimintojen toteutumisen riskiä. (Parkin ym., 2016.)

Pienyrityksillä voi olla myös vaikeampi omaksua kyberturvallisuuden ylläpitoon vaikuttavia käytänteitä. Viitseliäisyyteen ja asenteisiin puuttuminen voi olla vaikeata, riippuen kuinka syvälle juurtuneita vallassa olevat toimintamallit ovat. Kyberturvallisuuteen liittyvien seikkojen voidaan nähdä vievän aikaa tuottavuudelta. (Parkin ym., 2016, 71.)

Paljon voi toisaalta riippua yrityksen toimialasta: IT:n parissa toimivan pienyrityksen työntekijä saattaa hyvinkin olla kokeneempi kyberturvallisuuden suhteen kuin tietotekniikan ulkopuolella työskentelevä henkilö. Luonnollisesti nämä ovat yksilöllisiä seikkoja, joiden pohjalta ei voida tehdä selkeitä yleistyksiä.

3.4 IT:n, tekniikan ja järjestelmien tuntemus

Pienyritysten ymmärrys tietotekniikasta ja -järjestelmistä voivat vaihdella suuresti. Yritykset, jotka työskentelevät aktiivisesti kyseisellä alalla itse ja ovat siten ammattilaisia ovat oletettavasti enemmän asioista perillä kuin yritys, joka käyttää IT:tä vain johonkin välttämättömään, kuten kirjanpitoon ja sisäiseen viestintään. Kyberturvallisuuden ymmärrys ja soveltaminen tarvitsee tuekseen käsitystä käytössä olevasta tekniikasta, mutta toisaalta pelkkä tekninen tietotaito ei takaa toimivaa tietoturvaa. Syvempi ymmärrys tekniikan käyttämisestä ja sen syy-seuraussuhteista auttaa käyttäjiään sovellettavien kyberturvallisuusohjeiden kehittämisessä. Pienyritykset, joiden käsitys digitalisaatiosta ja siihen liittyvistä resursseista on puutteellista, ovat yksinkertaisesti erityisen haavoittuvaisia kyberuhkille. (van Haastrecht ym., 2021.) Täten kompetenssilla on jälleen suuri merkitys aihetta käsiteltäessä.

3.5 Pk-yritykset harvemmin kyberuhkien kohteena?

Thompson (2014, 8) nostaa esille, kuinka suuria yrityksiä ja organisaatioita pidetään usein houkuttelevampina kyberuhkien kohteina kuin pienempiä yrityksiä. Tämä ajattelu juontuu siitä, että isojen organisaatioiden käytössä olevan varallisuuden uskotaan houkuttelevan enemmän rikollisia, ja samoin isomman organisaation sisällä alttius inhimillisiin virheisiin vaikuttaa todennäköisemmältä. Luonnollisesti isommalla yrityksellä on enemmän menetettävää, jos ajatellaan puhtaasti liikevaihtoa.

Todellisuus on kuitenkin pk-yritysten kannalta karu: pienet organisaatiot ovat kyberrikollisille yhtä valideja kohteita kuin suuremmat. Tämä on vakava ongelma, varsinkin kun moni pieni ja keskisuuri yritys suunnittelee IT-turvallisuuteensa liittyvät käytänteet laiskasti, koska pienien toimijoiden ei uskota houkuttelevan kyberuhkia (Banham, 2017). Valveutuneet kyberrikolliset ovat erittäin tietoisia tästä ja voivat halutessaan kohdistaa hyökkäyksensä pk-yrityksiin odottaen potentiaalisesti pienempää vaivannäköä verrattuna suurien organisaatioiden kybersuojausten murtamiseen (Thompson, 2014).

Edes varastettavan materiaalin vähäisyys verrattuna suurempiin toimijoihin ei huoleta hakkereita. Läheskään kaikki kyberrikolliset eivät ole miljoonavoittoja tavoittelevia suurtoimijoita tai organisoidun rikollisuuden edustajia, vaan joukosta löytyy myös yksittäisiä toimijoita, joille pienikin saalis voi merkitä paljonkin (Broadhurst ym., 2014). Lisäksi useilta pieniltä yrityksiltä varastetut yksittäiset tiedonmuruset voivat yhdessä muodostaa rikolliselle arvokasta informaatiota, mikä kannustaa kyberhyökkäysten jatkamiseen. Toisaalta pienet yritykset voivat olla asiakassuhteessa isompaan, mikä voi avata väylän kyberrikollisille hyökätä suuremman kohteen kimppuun käyttäen pienyritystä välietappina (Banham, 2017).

Berryn ja Berryn (2018, 9) toteuttamassa tutkimuksessa vain harva pienyritys osoitti joutuneensa kyberrikoksen uhriksi, mikä voi ruokkia mielikuvaa siitä, että valtaosa yrityksistä on turvassa rikollisilta. Tämän kaltainen ajattelu on kuitenkin omiaan aiheuttamaan passiivisuutta yrityksen sisällä. Luulo siitä, ettei kyberrikosta tule tapahtumaan koska näin ei ole aiemminkaan käynyt, voi kostautua pahasti, mikäli tulevaisuudessa kybermurto toteutuu eikä siihen olla varauduttu millään lailla. Varsinkin, mikäli kybermurto on jo toteutunut ja tätä ei ole havaittu: portti vakoilulle ja hakkeroinnille on tällöin kertaalleen avattu ja toimii väylänä rikollisille aina siihen asti, kunnes tämä vuotokohta joskus paikallistetaan ja paikataan. Vasta kybermurron uhriksi joutuminen toimii usein herätyksenä (Sangani & Vijayakumar, 2012, 59).

Kaikki edellä mainittu yhdessä (potentiaalisten) puutteellisten kyberturvallisuusmetodien ja vanhentuneiden järjestelmien kanssa heikentää jo oletusarvoisesti heikoilla kantimilla olevaa tietoturvaa. Siksi ennaltaehkäisevällä toiminnalla on merkittävä rooli kyberturvallisuuden ylläpitämisessä, tämä pienyritysten olisi suotava tiedostaa.

3.6 Pienyrityksen riskit

Voisi olettaa, että mitä suurempi yritys, sitä suuremmat riskit. Tämä voi pitää paikkansa, mikäli ajatellaan puhtaasti taloudellisen menetyksen perspektiivistä. Suuremmalla organisaatiolla on luonnollisesti enemmän menetettävää, ja kyberuhkien vaikutukset ovat siksi suuret sekä yritykselle itselleen että sen yhteistyö- ja asiakasverkostoille. Toisaalta pieni organisaatio kamppailee samanlaisten kyberuhkien kanssa, ja tämä on potentiaalisesti pahemmassa pulassa jouduttuaan kyberrikollisuuden tai muun uhkan kohteeksi, sillä pieni organisaatio joutuu mahdollisesti käyttämään enemmän aikaa aiheutuneen vahingon korjaamiseksi. Ja aika on rahaa.

Lisäksi on organisaation koko millainen tahansa, se on aina altis kyberhyökkäyksille. Varsinkin kun kyberhyökkäykset ovat maailmalla jatkuvassa kasvussa ja niiden kyvykkyys ja uhkataso nousevat samaten (Saleem ym., 2017).

Jo aiemmin esille nostetut erot suurten ja pienten yritysten tavassa ja kyvyssä toteuttaa kyberturvallisuutta aiheuttavat potentiaalisia riskejä. Asiantuntemuksen ja resurssien puute johtavat pahimmillaan karkeisiin virheisiin kyberympäristöjen parissa ja luovat haavoittuvuuksia, joita hakkerit voivat hyödyntää (Parkin ym., 2016, 71). Pääoman puute estää tehokkaampien ja turvallisempien, ajantasaisten tietojärjestelmien käytön. Lisäksi virallisen, tehokkaasti valvotun kybersuunnitelman puute on itsessään merkittävä riskitekijä, joka altistaa pienyrityksen potentiaalisille väärinkäytöksille joko henkilökunnan tai ulkoisten tahojen toimesta.

Kyberrikollisuus, vakoilu ym. laaja-alaiset ja yleisesti tunnetut, jo aiemmin luetellut uhat kohdistuvat myös pienyrityksiin, eikä niitä käsitellä toistamieen tässä. Sen sijaan pienemmän näkyvyyden ongelmat, joita pienyrityksessä voi esiintyä mutta joita ei välttämättä noteerata, esitellään tarkemmin.

3.6.1 Vanhentunut teknologia

Monelle aktiivisesti IT:hen nojaavalle pienelle yritykselle tietojärjestelmien ja/tai digilaitteiden päivittäminen saattaa olla suhteettoman kallis menoerä. Tämä on merkittävä syy siihen, että näiden yritysten liiketoiminta, viestintä ym. työskentelylle olennaiset elementit nojaavat usein vanhentuneeseen teknologiaan. Tämä on äärimmäisen tärkeä riskitekijä, koska vanhat laitteet ja ohjelmat eivät sisällä ajan tasalla olevia turvakäytänteitä, tehden niistä selkeästi helpommin murrettavissa olevia (Hayes & Bodhani, 2013, 83). Tämä seikka jää usein helposti huomiotta, ja onkin ironista kuinka näin ilmiselvä riski olisi korjattavissa pienellä investoinnilla, johon pienyrityksellä ei yksinkertaisesti ole varaa.

3.6.2 Ilmaisten ohjelmistojen käyttö

Monet yrityksille kohdennetut tietokoneella käytettävät sovellukset ovat lisenssioikeuksilla tarjottavia ja maksullisia. Tällaiset rajatuilla käyttöoikeuksilla tarjottavat ohjelmistot epäävät loppukäyttäjältään mahdollisuudet muokata tai soveltaa tuotteen käyttöä muutoin kuin ennalta määriteltyjen ehtojen puitteissa. Vastineeksi organisaatio saa usein käyttöönsä vakaan ja kaupallisella tuella varustetun tuotteen. (Dhir & Dhir, 2017.) Kaikilla yrityksillä ei kuitenkaan ole välttämättä varaa tai halua maksaa kaupallisten ohjelmien käyttöön vaadittavaa summaa, varsinkin kun internet tarjoaa ilmaisia vaihtoehtoja esimerkiksi toimisto-ohjelmistojen osalta (Karjalainen, 2010). Monet näistä ilmaisista ohjelmista tai palveluista ovat tunnettuja avoimeen lähdekoodiin nojautuvia ohjelmistoja, joiden takana on joukko osaavia ammattilaisia ja joita päivitetään aktiivisesti. Joitakin tuotteita kehitetään erityisesti turvallisuus edellä. Esimerkiksi avoimeen lähdekoodiin perustuvien tietokoneiden käyttöjärjestelmien tapauksessa monet käyttäjät arvostavat näiden parempaa turvallisuutta ja ilmaista tuotetukea (Dhir & Dhir, 2017, 369).

Valitettavasti nämä huomiot eivät muuta sitä tosiseikkaa, että joidenkin ilmaisohjelmien laadunvalvonta voi jättää paljon toivomisen varaa. Käytännössä kuka tahansa voi laittaa internettiin levitykseen ohjelman, joka osoittautuu lopulta käytössä puutteelliseksi. Yrityksen kannalta vaaralliseksi tämä voi muodostua, mikäli sovellus pitää sisällään tietoisesti tai tiedostamatta auki jätetyn tietoturva-aukon, jota ulkopuoliset voivat hyväksikäyttää. (Maayan, 2019.) Tämän johdosta on hyvä selvittää, onko avoimen lähdekoodin omaavalla ohjelmalla takanaan aktiivinen päivityshistoria, joka osoittaisi, että mahdollisia ohjelman koodissa ilmeneviä valuvikoja korjataan säännöllisesti (Schryen, 2011). Lisäksi avoimen lähdekoodin ohjelmistojen käyttö voi kuluttaa pienyrityksen resursseja enemmän kuin maksullisten vaihtoehtojen käyttöönotto, mikä voi johtaa vaarallisiin virheisiin (Falkner & Hiebl, 2015, 130).

3.6.3 Työpaikan ulkopuolisten laitteiden käyttö

Siinä missä suuremmalla organisaatiolla omien laitteiden käyttöä voidaan valvoa ja erityisesti kieltää, ei pienyrityksellä ole välttämättä tällaista sääntöä. Työntekijän tuomat omat resurssit saatetaan päinvastoin nähdä vahvuutena tai esimerkillisenä toimintana, ja hyödyllisenä kustannuksia karsivana ratkaisuna (Olalere ym., 2015). Erityisesti yksityisyrittäjän voi uskoa käyttävän samaa tietokonetta sekä koti- että työkäyttöön (Bhattacharya, 2011, 301). Tämä on helposti ajateltuna vaivaton ratkaisu, ja ennen kaikkea säästää rahaa.

Kuten luvussa 2 on mainittu, moinen käytäntö tuo kuitenkin mukanaan riskejä. Ulkoiset laitteet voivat kantaa mukanaan haittaohjelmia omistajansa tietämättä, ja työpaikan verkkoon tai laitteisiin yhdistettynä voi altistaa koko työpaikan tietojärjestelmän viruksille. Henkilöstön tietokoneiden ja älylaitteiden käyttöä työn ulkopuolella ei juurikaan voida valvoa, ja varomaton verkkosurffailu saattaa helposti altistaa oman laitteen haittaohjelmille alttiiksi. (Kurpjuhn, 2015.)

3.6.4 Henkilökohtaisten asioiden hoitaminen työpaikalla

Laitteiden lisäksi henkilökohtaisten palvelujen, kuten oman sähköpostin käyttäminen työasioihin voi vaarantaa yrityksen toimintaa, varsinkin mikäli kyseisillä alustoilla käsitellään sensitiivistä tietoa. Uutiset sähköpostipalvelimien tietomurroista ovat vakava muistutus siitä, että kerralla miljoonien julkisten sähköpostin käyttäjien tiedot voivat helposti päätyä hakkereiden käsiin (Parkkari, 2017). Monet organisaatiot soveltavat tämän vuoksi niille luotuja omia domaineja työsähköpostin käyttöä varten, mutta erityisesti yksityisyrittäjät käyttävät ilmaisia sähköpostipalveluja, josta on vaikea päätellä, onko kyseessä pelkkä työsähköposti vai myös yksityiseen käyttöön tarkoitettu osoite.

Samaten esimerkiksi sosiaalisen median selaaminen työajalla ei välttämättä ole niin vaaratonta kuin voisi odottaa, varsinkin jos sen puitteissa tulee availtua levityksessä olevia epämääräisiä linkkejä tai tiedostoja. Tämä myös saattaa altistaa sosiaaliseen manipulointiin. (Thakur ym., 2019, 44.) Työpaikan turvallisuuden kannalta olisi parempi, jos sosiaalisessa mediassa leviävät uhat saataisiin edes eristettyä henkilökohtaisiin laitteisiin, mutta kuten edellä mainittu, omat laitteet voivat jo itsessään olla riskitekijä, varsinkin jos ne on kytketty osaksi työpaikan järjestelmiä. Tietenkin mikäli yrityksellä on toimintansa puolesta läsnäoloa sosiaalisessa mediassa, koskevat edellä kuvatut uhkatilanteet myös varsinaisia työpaikan laitteita, joilla kirjaudutaan sosiaalisen median palveluihin.

3.6.5 Kyberturvallisuussuunnitelman puute

Jos pienyritykseltä puuttuu seikkaperäinen turvallisuussuunnitelma ja toimintametodit kyberuhkien torjumiseksi, kaikkien tässä tutkimuksessa mainittujen riskitekijöiden mahdollisuus ja vaara kasvaa moninkertaisesti. Ilman suunni-

telmaa on harvoin olemassa toimivia edellytyksiä ja työkaluja tunnistaa uhkia ajoissa.

Erityisesti pienten organisaatioiden riskiksi tämä voidaan lukea siksi, että aiemmat tutkimukset osoittavat pk-yritysten usein ottavan varsin välinpitämättömän asenteen kyberturvallisuuteen kokonaisuudessaan (Fernandez de Arroyabe & Fernandez de Arroyabe, 2021, 4). Tämän myötä suunnitelmaa ei usein joko tehdä ollenkaan tai se tehdään ottamalla vain kaikkein välttämättömimmät ja/tai ilmeisimmät seikat huomioon.

3.6.6 Kyberturvallisuuden ulkoistaminen

Ulkoistaminen ei itsessään ole ongelmallinen konsepti yritykselle. Päin vastoin, omat rajansa tiedostava yritys hyötyy merkittävästi, mikäli onnistuu ulkoistamaan firman sisäisen osaamisen ylittävän tai liikaa rajallisia resursseja vievän toiminnan luotettavalle toimijalle

Ongelmaksi erityisesti kyberturvallisuuden ulkoistaminen muodostuu silloin, mikäli se vie yritykseltä kokonaan kontrollin omasta informaatioturvasta (Benz & Chatterjee, 2020, 532). Tällainen liiallinen luottamus IT-asiantuntijoihin kannustaa pahimmillaan passiivisuuteen ja yrityksen työntekijöiden oma tietämys aiheesta voi rapistua ajan myötä.

3.7 Riskienhallinta pienyrityksissä

Pienyritysten riskienhallinta saatetaan kokea kevyempänä prosessina muihin verrattuna. Pk-yritykset yleisesti voidaan nähdä suurempia firmoja ketterämpinä ja kykenevämpinä vastaamaan muutoksiin (Falkner & Hiebl, 2015, 122). Jo useasti esille nostettu pienyritysten resurssipula kyseenalaistaa kuitenkin tämän havainnon.

Kyberriskienhallinta pohjautuu käytännössä kaikissa olosuhteissa ja organisaatioissa samoihin periaatteisiin: riskien ennakointiin, aiheutuneen vahingon korjaamiseen ja virheistä oppimiseen (Eling ym., 2021). Pienyritysten on huomioitava samat seikat, vaikka mielikuvat uhkien puutteesta eläisivät vahvana.

Edellä esitellyissä riskienhallinnan prosesseissa pienyritykset joutuvat tekemään paljon valintoja haitallisempien ja vähemmän haitallisten riskien väliltä, mikä on luonnollista myös isommilla toimijoilla. Resurssien puute kuitenkin yksinkertaisesti estää monia pienempiä toimijoita tekemästä muuta kuin vähimmäistä riskien tunnistus- ja estämistyötä. Tämä yhdistettynä tietovajeeseen tekee tästä entistä hankalampaa. (Falkner & Hiebl, 2015.)

Pienyrityksien ollessa kyseessä ei voida aina turvautua erilliseen IT-asioista vastaavaan tiimiin, jonka tehtävänä olisi kyberympäristöihin liittyvien ongelmien nopea ratkaiseminen. Toisaalta tämän prosessin ulkoistaminen voi olla yritykselle liian kallista tai sitä ei tulla edes ajatelleeksi. Monet yritykset

luottavat paljon omaan osaamiseensa ja uhkien olemattomuuteen (Benz & Chatterjee, 2020).

Valveutunut ja osaava henkilökunta on täten edelleen olennainen osa toimivaa riskienhallintaa. Pienemmällä henkilökunnalla yhteisen ajattelutavan löytäminen ja kollektiivinen riskien tiedostaminen voi olla helpompaa, kun kaikki tuntevat toisensa varsin hyvin ja kommunikointi pienessä piirissä on potentiaalisesti sujuvampaa. Toisaalta luottamus siihen, että kaikki osaavat noudattaa sääntöjä, voi johtaa toiminnan valvonnan lepsuiluun.

4 TUTKIMUSMETODI

Tutkimuksen metodina käytetään laadulliseen tutkimukseen pohjautuvaa sisällönanalyysiä (Tuomi & Sarajärvi, 2018, 117). Aineiston keruu toteutetaan teemahaastattelun puitteissa, ja näitä haastattelujen tuloksia käytetään analyysin tekemiseen, verraten lukujen 2 ja 3 pohjustavan kirjallisuuskatsauksen havaintoihin. Laadullisessa analyysissa käytetään tässä yhteydessä induktiivista lähestymistapaa, haastattelujen tuloksia käytetään yleisten huomioiden tekemiseen (Tuomi & Sarajärvi, 2018, 107).

Tutkimuksen laadullisuus korostuu sen painotuksessa tutkittavan ilmiön (kyberturvallisuus mikrokokoisissa tilitoimistoissa) kokemuksien tarkasteluun. Kyberturvallisuuden, IT:n tai digitaalisuuden teknistä puolta ei tässä tulla käsittelemään sillä painopiste on nimenomaan ihmisten tuntemuksissa ja omakohtaisissa näkemyksissä. Tilastoja haastattelun tuloksista ei tehdä, vain litteroitu tiivistelmä (liite 1).

Tutkimuksessa on myös fenomenografisia piirteitä (Kettunen ym., 2021), sillä haastateltavien omia kokemuksia tullaan vertailemaan ja näistä haetaan sekä yhteneviä että poikkeavia tilanteita, joiden pohjalta tehdään havaintoja ja päätelmiä tilitoimistojen kyberturvallisuuskompetenssista. Pääpainopiste on kuitenkin sisällönanalyysissa

4.1 Tutkimukseen valitut tilitoimistot

Tutkimukseen haettiin mikrokokoisia (1-10 työntekijää) tilitoimistoja Keski-Suomen alueelta. Tilitoimistojen koko valittiin tutkimuksen varhaisessa suunnitteluvaiheessa, tutkimuksen intressinä ollessa pienten yritysten kyky vastata kyberturvallisuushaasteisiin. Haastateltavien yritysten rajaaminen juuri tälle alueelle sen sijaan tehtiin tutkimuksen ja haastattelujen toteuttamisen helpottamiseksi. Pääasiallisena tarkoituksena oli suorittaa haastattelut kasvotusten niin, että haastateltavat yritykset sijaitsevat riittävän lyhyen etäisyyden päässä Jyväskylästä

Tutkimukseen sopivien tilitoimistojen etsiminen toteutettiin selaamalla internetistä löytyviä yrityshakusivustoja, yritysrekistereitä ja/tai yritysten kotisivuja ja näiden antamien tietojen perusteella karsittiin yrityskooltaan liian suuret tilitoimistot. Myös tilitoimistot, joiden saattoi olettaa olevan osa suurempaa ketjua tai joiden taustalle toimii jokin emoyhtiö, jätettiin tutkimuksen ulkopuolelle. Mikrokokoisten yritysten kyberturvallisuuden tutkimisessa korostuu tässä tutkimuksessa näiden toimijoiden itsenäisyys ja kyky toimia omien rajallisempien resurssien puitteissa.

Soveliaiden tilitoimistojen omistajille, toimitusjohtajille tai viestintäasioista vastaaville henkilöille lähetettiin yhteydenottona kutsu tutkimukseen osallistumisesta. 40 yritystä vastaanotti kutsun, joista 9 yhdeksän lopulta suostui haastatteluun. Näille yrityksille lähetettiin tietosuojailmoitus/suostumuslomake, jolla määriteltiin rajat tutkimuksen skaalalle ja luottamuksellisen haastattelutiedon oikeaoppiselle käytölle sekä vahvistettiin tilitoimiston halukkuus osallistua haastatteluun. Tutkimukseen osallistuvien yritysten kanssa sovittiin ajankohta ja puitteet haastattelua varten. Samalla sovittiin kunkin yrityksen tapauksessa, kuka osallistuu haastatteluun. Haastateltavan henkilön täytyy olla joko vastuussa yrityksen tietoturvasta tai olla muuten hyvin perillä tilitoimiston kyberturvallisuustoimista. Tarkoituksena oli saada vastauksia heiltä, joilla on tutkimuksen aiheesta eniten tietoa kuten Tuomi & Sarajärvi kehottavat tekemään (2018, 98).

4.2 Haastattelupohja

Tutkimusta varten laadittiin mahdollisimman kattava mutta tiivis haastattelupohja kysymyksineen. Liian pitkää haastattelua ja liian useita kysymyksiä täytyi välttää, ettei tutkimukseen osallistuminen veisi liikaa aikaa tilitoimistojen omilta kiireiltä. Lisäksi suureen haastatteluun osallistuminen saattaa vaikuttaa liian raskaalta ja syödä mielenkiintoa, erityisesti puhelimitse suoritettuna. Haastattelun toteuttamisen laskettiin siksi vievän enimmillään noin puoli tuntia.

Kysymykset suunniteltiin hyvin pitkälti aiempien kyberturvallisuutta ja pk-yritysten toimintatapoja käsittelevien tutkimusten tarkastelun tuloksena. Myös tietoturvan kehittämiseen ohjeistavia oppaita käytettiin inspiraationa (Järvinen & Rousku, 2017). Kysymysten on tarkoitus avata kyberturvallisuutta yleisesti sekä teknisistä että käyttäjälähtöisistä näkökulmista. Aihepiirin ja kysymysten täytyy olla riittävän yksinkertaisia ja ymmärrettäviä, jotta IT:n loppukäyttäjän tasolla oleva henkilö kykenee hahmottamaan tiedusteltavia aiheita.

Haastattelun pääkysymyksiä on 32. Näistä lisäksi joidenkin pääkysymysten yhteydessä on 23 potentiaalisesti esitettävää tarkentavaa lisäkysymystä. Yhteensä haastattelussa esitettäviä kysymyksiä on siis 55.

4.3 Aineiston keruu

Haastattelut toteutettiin huhtikuun ja joulukuun 2020 välisenä aikana. Kesällä haastatteluja ei toteutettu yritysten mahdollisten lomien ja muiden järjestelyjen vuoksi.

Kutakin tilitoimistoa haastateltiin puhelimitse, ja näiden haastattelujen tulokset kirjattiin ylös ja litteroitiin. Haastatteluun osallistunut henkilö sai luettavakseen kysymykset ja antamansa vastaukset mahdollisia korjauksia ja tarkentavia lisäyksiä varten. Hyväksytyistä haastatteluvastauksista koostettiin dokumentti, joissa kaikkien tilitoimistojen vastaukset esitettyihin kysymyksiin on anonyymisti esitettynä. Vastauksia käsitellään ja analysoidaan luvussa 6.

5 TILITOIMISTOJEN HAASTATTELU

Tutkimuksen keskeisenä elementtinä toimii tilitoimistoille kohdistettu haastattelu, jolla kartoitetaan yritysten omia näkökulmia ja kokemuksia. Kuten edellä mainittu, haastattelu on muodoltaan avoin haastattelu. Tämä antaa vastaajille mahdollisuuden avata omia näkemyksiä ja kokemuksia.

5.1 Haastattelukysymykset

Tilitoimistoille esitettäviä päähaastattelukysymyksiä on yhteensä 32, joista osa sisältää tarkentavia lisäkysymyksiä (liite 1). Kukin niistä selvennetään tässä kappaleessa.

1) **Kuinka monta henkilöä työskentelee yrityksessänne?** Kysymyksen kannalta on olennaista selvittää, että haastateltava yritys on varmasti kooltaan mikrokokoinen (henkilöstökoko 1-10). Lisäksi vaihtelut yritysten henkilöstökoossa saattaa vaikuttaa siihen, kuinka yrityksissä kyberturvallisuutta käsitellään.

2) **Mikä on teidän (vastaajan) asema yrityksessä?** Lähtökohtana on, että tutkimusta varten haastatellaan yrityksessä tietoturvasta eniten ymmärtävää tahoa, joka osaa antaa selkeän ja oikean kuvan kyberturvallisuuden toteutumisesta yrityksen sisällä. Kysymyksellä pyritään tämän yhteydessä selvittämään, millaisessa roolissa tämä vastuuhenkilö on.

3) **Nojaako yrityksenne työnteko pääsääntöisesti tietokoneisiin ja digitaalisiin laitteisiin, ts. onko digitalisaatiolla ollut selkeä vaikutus yrityksenne toimintaan?** 2020-luvulla digitalisaatio ja riippuvuus tietokoneista sekä internetistä luovat puitteet aktiiviselle työskentelylle IT:n parissa. Tämä vuorostaan nostaa tarvetta kyberturvallisuuden tuntemukselle. Tilitoimistot käsittelevät paljon asiakasdataa, ja on siksi odotettavissa, että merkittävä

osa alan yrityksistä on omaksunut digitalisaation osaksi toimintamenetelmiään. Vaikka tämän uskoisi olevan varma oletus 2020-luvun Suomessa, tämä on syytä tarkistaa erillisen kysymyksen muodossa.

4) **Miten määrittelette termin ”kyberturvallisuus”?** Kysymys on tarkoituksenmukaisesti jätetty avoimeksi, jotta tutkimukseen saataisiin yksilökohtaisia tulkintoja kyberturvallisuudesta yleensä. Tässä peräänkuulutetaan vastaajan omaa näkemystä ja täten kompetenssia aiheesta, väärää vastausta ei ole olemassa, varsinkin kun kyberturvallisuus terminä on laaja ja mahdollisesti vaikeaselkoinen.

5) **Kuka yrityksessänne huolehtii tietoturvasta?** Kysymyksessä 2 selvitetään haastatteluun osallistuvan henkilön roolia, mutta tämä ei välttämättä merkitse samaa kuin tietoturvasta vastuun ottava taho. Siksi haastattelussa tiedustellaan erikseen, kuka tai mikä tämä vastuutaho on.

6) **Onko yrityksenne ulkoistanut IT-tuen tai tietoturvan toteutuksen jollekin ulkoiselle taholle?** Kuten aiemmissa tutkimuksissa on todettu, mikrokokoisen yrityksen resurssit ovat oletusarvoisesti rajalliset, ja esimerkiksi IT-tuki ja/tai tietoturva saatetaan tämän johdosta ulkoistaa (Benz & Chatterjee, 2020). Tämä ennakko-oletus on tärkeä selvittää ja mahdollisesti kumota, riippuen tutkimuksen tuloksista.

7) **Onko yrityksenne henkilökunnalla koulutusta tietoturvan saralla?** Kyberturvallisuuden/tietoturvan laajempi tuntemus ja ammattimainen soveltaminen ei välttämättä vaadi virallista koulutusta. Oletusarvoisesti monet yrittäjät opettelevat käytänteitä itse omien kokemustensa pohjalta. Alan koulutus auttaa kuitenkin ymmärtämään aihetta uusimpien tietojen valossa. Kysymyksellä selvitetään siis, onko kyberturvallisuuteen liittyvä tietotaito peräisin alan koulutuksesta.

    a) **Jos on, järjestetäänkö tämän tiimoilta säännöllistä jatkokoulutusta?** IT-alalla uutta tietoa syntyy jatkuvasti ja käytänteet päivittyvät sen mukaisesti. Mikäli tilitoimiston henkilökunnalla on kyberturvallisuutta koskeva koulutuspohja, on hyvä selvittää, ylläpidetäänkö tätä osaamista säännöllisellä jatkokoulutuksella.

8) **Onko yrityksenne ostanut tietojärjestelmiä, -ohjelmia ja/tai -palveluita (mukaan lukien lisenssit)?** Yritysten käyttämiä ohjelmistoja ja työkaluja myydään samalla tavoin kuin kuluttajille suunnattuja vastineita, joskin joitakin eroja sisällössä ja ominaisuuksissa voi ilmetä. Tutkimuksen kannalta kuitenkin on olennaisempaa selvittää käyttävätkö tilitoimistot näitä maksullisia sovelluksia ja palveluja. Maksullisilta sovellus- ja palveluntarjoajilta on odotettavissa jonkinasteista asiakaspalvelua, huoltoa ja tietoturvan ylläpitämistä, erityisesti isoilta ja/tai luotetuilta toimijoilta (Dhir & Dhir, 2017).

a) **Jos on, huolehtivatko näiden palveluiden tarjoajat ohjelmistojen tms. toiminnasta ja päivityksestä?** Luotettava IT-tuotteen kehittäjä jatkaa tuotteen kehitystä ja päivittämistä niin, ettei loppukäyttäjän tarvitse jäädä yksin ilmenevien ongelmien kanssa. Näin tietoturvaan liittyvät ominaisuudet pidetään myös ajan tasalla. Mikäli tämä ei toteudu, on potentiaalisen kyberriskin siemen olemassa.

b) **Käyttääkö yrityksenne ilmaisia vaihtoehtoja?** Internet on täynnä vaihtoehtoisia sovelluksia ja ohjelmia, jotka kilpailevat olemassa olevien maksullisten palvelujen kanssa. Tutkimuksen kannalta on tärkeää huomioida, ettei ilmainen ohjelma tarkoita automaattisesti haitallista, vaarallista tai verrokkituotteita huonompaa. Pikemminkin on nostettava esille se riski, että ilmainen tuote saattaa omata taustaltaan heikomman käyttäjätuen kehittäjän vähäisempien resurssien johdosta, ilmainen tuote on saatettu ladata epämääräisistä lähteistä, ohjelman kylkiäisinä saattaa tulla kolmannen osapuolen tartuttama haittaohjelma jne. Riittävä varovaisuus ja ymmärrys ilmaisten ohjelmistojen käyttöön liittyen auttaa välttämään pahimmat sudenkuopat, mutta tunnettuihin brändeihin tukeutuminen saattaa olla yrityksen toiminnan ja turvallisuuden kannalta helpompaa.

9) **Miten määrittelette termin ”tietoturvariski”?** Kuten kysymyksen 4 tapauksessa, tietoturvariskin määrittelyssä haetaan ensisijaisesti yksilökohtaista ymmärrystä kyberturvallisuuden käsitteistä ja ilmiöistä. Avoin kysymys antaa vastaajalle tilaa pohtia, mitä riski terminä erityisesti tietoturvan puitteissa pitää sisällään. Se, onko vastaus lähellä yleisesti hyväksyttyä määritelmää, on sitten osa haastattelujen tulosten arviointia.

10) **Onko yrityksellänne mielestänne ilmeisiä tietoturvariskejä, joihin pitäisi puuttua?** Yritysten annetaan itse pohtia, millaisia tietoturvaan liittyviä riskejä, jos yhtään, heidän toiminnassaan ilmenee. Tietoturvaongelmien kartoittamiseen voidaan tarvittaessa palkata ammattitaitoinen osaaja, joka selvittää potentiaaliset ongelmat yrityksen toiminnassa. On kuitenkin kyberturvallisuuden kannalta olennaista, että jokainen tietoverkkoihin aktiivisesti kytköksissä oleva toimija osaa havaita itse näitä toimintaa vaarantavia seikkoja. Virheiden huomioiminen ennakkoon auttaa ehkäisemään pahimman skenaarion toteutumisen.

11) **Onko yrityksellänne selkeätä tietoturvasuunnitelmaa?** Yrityksessä, jossa toimii useampi henkilö, toimintojen yhtenäistäminen ja yhteiset säännöt auttavat yhteisen liiketoiminnan organisoimisessa. Mikrokokoisella yrityksellä toimintasuunnitelmat saattavat tosin olla enemmän epävirallisia. Tietoturva, joka kattaa laajasti sekä yksittäisiä toimijoita että koko organisaation laajuisia ratkaisuja koskevat toimenpiteet, vaatii erityistä tarkkuutta. Siksi on hyvä selvittää, onko haastatelluilla tilitoimistoilla käytössä jonkin tasoista tietoturvasuunnitelmaa tai kyberstrategiaa.

a) **Jos on, milloin se on kehitetty, ja päivitättekö sitä säännöllisesti?** Jatkokysymyksellä selvitetään tietoturvasuunnitelman ajanmukaisuutta. Kuten aiemmissa yhteyksissä on todettu, kyberturvallisuuteen liittyvät teknologiat, uhat ja käytänteet uudistuvat tiuhaan, ja pysyäkseen perässä kyberturvallisuuden ammattilaiset päivittävät osaamistaan jatkuvasti. Ei-ammattimaisilta toimijoilta tällaista ei voine odottaa, mutta tietoturvasuunnitelman ajoittainen tarkastus on toimenpiteenä hyödyllinen, mikäli tällainen on aiemmin kehitetty.

b) **Jos ei, aiotteko kehittää sellaisen tulevaisuudessa?** Vaihtoehtoisesti, mikäli tietoturvasuunnitelman kehitys ei ole ollut tilitoimistolla aiemmin agendana, on tarpeen kysyä, mikäli tällainen on jatkon suhteen ajankohtaista.

12) **Onko yrityksenne toimintaa varten luotu suljettu yksityinen lähiverkko?** Avoimet verkot ovat huomattava tietoturvariski. Yleisissä tiloissa, kuten kahviloissa, avoimet verkot ovat yleisiä osana asiakkaiden palvelutarjontaa, mutta sensitiivistä dataa käsittelevien yritysten toiminnan kannalta ne tarjoaisivat hakkereille ihanteelliset puitteet vakoiluun tai tietomurtoihin. Salasanalla suojatut yksityiset verkot ovat selkeä ratkaisu tähän, ja siksi haastattelussa selvitetään ovatko tilitoimistot huomioineet tämän.

13) **Onko työpaikkanne verkkoon yhteydessä laitteita, joita ei käytetä työntekoon?** Yhteisessä verkossa olevia laitteita voi käyttää ketterään tiedonjakamiseen laitteiden välillä, mutta tässä on olemassa mahdollisuus, että yhteen laitteeseen iskostunut haittaohjelma voi helposti levitä muihin. Erityisesti IoT-teknologiaa (Internet of Things) hyödyntävät, huonosti suojatut laitteet toimivat helposti väylänä kyberhyökkäyksille (Abomhara & Køien, 2015). Vaikkei kyseessä olekaan mikään absoluuttinen ratkaisu, voi tällaista ongelmaa välttää työpaikalla liittämällä verkkoon vain laitteita, joita käytetään pääsääntöisesti työntekoon eikä nettisurffailuun potentiaalisine lieveilmiöineen. Tämä ei tietenkään sulje pois mahdollisuutta, että työpaikan laitteita käytetään kurinalaisen työnteon ohella yksityiseen käyttöön, ja tätä seikkaa käsitellään erikseen kysymyksessä 30.

14) **Kuinka usein päivitätte käytössänne olevia laitteita tai ohjelmia?** Pysyäkseen uusimpien tietotekniikan muutosten perässä, kehottavat IT-ohjelmistojen, -laitteiden ja -palvelujen kehittäjät ja valmistajat käyttäjiä päivittämään näitä säännöllisesti. Erityisesti tietoturvan kannalta on tärkeää, että kaikki tietoverkkoihin ja internettiin kytköksissä olevat laitteet ja ohjelmat päivittyvät tiheään, jotta potentiaaliset hakkeroinnille ja uusimmille viruksille alttiit väylät saadaan tukittua. Vaikka monet näistä palveluista suorittavatkin päivitykset automaattisesti, on tärkeää selvittää tilitoimistojen yleistä tiedostamista tähän aiheeseen.

15) **Käytättekö paljon ulkoisia (muisti)laitteita (puhelimet, ulkoiset USB-kiintolevyt jne.) tiedostojen siirtämisessä koneelta toiselle?** Tiedonsiirto laitteelta toiselle voi pitää sisällään potentiaalisia ongelmia, kuten aiemmassa yhteydessä on todettu (Kurpjuhn, 2015). Mikäli yhdestä koneesta on tiedostamatta siirretty muistilaitteeseen haittaohjelman korruptoima tiedosto, joka sitten siirtyy muistilaitteen myötä toiseen koneeseen, on haittaohjelma levinnyt jo kahteen koneeseen. Tilitoimistot käsittelevät paljon dataa, joten on oletettavaa, että tiedonsiirtoa tapahtuu aktiivisesti työn puitteissa. Siksi on hyvä selvittää, käytetäänkö tähän ulkoisia laitteita.

16) **Onko työpaikallanne käytössä webkameroita tai mikrofoneja?** Webkamerat ja mikrofonit ovat alttiita kaappauksille, sillä niillä voidaan pahimmassa tapauksessa käyttää tietokoneen tai yleisesti työpisteen ympäristön vakoiluun (Lehto ym., 2015, 79). Koska digitalisaation myötä etätyöskentely on yleistynyt ja sitä mukaa videopuhelut/-palaverit ovat tulleet osaksi (toimisto)työtä, on syytä selvittää, onko yrityksellä käytössä ko. laitteita.

    a) **Jos on, ovatko ne oletusarvoisesti toimintavalmiudessa?** Mikäli mikrofoni ja/tai webkamera suljetaan – ja varmimmassa tapauksessa irrotetaan kokonaan emolaitteesta – kun niitä ei käytetä, ei näitä voida käyttää vakoiluun. Moinen varotoimenpide on tehokas, mutta suurella todennäköisyydellä unohtuu helposti.

17) **Onko yrityksenne varautunut tilanteisiin, joissa ette pysty käyttämään tietojärjestelmiä tai Internetiä?** Ilman toimivaa tietoverkkoa monen yrityksen toiminta saattaisi halvaantua täysin, varsinkin mikäli se on ehdottoman riippuvainen internetistä ja IT-järjestelmistä. Tutkimuksen kannalta on järkevä selvittää, ovatko mikrokokoiset tilitoimistot varautuneet moisiin tilanteisiin, ja siten mahdollisesti saada viitettä siitä, kuinka tietoverkoista riippuvaista näiden liiketoiminta on.

    a) **Onko kyseisiä tilanteita tullut vastaan?** Jatkokysymyksellä pyritään saamaan käsitystä siitä, kuinka yleisiä edellä mainitun kaltaiset tilanteet ovat mikrokokoisten tilitoimistojen keskuudessa.

    b) **Jos vastaava tilanne on tapahtunut, kuinka kauan tilanteen korjaaminen keskimäärin vei?** Niille yrityksille, jotka ovat toimintansa osalta riippuvaisia tietojärjestelmistä, pitkä odotusaika toiminnan jatkamiselle voi osoittautua kalliiksi. Siksi tällaiset tilanteet on hyvä korjata mahdollisimman nopeasti. Vaikka mikrokokoiset tilitoimistot eivät välttämättä olisikaan kriittisellä tavalla riippuvaisia IT:stä, ongelmanratkaisun ketteryys on yksi kyberturvallisuuden perusasioista, jota on hyvä tutkia tässä yhteydessä.

18) **Onko yrityksenne varautunut laitteistoihinne kohdistuviin fyysisiin ongelmatilanteisiin, esim. hajoaminen tai varkaudet?** Odottamaton IT-

laitteen särkyminen tai varkaus osoittautuu helposti paljon suuremmaksi menetykseksi kuin mitä laitteen rahallinen arvo antaisi olettaa. Asiakasdataa on vaikea saada korvattua, ja varkauksien kohdalla seuraukset voivat olla kauaskantoisia, mikäli varas pääsee laitteessa oleviin tiedostoihin käsiksi ja kykenee väärinkäyttämään sitä. Näin ollen ennakkotoimet tällaisten tilanteiden ehkäisemiseksi ovat äärimmäisen tärkeitä.

a) **Onko yrityksenne tietojärjestelmistä ja tiedoista olemassa kattavat varmuuskopiot ja säännöllinen varmuuskopiointi?** Jatkona edelliseen kysymykseen, varmuuskopiointi on vähintä, mitä tiedostojen yllättävää katoamista vastaan voidaan tehdä. Säännöllinen varmuuskopiointi ja turvallinen varmuuskopioiden säilyttäminen varkauksien tai muun datan häviämisen varalta ovat siten tärkeitä toimenpiteitä kyberturvallisuuden kannalta, vaikkei tällä voidakaan vaikuttaa siihen mitä varastetulla datalla lopulta tehdään.

19) **Tekeekö yrityksenne henkilökunta usein töitä kotoa käsin?** Etätyöskentely on digitalisaation myötä yleistynyt huomattavasti. Tämä tarjoaa paljon toimivia puitteita yrittäjille, jotka hyödyntävät mielellään vapaa-aikaa tai työpaikan ulkopuolisia tiloja työntekoon, mutta tämän varjopuolena on aina olemassa pelko tietoturvan laiminlyönnistä turvalliseksi koetussa kotiympäristössä.

a) **Jos tekee, miten työntekijät huolehtivat tietoturvan ylläpitämisestä työpaikan ulkopuolella?** Jatkokysymyksellä selvitetään, onko mahdolliselle etätyöskentelylle taattu tietoturvan kannalta sopivia puitteita.

b) **Onko kotona työskentelyä varten olemassa oma tietoturvasuunnitelma?** Aiemmassa yhteydessä on korostettu tietoturvasuunnitelman hyödyllisyyttä erityisesti yritystoiminnassa ja sitä, kuinka sellaisen järjestäminen parhaimmillaan tehostaa kyberturvallisuuden ylläpitämistä. Luonnollisesti etätyöskentelypiste voi olla työnteon kannalta erilainen ympäristö kuin työpaikan toimisto, ja siten asettaa erilaiset tarpeet toimintasuunnitelman kannalta.

c) **Onko työntekijöillä käytössä kattava tietoturvajärjestelmäpaketti kotona?** Yrityksen tietoturvan peruspilarina saattaa olla vahva, koko organisaation kattava tietoturvajärjestelmä, joka suojaa kaikkia yrityksen laitteita. Se, onko vastaavan tasoinen järjestely käytössä myös työntekijöiden kotona vai ovatko työpaikan ulkopuolella käytettävät laitteet tältä osin alttiimpia mahdollisille kyberrikoksille tai häiriöille, on tärkeätä selvittää.

20) **Teettekö tärkeitä/luottamuksellisia työtehtäviä mobiililaitteilla?** Mobiililaitteet, kuten älypuhelimet, ovat tänä päivänä niin tehokkaita että niillä pystytään suorittamaan monia samoja työtehtäviä kuin työpaikan pöytäko-

neilla, kunhan vain sopiva ohjelma löytyy. Mobiililaitteiden kyberturvallisuus on kuitenkin oma lukunsa koko yrityksen tietoturvasuunnitelmaa silmällä pitäen, ja mobiililaitteiden tietoturvallisuuden luotettavuus on edelleen tietynlainen kysymysmerkki, varsinkin kun osa laitteista ei omaa minkäänlaista virustorjuntaa.

21) **Miten toimitte fyysisen tiedostomateriaalin (esim. tulosteet) tietoturvan kanssa? Arkistointi, säilytys, luottamuksellisuuden takaaminen?** Vaikka digitalisaatio on johtanut väistämättä siihen, että valtaosa maailmalla käsiteltävästä tärkeästä datasta on digitaalisessa muodossa, on fyysinen tiedostomateriaali monille yrityksille tuttu ja edelleen käytössä oleva tallennemuoto. Fyysinen materiaali esimerkiksi tulosteiden muodossa asettaa kuitenkin omanlaiset haasteensa, kuten tulipalon tai varkauksien suhteen. Siksi on tärkeää, että näiden tietojen turvaaminen on myös tärkeä prioriteetti yritykselle, joka arkistoi dataa fyysisesti. Yritysten hallinnoima data on kuitenkin arvokasta, huolimatta siitä missä muodossa sitä säilytetään.

22) **Miten yrityksenne hävittää tarpeettoman mutta arkaluontoisen/salassa pidettävän materiaalin?** Yrityksen toiminnassa syntyy paljon joko yrityksen omaa toimintaa käsittelevää tai asiakkaiden tietoja sisältävää dataa, ja ajan myötä osa tästä datasta osoittautuu tarpeettomaksi arkistoinnin kannalta. Tällöin näistä dokumenteista hankkiudutaan tavalla tai toisella eroon, joko tilan luomiseksi tai näiden tietojen vääriin käsiin päätymisen estämiseksi. Vanhentunut datakin voi nimittäin sisältää hakkereille arvokkaita tiedonmurusia, joita käyttää rikollisia tarkoitusperiä varten. Jopa yritysten roskalaatikoiden tonkimisella saatetaan löytää sosiaalista manipulointia edistävää tietoa yrityksestä ja sen työntekijöistä (Koyun, & Al Janabi, 2017). Siksi tällaisen materiaalin oikeaoppinen ja turvallinen hävittäminen on erittäin tärkeää.

    a) **Entä vanhat ja tarpeettomat laitteet?** IT-laitteisiin, erityisesti tallennustilaa sisältäviin, pätevät samat käytänteet kuin digitaaliseen tai fyysiseen tiedostomateriaaliin. Mikäli vanhasta ja/tai tarpeettomaksi käyneestä laitteesta halutaan hankkiutua eroon, on se syytä hävittää tehokkaasti ja tietoturvallisesti. Vanhoihin kiintolevyihin ja muistitikkuihin voi helposti unohtua jotain arvokastakin dataa, mikäli näitä ei puhdisteta asianmukaisesti.

23) **Onko työntekijöillänne yhtäläiset oikeudet kaikkiin tietojärjestelmänne tietoihin?** Suuremmissa yrityksissä vallitsee suurella todennäköisyydellä tarkasti määritellyt roolit, mitkä määräytyvät työtehtävien ja/tai työntekijän hierarkkisen aseman mukaan. Näille rooleille saatetaan asettaa rajoitteita tiedonpääsyn suhteen, eli eri työtehtävissä olevat eivät pääse käsiksi sellaisiin tietoihin, mitkä eivät koske kyseisen työntekijän tehtäviä. Näin ehkäistään mahdollisia väärinkäytöksiä tai tahattomia tiedonkäsittelyn virheitä, ja ongelman ilmetessä voidaan helpommin paikantaa kyberturvallisuu-

den vuotokohta. Mikroyrityksillä, joiden työntekijöiden lukumäärä on laskettavissa kahden käden sormin ja työtehtävät ja roolit saattavat sekoittua paljonkin, tällainen käytäntö ei välttämättä ole itsestäänselvyys.

24) **Miten työntekijänne suojaavat salasanoja ja käyttäjätietojaan?** Salasanojen suojaaminen väärinkäytöksiltä on ehdottoman tärkeä toimenpide kyberturvallisuuden kannalta. Mikäli kirjautumistiedot päätyvät vääriin käsiin, on tilannetta vaikea korjata ennen kuin vahinko on jo ehtinyt tapahtua. Se, millaisin keinoin tätä suojausta edesautetaan, on varsin yksilökohtaista, mutta tämän asian selvittäminen antaa hyvän kuvan kyberturvallisuuden yleisestä tasosta. Mikäli kaikkein ilmeisimpiin tietoturvaseikkoihin suhtaudutaan lepsusti, saattaa se johtaa siihen, että muutkin tietoturvakäytänteet kärsivät.

    a) **Onko yrityksessänne käyttäjätunnukset tai salasanat jossain fyysisesti näkyvillä?** Salasanojen tai muiden käyttäjä-/kirjautumistietojen säilyttäminen näkyvästi esillä toimistoympäristössä on yksi räikeimmistä virheistä, mitä IT:n käyttäjä voi tehdä. Tästä huolimatta tämä on valitettavan yleinen tapa, jota perustellaan esim. vaivattomuudella tai salasanojen helpolla unohtamisella. Toimistossa käyvät työpaikan ulkopuoliset henkilöt ja kaapattujen webkameroiden kautta toimivat hakkerit voivat helposti noteerata esillä olevat kirjautumistiedot ja väärinkäyttää niitä. Siksi on toivottavaa, että tällaista käytäntöä ei esiinny tilitoimistojen kaltaisissa ympäristöissä, joissa salassa pidettävää tietoa käsitellään usein.

    b) **Kuinka usein päivitätte salasanoja?** Mitä tiheämmin palvelujen ja käyttäjätunnusten salasanoja päivitetään, sitä pienempi on todennäköisyys, että niitä ehditään hakkeroimaan. Siksi aktiivinen salasanojen uusiminen – ja tietenkin mahdollisimman monimutkaisten salasanojen käyttö – on osa tehokasta tietoturvaa. Näin myös vältytään tuudittautumasta valheelliseen turvallisuuden tunteeseen, mihin passiivisuus tämän johdosta helposti johtaa.

25) **Onko yrityksenne käytössä pilvipalveluita?** Pilvipalvelut ovat mullistaneet sovellustoiminnan sekä tiedonjakamisen ja -tallentamisen konseptin IT:n puolella, monien toimintojen siirtyessä suoraan internettiin. Siksi monet yritykset ovat omaksuneet ne osaksi liiketoimintaansa, jollei muuten niin tiedon tallentamisen muodossa.

    a) **Jos on, miten huolehditte näiden tietoturvasta?** Pilvipalvelut ovat alttiita kyberuhkille, luonnollisesti siksi että koko konseptin toiminta on sidoksissa internettiin. Pilvipalveluissa sijaitseviin tiedostoihin pääsee teoriassa ulkopuolinenkin käsiksi, mutta nämä ovat lähtökohtaisesti salasanojen tai muiden salauskeinojen takana suojassa. Se, ovatko tilitoi-

mistot itse aktiivisia osapuolia pilvipalveluiden tietoturvan ylläpitämisessä, on hyvä selvittää.

26) **Turvaudutteko tietojenkäsittelyssä ulkopuolisiin toimijoihin?** Mitä enemmän yrityksen liiketoiminnan piirissä on tekijöitä, sitä vaikeampaa on kontrolloida sitä, miten tieto liikkuu yrityksen sisällä. Erityisen haastavaksi tilanne voi teoriassa muodostua, mikäli yritys ulkoistaa jonkin tiedonkäsittelyn aspektin, esimerkiksi kirjanpidon, jollekulle muulle. Näin syntyy helposti tiedonvälityksen ketjussa saumakohta, johon kyberrikolliset voivat iskeä.

27) **Onko yrityksellänne kotisivuja?** Kotisivut ovat nykypäivänä helppo tapa saada yritykselle näkyvyyttä. Nämä ovat myös ilmeisiä julkisia kohteita kyberhyökkäyksille, joten on tärkeätä selvittää, onko tilitoimistoilla näitä käytössä.

    a) **Jos on, annatteko julkaista sivustollanne mainoksia?** Verkkosivuilla olevat mainokset ovat kyberrikollisille otollinen keino aiheuttaa uhreilleen harmia. Huomiota herättävät kuvat tai videot, jotka mainostavat jotain houkuttelevaa tarjousta tms. saattavat houkutella pahaaavistamattoman internetin selaajan klikkaamaan tätä ja siten avata linkin tietoja kalastelevalle sivustolle tai laukaista selaimen kautta tarttuvan viruksen (Zarras ym., 2014). Vaikka sivustolla ei olisikaan käytössä mainoksia, saattavat haittaohjelmat silti lisätä näitä omin päin. Tällöin outojen mainosten ilmestyminen kotisivuille on selkeä merkki siitä, että jokin on pielessä.

    b) **Milloin olette viimeksi päivittäneet kotisivunne?** Kun kotisivuja päivitetään harvakseltaan, vallitsee mahdollisuus, että sivustolle jää vanhentunutta infoa, joka saattaa hämätä sivustolla kävijöitä. Kyberturvallisuuden kannalta ongelmaksi muodostuvat sivustolle pesiytyvät haittaohjelmat, jotka esimerkiksi edellä mainittujen valheellisten tai kaapattujen mainosten avulla aiheuttavat vahinkoa. Sivuston säännöllinen tarkistus ja päivitys pitävät huolen, että moiset tilanteet saadaan parhaimmillaan ehkäistyä.

    c) **Onko sivustollanne paljon linkkejä ja/tai yhteystietoja, joita voi kopioida?** Kotisivuilla olevat linkit ja yhteystiedot voivat olla tarpeellisia yrityksen tiedonvälitykselle, mutta myös hakkerit hyötyvät tästä varsin viattoman oloisesta seikasta. Esimerkiksi sähköpostiosoitteet ovat kysyttyä materiaalia roskapostia lähettäville tahoille, jotka poimivat niitä kaikkialta mistä pystyvät, linkkejä voidaan muokata ohjaamaan klikkaajansa vääriin osoitteisiin, ja henkilötiedot, osoitteet ja puhelinnumerot saattavat päätyä vääriin käsiin. Tietenkin yrityksen toiminnan kannalta olisi houkkamaista jättää kaikki yhteystiedot ja linkit kokonaan

pois sivustolta, mutta näiden pitäminen minimissään ehkäisee pahinta väärinkäyttöä.

d) **Onko domaininne tarjoaja maksullinen toimija vai ilmaisen verkkotunnuksen tarjoava taho?** Kysymyksen ei ole tarkoitus johdatella ajattelemaan, että kaikki ilmaisia web-domaineja (verkkotunnuksia) tarjoavat tahot olisivat epäluotettavia. Toisaalta servereiden vuokraamisessa pätee samat ohjenuorat kuin internetin tarjontaa yleisesti tarkasteltaessa: jos jokin on ilmaista tai vaikuttaa lähtökohtaisesti liian hyvältä ollakseen totta, sen takana saattaa olla jotain hämäräperäistä. Terve skeptisyys on siis valttia tässäkin. Vähemmän vaaralliset erot näkynevät ilmaispalveluissa esimerkiksi serverin tallennustilan määrässä ja rajallisemmassa palvelutasossa. Kun henkilö tai yritys maksaa kotisivuilleen varatusta domainista, on syytä odottaa vastineeksi luotettavuutta, tehokasta suojausta ja nopeaa palvelua vikatilanteiden sattuessa.

28) **Saatteko sähköpostin kautta usein roskapostia?** Mikäli sähköposti täyttyy roskapostista, on se merkki siitä, että sähköpostiosoite on päätynyt massapostia lähettävien tahojen – ja mahdollisesti hakkereiden – käsiin. Vaikka tähän ei olisikaan mitään muuta tehtävissä kuin olla avaamatta näitä ja antaa roskapostinsuodattimien tehdä tehtävänsä, tai vaihtaa sähköpostiosoite uuteen, tämä on selkeä muistutus siitä kuinka alttiita sähköpostiosoitteet ovat väärinkäytöille.

29) **Toimiiko yrityksenne aktiivisesti sosiaalisessa mediassa?** Nykypäivänä sosiaalinen media tarjoaa paljon kanavia viestintään ja markkinoimiseen, ja monet yritykset hyödyntävät tätä kehitystä. Some tarjoaa myös huijareille täydellisen alustan tavoittaa lukemattomia ihmisiä, ja yrityksetkin ovat heille otollinen kohderyhmä. Erityisesti sosiaalinen manipulointi hyötyy somen arkipäiväistymisestä (Albladi & Weir, 2018). Näin ollen sosiaalisessa mediassa toimiminen kysyy varovaisuutta tilitoimistoilta.

30) **Käytättekö työpaikkanne laitteita muuhun kuin työntekoon, esim. yksityisten asioiden hoitamiseen?** Aiemmassa yhteydessä on mainittu työpaikan verkkoon yhdistetyt laitteet, joita ei käytetä työntekoon. Selvittämisen arvoinen seikka on myös tietokoneiden yms. töiden kannalta olennaisten laitteiden käyttäminen huvitteluun tai yksityisten asioiden hoitamiseen. Näissä yhteyksissä on aina olemassa vaara, että laitteisiin saattaa surffailun jäljiltä jäädä haittaohjelmia, kevyistä seurantaevästeistä potentiaalisiin lamauttaviin viruksiin. Työpaikan koskemattomuuden kannalta on järkevää eristää tällaiset uhat henkilökohtaisiin laitteisiin ja pitää ne erossa työpaikan verkoista ja laitteista.

31) **Minkä miellätte tällä hetkellä tärkeimmäksi digitalisaation aiheuttamaksi uhkatekijäksi?** Avoimen kysymyksen tarkoitus on selvittää tilitoimistojen yleistä käsityskykyä kyberuhkista, ja saada miettimään merkittävimpiä

uhkatekijöitä toivon mukaan edellisten kysymysten innostamana. Tämän perusteella on hyvä käsitellä alati kasvavaa digitalisaatiota kriittisestä näkökulmasta. Koska kyberturvallisuus lähtee ensisijaisesti ihmisistä, on siksi tärkeätä, että yleinen tietoisuus aiheesta ja aiheen pohtiminen oman toiminnan viitekehyksestä nousee keskiöön.

32) **Onko yrityksenne joutunut kyberrikollisuuden tai hakkeroinnin kohteeksi?** Tämän ja jatkokysymysten avulla selvitetään tilitoimistojen omakotaisia kokemuksia kyberuhkista. Mikäli moisia kokemuksia ei ole yrityksellä tullut vastaan, on heillä ollut joko tuuria tai tietoturva-asiat jokseenkin hyvällä mallilla – tai sitten kyberhyökkäykset ovat jääneet kokonaan pimentoon, mutta ilman havaittavia menetyksiä. Yhtä kaikki kokemukset ovat toivottavasti johtaneet siihen, että kyberturvallisuusseikkoja ollaan tapahtuneen johdosta arvioitu uudelleen.

   a) **Mihin isku(t) on kohdistunut?** Mikäli kyberhyökkäyksistä on yrityksellä jonkinlaista havainnoivaa kokemusta, täytyy seuraavaksi selvittää mihin nämä aiemmat iskut ovat kohdistuneet. Mikäli näissä ilmenee paljon toistuvuutta, kertoo se mahdollisesta yleisestä tietoturva-aukosta mikrokokoisten tilitoimistojen keskuudessa.

   b) **Koitteko taloudellisia tappioita tämän/näiden takia?** Kaikki kyberhyökkäykset eivät johda suoraan taloudelliseen menetykseen, mutta tällaiset tapaukset jäävät luonnollisesti parhaiten muistiin. Jälkimmäisissä tilanteissa tietoturvan aukot ovat olleet sen verran merkittäviä, että yrityksen toiminta on selkeästi kärsinyt. Vastavuoroisesti taloudellisten tappioiden puute saattaa kertoa siitä, että tilanteeseen on reagoitu nopeasti, tai sitten arvokkaat tiedot ovat olleet hakkereiden tavoittamattomissa.

   c) **Miten ratkaisitte hakkeroinnin aiheuttamat ongelmat?** Erilaisiin kyberhyökkäyksiin reagoidaan eri tavalla riippuen luonnollisesti uhrin käytössä olevasta tietotaidosta ja/tai resursseista. On tutkimuksen kannalta mielenkiintoista selvittää, millä keinoin näitä potentiaalisia ongelmia on lähdetty ratkomaan, tämä kun kertoo paljon haastateltavien yritysten keinoista ja kyberturvallisuuskompetenssista.

6 HAASTATTELUJEN TULOKSET JA ARVIOINTI

Tässä luvussa tarkastellaan haastattelujen tuloksia. Haastatteluissa esitettyihin kysymyksiin annetut vastaukset puidaan tiivistetysti, ja näiden pohjalta pyritään luomaan yleinen kuva mikrokokoisten tilitoimistojen kyberturvallisuuskompetenssista.

6.1 Vastaukset haastattelukysymyksiin

Haastattelujen tuloksia käsitellään tässä kysymys kerrallaan. Eriäviä vastauksia vertaillaan keskenään ja vastauksia analysoidaan yleisesti aiemmissa luvuissa esitettyjen havaintojen pohjalta. Kaikki vastaukset haastattelukysymyksineen ovat luettavissa liitteestä 1.

1) **Kuinka monta henkilöä työskentelee yrityksessänne?** Haastateltujen tilitoimistojen henkilöstön koko vaihtelee 2-7 työntekijän välillä. Kolme vastaajayrityksistä on 2 hengen, viisi 4 tai 5 hengen, ja yksi 7 hengen yrityksiä. Lisäksi kaksi näistä yrityksistä ilmoittaa henkilöstönsä koostuvan osittain osa-aikaisista työntekijöistä tai harjoittelijoista. Kaikki tutkimukseen osallistuneet tilitoimistot siis ovat mikrokokoisia, kuten tutkimus vaatii.

2) **Mikä on teidän (vastaajan) asema yrityksessä?** Neljä haastatteluun vastannutta kertoo asemakseen toimitusjohtaja, loput viisi haastateltavaa yrittäjä tai omistaja. Haastatteluun osallistui siis selvästi johtavassa asemassa olevia henkilöitä, joilla oletettavasti on kokonaisvaltainen käsitys yrityksensä toiminnasta sekä lopullinen päätösvalta tietoturvan toteuttamisesta.

3) **Nojaako yrityksenne työnteko pääsääntöisesti tietokoneisiin ja digitaalisiin laitteisiin ts. onko digitalisaatiolla ollut selkeä vaikutus yrityksenne toimintaan?** Kaikki tutkimukseen osallistuneet yritykset kertovat digitalisaation vaikuttaneen toimintaansa merkittävällä tavalla. Tämä ei varsinaisesti yllätä: kuten jo aiemmissa luvuissa on korostettu, digitalisaatio on tehnyt tiedonkäsittelystä ketterämpää, joten tilitoimistoille on hyvin luontaista

joko siirtyä kokonaan digitaaliseen työskentelyyn tai ottaa IT:n tuomat hyödyt osaksi liiketoimintaansa.

4) **Miten määrittelette termin ”kyberturvallisuus”?** Yhdeksältä vastaajalta saatiin hyvin erilaisia tulkintoja kyberturvallisuus-termin määrittelemiseksi. Vastauksissa toistuivat erilaiset keinot ja termit kuten ”yleinen tietoturva” tai ”tietoturvaan liittyvät seikat”, IT:n puitteissa toteutuva suojaus/turvallisuus, virustorjunta/palomuurit ja digitaalisen tiedon turvallisuuden takaaminen. Toisaalta erilaisia uhkia lueteltiin kuten ”tietokoneiden ja internetin kautta tulevat uhat”, verkkohuijaukset ja laitteiden hajoamiseen liittyvät tekijät. Kaikki ovat tavalla tai toisella osa kyberturvallisuuden käsitettä, joten ymmärrystä aiheesta kyllä löytyy.

5) **Kuka yrityksessänne huolehtii tietoturvasta?** Ehdoton enemmistö (8) vastaajista ilmoitti ottavansa henkilökohtaisen (pää)vastuun tietoturvan järjestämisestä. Tarkentavasti muutama vastaaja kertoi delegoivansa osan toiminnasta IT-tuelle tai ohjelmistojen tarjoajalle. Näistä yksi vastaaja ilmoittaa tukeutuvansa ammattilaisiin täysimääräisesti. Yksi vastaajista kertoo kaikkien yrityksen työntekijöiden ottavan vastuun tietoturvasta, mutta lopulta yrittäjä itse toimii edelleen vastuuhenkilönä. Vastauksissa siis toistuu yhtenäinen teema: yrityksen johtohenkilö (yrittäjä/omistaja/toimitusjohtaja) huolehtii pääsääntöisesti tietoturvasta, saaden siihen tukea joko muilta työntekijöiltä tai IT-alan ammattilaisilta. Tämä on jokseenkin odotettava asetelma mikrokokoiselta yritykseltä.

6) **Onko yrityksenne ulkoistanut IT-tuen tai tietoturvan toteutuksen jollekin ulkoiselle taholle?** IT-tuen ja/tai tietoturvan toteutuksen ulkoistaminen vaikuttaa haastattelujen perusteella olevan yleinen käytäntö. Kahdeksan vastaajaa yhdeksästä ilmoittaa ulkoistamistoimenpiteistä ainakin jossain muodossa, yleisimpinä toistuvina tahoina mainitaan atk-alan yritys/atk-tukihenkilö (2 vastausta) tai maksullinen virustorjuntapalvelu (2 vastausta). Kaksi haastateltavista turvautuu kertomansa mukaan ulkoiseen apuun ongelmatilanteesta riippuen, värväten tilanteeseen sopivan ammattilaisen avuksi. Yksi vastaajista avaa vastaustaan tarkemmin kertomalla maksullisen virustorjunnan lisäksi verkkosivujen ulkoistamisesta mainostoimistolle, operaattorin vastuusta sähköpostin tietoturvassa ja pilvipalvelujen käytöstä ohjelmien tallennustilana. Vain yksi haastattelija ilmoittaa, ettei ulkoista näitä tehtäviä. Vastaukset antavat selkeää viitettä siitä, että mikrokokoiselle tilitoimistolle on luontevaa turvautua teknisen tuen suhteen ulkoiseen apuun.

7) **Onko yrityksenne henkilökunnalla koulutusta tietoturvan saralla?** Vain yksi haastateltavista kertoo yrityksensä omaavan jonkinlaista peruskoulutusta tietoturvaan liittyen, mutta mitään erityisosaamista ei henkilöstöltä löydy. Tämä tukee yleistä ja edellisen kysymyksen yhteydessä noussutta käsitystä, että kyberturvallisuuden tekniset seikat ulkoistetaan helposti ul-

koisille ammattilaisille. Jonkinlaista ymmärrystä aiheesta kuitenkin vaikuttaa olevan, kahden haastateltavan ilmoitettua, että yrityksen sisällä käydään keskusteluja tietoturvasta. Yksi vastaajista kertoo perehdyttävänsä muut työntekijät yleisiin käytänteisiin, mutta tämän suhteen on hankala tehdä johtopäätöstä, onko toimitusjohtajalla itsellään runsasta kokemusta vai yleistä ymmärrystä tietoturvan perusteista.

a) **Jos on, järjestetäänkö tämän tiimoilta säännöllistä jatkokoulutusta?** Yllä esitetyt vastaukset osoittavat myös jatkokysymyksen suhteen, ettei säännöllistä jatkokoulutusta tietoturvaan liittyen järjestetä, kun spesifi pohjakoulutus puuttuu. Tutkimuksen kannalta tämä on varsin selkeä osoitus yleisen kyberturvallisuuden koulutustason puutteesta.

8) **Onko yrityksenne ostanut tietojärjestelmiä, -ohjelmia ja/tai -palveluita (lisenssit)?** Kaikki tutkimukseen osallistuneet yritykset käyttävät omien sanojensa mukaan maksullisia järjestelmiä, ohjelmia tai palveluita IT:n parissa. Tämä on sikäli positiivinen osoitus siitä, että tilitoimistot tukeutuvat oletettavasti tunnettuihin ohjelmisto- tai palvelutarjoajiin, joilta on syytä odottaa tehokkuutta ja aktiivista asiakastukea.

a) **Jos on, huolehtivatko näiden palveluiden tarjoajat ohjelmistojen tms. toiminnasta ja päivityksestä?** Kaikki haastateltavat kertovat jatkokysymyksen yhteydessä näiden palvelujen tarjoajien huolehtivan kyseisten ohjelmistojen ja palvelujen toiminnasta ja uusimmista päivityksistä.

b) **Käyttääkö yrityksenne ilmaisia vaihtoehtoja?** Toisaalta kaksi yrityksistä vastasi tähän jatkokysymykseen käyttävänsä myös ilmaisia vaihtoehtoja yritystoiminnassaan. Tämä ei varsinaisesti kerro siitä, muodostaako ilmaisten sovellusten tai ohjelmien käyttö itsessään minkäänlaista kyberuhkaa haastatelluille yrityksille: lähinnä tämän perusteella voidaan päätellä, että näitä käytetään lisenssiohjelmien rinnalla.

9) **Miten määrittelette termin ”tietoturvariski”?** Tähänkin avoimeen kysymykseen haastateltavat antoivat jokseenkin vaihtelevia vastauksia. Useilla toistui kantavana teemana uhka (suojaamattomien) henkilötietojen tai arkaluontoisten/käsiteltävien tietojen päätymisestä ulkopuolisten käsiin, kaikki oivia vastauksia. ”Tietoturvan heikko taso yleisesti” ja ”heikko lenkki tietoturvassa” ovat myös lyhyitä mutta täsmällisiä vastauksia. Toisaalta kysymystä lähestyttiin myös ratkaisukeskeisin ilmaisuin ”varmistutaan että tieto käsitellään oikein” ja ”hahmotetaan salassa pidettävät tiedot, ja miten tietoa voidaan jakaa ja säilyttää turvallisesti”, jotka kuulostavat enemminkin riskienhallinnan määritelmältä mutta ovat sikäli kyllä päteviä vastauksia.

10) **Onko yrityksellänne mielestänne ilmeisiä tietoturvariskejä, joihin pitäisi puuttua?** Haastateltavat tilitoimistot vaikuttavat jakautuvan vahvasti sen osalta, miten ne hahmottavat omassa liiketoiminnassaan ilmeneviä riskejä.

Viisi vastaajaa kertoo, ettei heillä ole havaittu ilmeisiä tietoturvariskejä. Tämä kuulostaa lähtökohtaisesti hyvältä, mutta tämän perusteella ei voi päätellä, johtuuko tietoturvariskien puute hyvästä yleistilanteesta vai siitä ettei riskejä osata hahmottaa. Jälkimmäinen vaihtoehto on jo itsessään potentiaalinen riski. Loput neljä vastaajaa sen sijaan nostavat esille salasanojen suojauksen tai toistuvan käytön, fyysisen/digitaalisen murtautumisen yrityksen tietoihin sekä henkilöstön oman valppauden.

11) **Onko yrityksellänne selkeätä tietoturvasuunnitelmaa?** Vain kaksi haastateltavaa ilmoittaa tilitoimistonsa omaavan tietoturvasuunnitelman. Näistä yksi avaa tarkemmin yrityksen toteuttamia prosesseja: yrityksen toiminnasta poikkeavat tapahtumat kirjataan ylös, työtehtävät suoritetaan muilla kuin henkilökohtaisilla laitteilla, ja arkaluontoista tietoa välitetään vain suojatuilla yhteyksillä ja metodeilla. Nämä ovat hyviä esimerkkejä tietoturvasuunnitelman toteuttamisesta, mutta on valitettavaa, ettei tämä ilmiö toistu valtaosalla haastatelluista. Loput seitsemän eivät kertomansa mukaan ylläpidä tietoturvasuunnitelmaa.

    a) **Jos on, milloin se on kehitetty, ja päivitättekö sitä säännöllisesti?** Edellä mainitut kaksi haastateltavaa kertovat tietoturvasuunnitelmansa kehittämisestä ja päivityksestä: toinen tilitoimistoista on omaksunut suunnitelmansa alle kaksi vuotta sitten (haastattelun toteutusajankohdasta), mutta ei päivitä sitä säännöllisesti. Toinen taas ilmoittaa kehittäneensä suunnitelman ”parin viime kuukauden sisällä”, ja suunnitelmaa päivitetään säännöllisesti ja tietoa jaetaan yrityksen sisällä.

    b) **Jos ei, aiotteko kehittää sellaisen tulevaisuudessa?** Seitsemän haastateltua tilitoimistoa, jotka eivät omaa tietoturvasuunnitelmaa antavat varsin jakautuneen näkemyksen suunnitelman käyttöönotosta. Kolme haastateltavaa kokee, että tälle voi hyvinkin olla tarve tulevaisuudessa, joten varovaisesti arvioiden tietoturvasuunnitelman käyttöönotto lisääntyy tältä osin. Toisaalta loput neljä vastaajaa kertovat, ettei tätä tulla soveltamaan, syyksi kerrotaan henkilökunnan pieni koko tai epävarmuus siitä mitä tietoturvasuunnitelma pitää sisällään.

12) **Onko yrityksenne toimintaa varten luotu suljettu yksityinen lähiverkko?** Kahdeksan vastaajaa yhdeksästä kertoo käyttävänsä yrityksensä toiminnassa suljettua lähiverkkoa. Tämä on tietoturvan kannalta äärimmäisen olennainen elementti, ja on lupaavaa tutkimuksen kannalta, että selkeä valtaosa tilitoimistoista noudattaa tätä käytäntöä. Näin vieraiden tahojen tunkeutuminen yrityksen tietoverkkoihin saadaan suurelta osin estettyä.

13) **Onko työpaikkanne verkkoon yhteydessä laitteita, joita ei käytetä työntekoon?** Kaikki vastaajat ilmoittavat, että työpaikan verkko on pyhitetty vain työntekoon käytettäville laitteille. Mikäli tämä toteutuu täysin käytännössä, on se hyvä merkki tilitoimistojen toiminnasta kyberturvallisuuden

parissa. Ylimääräisten laitteiden yhdistäminen tietokoneisiin saattaa olla ennalta huomaamaton riskitekijä muistilaitteiden jne. saattaessa olla haitta-ohjelmien saastuttamia, ja kun nämä pidetään työpaikan verkon ulkopuolella, suljetaan yksi potentiaalinen tietoturvariski.

14) **Kuinka usein päivitätte käytössänne olevia laitteita tai ohjelmia?** Tilitoimistot luottavat haastattelujen perusteella vahvasti palveluiden automaattiseen päivitystahtiin: kahdeksan vastaajaa yhdeksästä kertoo ainakin ohjelmistojen päivittyvän omatoimisesti ja yksi vastaaja ilmoittaa päivittävänsä laitteet ja/tai ohjelmat palveluntarjoajan suositusten mukaisesti. Toisaalta tämä on selkeä osoitus digitalisaation kehityskulusta, jossa laitteiden ja ohjelmistojen automatisaatio huolehtii mm. päivityksistä, mutta vastavuoroisesti käyttäjien oma päivitystahti jää harvakseltaan toteutuvaksi. Kaksi vastaajaa ilmoittaa automaattisen päivityksen ulkopuolelle jäävien toimintojen olevan satunnaista.

15) **Käytättekö paljon ulkoisia (muisti)laitteita (puhelimet, ulkoiset USB-kiintolevyt jne.) tiedostojen siirtämisessä koneelta toiselle?** Ulkoisten muistilaitteiden käyttäminen tiedonsiirtotarkoituksessa vaikuttaa tehneen tilaa muille metodeille. Kuusi tutkimukseen osallistunutta tilitoimistoa antaa kysymykseen suorapuheisen kieltävän vastauksen, neljän heistä tarkentaessa tiedostojen siirron tapahtuvan pääsääntöisesti pilviympäristössä. Pilvipalveluista onkin tullut erottamaton osa monien tilitoimistojen työntekoa, kuten haastattelun vastaukset myöhemmin tulevat osoittamaan. Loput kolme vastaajaa kertoo käyttävänsä ulkoisia muistilaitteita pääsääntöisesti varmuuskopiointiin, yhden vastaajan korostaessa vain työpaikan käyttöön tarkoitettujen muistitikkujen soveltamista.

16) **Onko työpaikallanne käytössä webkameroita tai mikrofoneja?** Kuusi vastaajaa kertoo yrityksensä tiloissa olevan webkamera ja/tai mikrofoni. Videopuhelujen yleistyessä myös yritysten toiminnassa tämä käytäntö ei juurikaan yllätä. Lisäksi on huomioitavaa, että älypuhelimet, joita on varmasti lähes kaikilla käytössä tänä päivänä, omaavat luonnollisesti äänen nauhoitukseen sopivan tekniikan. Ei ole varmaa, kuinka moni huomioi tämän vastauksessaan, tätä ei sentään erikseen painotettu kysymyksessä.

    a) **Jos on, ovatko ne oletusarvoisesti toimintavalmiudessa?** Edellä mainituista kuudesta vastaajasta kolme ilmoittaa mikrofonien ja/tai webkameroiden olevan jatkuvasti toimintavalmiudessa. Tämä on kyberturvan kannalta huomioitava korjausta vaativa seikka, sillä kyseiset laitteet ovat alttiita kaappauksille, ja ne saattavat nauhoittaa kuvaa tai ääntä hakkereiden käyttöön täysin huomaamattomasti (Saleem ym., 2017). Näiden pitäminen sammuksissa siihen asti, kunnes niitä tarvitaan, ehkäisee väärinkäytöksiä selkeästi. Loput kolme vastaajaa kertookin pitävänsä laitteet sammuksissa. Sekä työnteon että henkilökohtaisen arjen kannalta tärkeää älypuhelinta on vaikeampi alkaa sulkemaan kokonaan

työn ajaksi, mutta kenties sen säilyttäminen etäämpänä työpisteestä olisi sopiva ratkaisu.

17) **Onko yrityksenne varautunut tilanteisiin, joissa ette pysty käyttämään tietojärjestelmiä tai internetiä?** Ottaen huomioon kuinka riippuvaisia tilitoimistot ovat internetistä ja digitaalisista työympäristöistä, olisi hyvä, että jonkinlaisia vararatkaisuja toiminnan jatkamiselle löytyisi. Mitään selkeitä suunnitelmia toiminnan korvaamiselle eivät haastateltavat anna, mutta laajakaistayhteyden korvaaminen mobiiliverkolla tai muulla varajärjestelmällä toistuu kuudella vastaajalla. Yksi haastateltava kertoo yrityksen kirjanpitojärjestelmän olevan itsessään riippumaton internetistä, joten ainakaan verkkokatkosten osalta mitään varautumista ei tarvita. Kaksi vastaajaa ilmoittaa, ettei yritys varaudu juuri ollenkaan vastaaviin tilanteisiin. Mielenkiintoista tutkimuksen kannalta on, että tietojärjestelmiä ei ole erikseen huomioitu pois lukien verkkoyhteydet, joten näihin liittyvät heikkoudet jäävät tältä osin selvittämättä. Kenties kysymyksenasettelu ei ole avannut riittävästi näitä vaihtoehtoja.

    a) **Onko kyseisiä tilanteita tullut vastaan?** Kuusi yhdeksästä haastateltavasta kertoo yrityksensä kokeneen tietojärjestelmiä tai internetin kaataneita tilanteita, ja näistäkin valtaosa liittyy verkkokatkoksiin: neljä edellä mainituista mainitsee lähiverkon/valokuituyhteyden kaatumisen tai palveluntarjoajan ongelmat. Yksi vastaajista kertoo itsestä riippumattomat sähkökatkokset ongelmatilanteeksi. Kolmella vastaajista ei oman kertomansa mukaan ole tullut vastaan tilanteita, joissa järjestelmien kaatuminen olisi estänyt työnteon.

    b) **Jos vastaava tilanne on tapahtunut, kuinka kauan tilanteen korjaaminen keskimäärin vei?** Viisi haastateltavaa vastaavat tähän edelleen pääsääntöisesti verkkoyhteyksien aiheuttamien ongelmien näkökulmasta. Tilitoimiston laajakaistayhteyden palauttaminen on vaihdellut muutamasta minuutista tai tunnista pariin päivään, joten verkkoongelmien kirjo on selkeästi ollut vaihtelevaa ja ainakin yhden vastaajan perusteella hyvin riippuvaista palveluntarjoajasta. Ottaen huomioon, että mobiiliverkon omaksuminen on varsin yleistä tutkimukseen osallistuneiden yritysten keskuudessa, verkko-ongelmien aiheuttamat haitat lienevät minimaalisia. Yksi vastaajista kertoo myös ohjelmistokatkojen aiheuttamista ongelmista ja niiden vieneen jopa puolitoista päivää, mikä on jo yritystoiminnan kannalta hankalampaa.

18) **Onko yrityksenne varautunut laitteistoihinne kohdistuviin fyysisiin ongelmatilanteisiin, esim. hajoaminen tai varkaudet?** Varmuuskopiointi on kiitettävän yleinen käytäntö haastateltujen tilitoimistojen keskuudessa: 8 vastaaja yhdeksästä kertoo tärkeiden tietojen tallentamisesta tiedon säilyvyyden takaamiseksi fyysisten ongelmatilanteiden varalta. Muita mainittuja varotoimenpiteitä ovat atk-tukihenkilön apu hajoamistilanteissa, kame-

roiden ja/tai muiden hälytysjärjestelmien käyttö (lukitussa) liikekiinteistössä sekä kattava vahinkovakuutus. Näiden perusteella haastatellut tilitoimistot vaikuttavat olevan varsin hyvin varautuneita laitteistojen hajoamisiin tai varkauksiin.

a) **Onko yrityksenne tietojärjestelmistä ja tiedoista olemassa kattavat varmuuskopiot ja säännöllinen varmuuskopiointi?** Kuten edeltävän kysymyksen vastaukset asiaa pohjustivat, on varmuuskopiointi erittäin yleinen käytäntö yrityksen käytössä olevan tiedon turvaamiseksi. Kaikki yhdeksän vastaajaa ilmoittavat tästä erikseen kysyttäessä yrityksensä suorittavan kattavan ja säännöllisen varmuuskopioinnin. Näistä peräti seitsemän käyttää pilvipalveluja varmuuskopiointiin, ja vain yksi vastaaja täsmentää tallentavansa tietonsa viikoittain ulkoisille kovalevyille. Digitaalisen tiedon tallentaminen ja turvaaminen pilveen on siis tullut jäädäkseen, mikä ei sinänsä ole yllättävää datan jakamisen ja tallentamisen helppouden vuoksi. Toisaalta pelkästään pilvipalveluihin turvautuminen voi olla riskitekijä, sillä tällöin potentiaaliset tietomurrot saattavat tehdä varmuuskopioinnin tyhjäksi.

19) **Tekeekö yrityksenne henkilökunta usein töitä kotoa käsin?** Kysymys etätyöskentelystä osui erityisen poikkeukselliseen hetkeen, globaalin koronaviruspandemian vallitessa haastattelujen toteutuksen aikana ja kannustaessa työntekijöitä alalla kuin alalla etätyöskentelyyn. Vaikka kysymyksen yhteydessä ei erityisesti eroteltu poikkeusoloissa etätyöskentelyä normaalista olosuhteista, on varsin mahdollista, että koronapandemia saattoi vaikuttaa joidenkin haastateltujen vastauksiin. Kaikki yhdeksän haastateltavaa kertoo yrityksessään ilmenevän kotoa käsin työskentelyä ainakin jossain määrin, vaihdellen yksinkertaisesta ”kyllä”-vastauksesta (2 vastaajaa) ”ei usein/silloin tällöin/jonkin verran”-vastauksiin (3 vastaajaa). Yksi haastateltava itse (toimitusjohtaja) tekee töitä kotoa käsin, muun henkilökunnan tehdessä näin oletettavasti joko hyvin vähän tai ei ollenkaan, ja yksi vastaaja korostaa etätyöskentelyn yleisyyttä yrityksen kannettavilla koneilla, poissulkien omien laitteiden käytön. Kaksi haastateltavista ilmoittaa turvautuvansa etätyöskentelyyn lähinnä poikkeusoloissa, ja näissä vastauksissa korostunee eniten tutkimuksen aikaiset olosuhteet. Digitalisaatio on luonnollisesti tarjonnut paremmat puitteet etätyöskentelylle ja monet mikrokokoiset tilitoimistotkin näyttävät turvautuvan tähän mahdollisuuteen, mutta herää kysymys, miten etätyöskentely konseptina olisi mielletty, ellei koronaviruspandemia olisi nostanut tätä yhteiskunnallisen huomion keskiöön.

a) **Jos tekee, miten työntekijät huolehtivat tietoturvan ylläpitämisestä työpaikan ulkopuolella?** Tietoturvallisen etätyöskentelyn kannalta puitteet kotona pitää olla toimivat. Haastatellut tilitoimistot antavat tältä osin varsin kirjavasti erilaisia toimintasääntöjä. Yleisesti mainitaan kotona käytössä olevat virustorjuntaohjelmistot, tärkeän datan säilyttäminen salasanojen tai turvatun sähköpostin/pilvipalvelun takana se-

kä yrityksen (kannettavien) tietokoneiden tai puhelinten käyttö henkilökohtaisten sijasta. Muita yksittäisiä seikkoja ovat yrityksen yhteisten sääntöjen noudattaminen kotona, työkoneen sijainti vieraiden ulottumattomissa ja yrityksen suunnitelmat tärkeiden fyysisten asiakirjojen luopumisesta etätyöskentelyssä. Yksi vastaajista kertoo etätyöskentelyn sujuvan vain kotiympäristön tarjoamissa puitteissa ja toinen toteaa, ettei etätyöskentelystä ole muodostunut vakiintunutta tapaa ja siksi työntekijöiden työskentelystä kotona ei ole juurikaan tietoa.

b) **Onko kotona työskentelyä varten olemassa oma tietoturvasuunnitelma?** Yksikään haastatelluista tilitoimistoista ei omien sanojensa mukaan ole kehittänyt etätyöskentelyä varten erillistä suunnitelmaa tietoturvan ylläpitämistä silmällä pitäen. Kolme vastaajaa kertoo, että kotona pätevät samat säännöt kuin työpaikalla eikä erillistä suunnitelmaa yksinkertaisesti tarvita. Tämä ei itsessään ole välttämättä huono asia: mikäli etätyöskentely-ympäristö on lähtökohtaisesti turvallinen ja henkilökohtaiset tietoturvaratkaisut täyttävät jonkinlaisen minimivaatimuksen, tai työpaikan tietoturvasuunnitelma on riittävän kattava, että sitä voidaan soveltaa etätyöskentelyyn niin puitteet ovat jokseenkin kunnossa. Mikrokokoiselle yritykselle ero kotona tai toimistolla työskentelyyn voi olla hyvinkin häilyvä. Kotiolosuhteet voivat kuitenkin poiketa merkittävästi työpaikan vastaavista, varsinkin mikäli työntekijä päätyy laskemaan varaustasoaan työpaikan ulkopuolella.

c) **Onko työntekijöillä käytössä kattava tietoturvajärjestelmäpaketti kotona?** Viisi vastaajaa yhdeksästä kertoo omaavansa työskentelyään varten jonkinlaisen tietoturvajärjestelmän käytössään olevissa laitteissa: yhden mukaan yrityksen (kannettavissa) koneissa on kattava tietoturva, kaksi mainitsee omaavansa kotona saman kattavan tietoturvapaketin kuin toimistolla, kaksi vastaaja käyttää laajaa maksullista virustorjuntapalvelua tai käytössä olevan virustorjuntaohjelman tarjoamia omia palveluita. Kolme vastaajaa ei antanut spesifiä vastausta pääosin siksi, ettei yrityksessä yleisesti työskennellä kotoa käsin, ja yksi vastaajista kertoo, ettei erillistä kattavaa tietoturvajärjestelmää ole oletusarvoisesti käytössä. Vastausten kirjo antaa yleisesti varsin lupaavan kuvan tietoturvan ylläpitämisestä kotiympäristössä, valtaosan vastaajista omaavan vähintään jonkinlaisen virustorjuntakapasiteetin etätyöskentelyyn.

20) **Teettekö tärkeitä/luottamuksellisia työtehtäviä mobiililaitteilla?** Tilitoimistot tekevät haastattelujen perusteella hyvin vähän tärkeitä töitä mobiililaitteilla. Neljä vastaajaa ilmoittaa kysymykseen kieltävästi, kaksi vastaajaa kertoo yrityksen tekevän näin vain harvoin ja kaksi antaa myöntävän vastauksen. Yksi haastateltava toteaa yrityksen käyttävän mobiililaitteita vain omaan yritykseen liittyvään työskentelyyn, ei asiakkaita koskevien tehtävien puitteissa. Ottaen huomioon, kuinka epävarmaa mobiililaitteiden turvallisuus on, tai kuinka vähän siitä tiedetään arjen käytössä, tämä on lupaa-

va merkki. Se, että varotoimenpiteenä – joko tietoisesti tai ei – potentiaalinen tietoturvauhka saadaan paikattua, on itsessään hyvä seikka.

21) **Miten toimitte fyysisen tiedostomateriaalin (esim. tulosteet) tietoturvan kanssa? Arkistointi, säilytys, luottamuksellisuuden takaaminen?** Fyysisen materiaalin tietoturva ja sen takaaminen tarjoaa paljon erilaisia vastauksia. Tilojen tai kaappien lukitseminen toistuu kuitenkin usein (viisi vastaajaa), samoin materiaalin hävitys tarpeen tullen (4 vastaajaa) sekä asiakasta koskevan henkilökohtaisen materiaalin palauttaminen asianosaisille (3 vastaajaa). Muita ilmoitettuja keinoja ovat mm. kansioiden nimeämättä jättäminen tai dokumenttien pitäminen piilossa ulkopuolisilta. Kaksi vastaajaa kertoo yrityksensä siirtyneen kokonaan sähköiseen arkistointiin tai tiedostojen käsittelyyn pääasiallisesti pilvipalveluissa, eli askeleita täysin digitaaliseen toimintaan on selvästi otettu. Muuten tilitoimistot näyttävät toteuttavan fyysisten dokumenttien tietoturvaa hyvin odotetulla, selkeillä tavoilla.

22) **Miten yrityksenne hävittää tarpeettoman mutta arkaluontoisen/salassa pidettävän materiaalin?** Kaikki vastaajat kertovat hävittävänsä kertyvän tarpeettoman tietosuojamateriaalin kuten asiakastietoja sisältävät dokumentit, mikä on tietoturvan kannalta erinomainen asia. Metodit näyttävät jakautuvan pääasiassa kahteen vaihtoehtoon: joko paperiset asiakirjat silputaan tai poltetaan tilitoimiston toimesta (5 vastaajaa), tai ne päätyvät tietosuojajätteen lajitteluun hävitettäväksi tietoturvapalvelujen toimesta (4 vastaajaa). Jälkimmäinen vaihtoehto lienee (mikäli palveluntuottaja toimii oikeaoppisesti) tietoturvallisin jo siksikin, että tietosuojajäte kerätään usein lukittuihin säiliöihin, jotka toimitetaan valvottua sisällön hävitystä varten. Mutta kaikki tämä koskee vain fyysisiä dokumentteja, eikä tähän kysymykseen vastanneista moni ottanut huomioon digitaalisessa muodossa ilmenevää materiaalia, erityisesti pilvipalveluihin tallennettujen tiedostojen osalta ei ole ehdotonta selvyyttä siitä, poistetaanko vanhat tiedostot vai jäävätkö tiedostot unohduksiin pilveen. Fyysisiin tallennuslaitteisiin liittyvät tallenteiden loppukäsittelyt otettiin toisaalta varsin hyvin huomioon jatkokysymyksen yhteydessä.

   a) **Entä vanhat ja tarpeettomat laitteet?** Vanhoihin ja tarpeettomiin laitteisiin luetaan myös tallennuslaitteet, kuten kovalevyt ja muistitikut. Siksikin niiden sisältämien tallenteiden/tiedostojen loppukäsittely on edellisen kysymyksen kannalta relevanttia selvittää. Kuusi vastaajista kertoo hävittävänsä tällaiset laitteet joko itse tai antavansa laitteet atktuelle tai muulle luotettavalle toimijalle tuhottavaksi. Yksi vastaaja ilmoittaa säilyttävänsä tietokoneiden kovalevyt ja toimittavansa loput laitteet asiaankuuluville vastaanottopaikoille, loput kaksi yritystä ei joko ole kokenut laitteiden hävittämiselle tarvetta tai heillä ei ole vielä suunnitelmaa vanhojen laitteiden varalle. Jälkimmäisen tapauksessa oletuksena yritys tullee tyhjentämään laitteet kaikista tiedostoista ja antaa ne hävitettäväksi. Eli tilitoimistoilla näyttää olevan vahva käsitys

siitä, kuinka koneita ja tallennuslaitteita on käsiteltävä kun ne osoittautuvat tarpeettomiksi ja tietoturvan kannalta tärkein seikka, eli tiedostojen ulkopuolelle päätymisen estäminen, pyritään toteuttamaan oikein.

23) **Onko työntekijöillänne yhtäläiset oikeudet kaikkiin tietojärjestelmänne tietoihin?** Mitä tulee yrityksen tietojen jakamiseen työpaikan sisällä, tilitoimistoilla vaikuttaa olevan varsin selkeät käytänteet. Valtaosa vastanneista yrityksistä (viisi yhdeksästä) ilmoittaa selkeästi, ettei kaikilla työntekijöillä ole yhtäläisiä käyttöoikeuksia tietojärjestelmiin, ja loppujen neljän tilitoimiston mukaan osaan tiedoista tällaiset oikeudet löytyy, sanamuodon vaihdellen ”kyllä lähes kaikkiin” ja ”oikeudet myönnetään työntekijän roolin mukaan”. Tästä voitaneen päätellä, että – kuten useasti pienyrityksissä on käytänteenä – mikrokokoisessa tilitoimistossa vain harvalla, lähinnä omistajalla on täydet pääsyoikeudet kaikkiin yrityksen tiedostoihin ja loput työntekijät saavat käyttöönsä kaiken tarvittavan. Missä sitten menee raja sen osalta, kuinka paljon ja tietoturvan kannalta kuinka tärkeitä tietoja jää työntekijöiden käytön ulkopuolelle lienee yksilökohtaista. Se, että tietojärjestelmien tiedot eivät ole kaikkien saatavilla ja siten mahdollisesti altistu työntekijöihin kohdistuville tietovuodoille on itsessään hyvä toimenpide. Toisaalta tämä herättää huomiota siihen, miten yrityksen toiminnan käy, jos omistajan henkilökohtaiset oikeudet yhtäkkiä katoaisivat.

24) **Miten työntekijänne suojaavat salasanoja ja käyttäjätietojaan?** Tilitoimistoilla vaikuttaa olevan käytäntönä järjestää kullekin työntekijälleen omat henkilökohtaiset käyttäjätunnukset ja salasanat, mikä on luonnollisesti odotettavaa. Miten sitten näitä sekä muita yrityksen yhteisessä käytössä olevia salasanoja säilötään tai suojataan, vaihtelee jonkin verran. Kolme vastaajaa kertoo, että käyttäjät iskostavat tunnuksensa ja salasanat omaan muistiinsa ja yksi ilmoittaa, ettei salasanoja kirjata mihinkään ylös. Nämä ovat tietoturvan kannalta toisaalta hyviä seikkoja, kun mitään muistiinpanoja näistä ei jää, mutta ihmisen muisti ei kaikissa tapauksissa ole välttämättä kaikkein luotettavin työkalu. Muita toistuvia seikkoja ovat salasanojen säilyttäminen erillään muista (2 vastaajaa) tai tallettaminen varmaan/lukittuun paikkaan (2 vastaajaa). Muutama tilitoimisto (3 vastaajaa) on omaksunut digitalisaation salasanojen hallinnoimiseksi ja ottanut käyttöönsä tätä tarkoitusta varten kehitetyn ohjelman. Tällaiset salasanoja tallentavat sovellukset omaavat yleensä varsin vahvan suojauksen, joten niiden käyttö on turvallista – kunhan ohjelma on luotettava ja käyttäjä ei unohda sovelluksen pääsalasanaa.

   a) **Onko yrityksessänne käyttäjätunnukset tai salasanat jossain fyysisesti näkyvillä?** Kaikki tutkimukseen osallistuneet tilitoimistot noudattavat yksinkertaista tätä helppoa ja yksinkertaista sääntöä käyttäjätunnusten ja salasanojen säilyttämisen suhteen: niitä ei pidetä toimistossa tai muualla näkyvillä muistutuksena kaikille. Näin estetään mahdollisten toimistoon astuvien ulkopuolisten tai webkameran hakkeroivan kyberrikollisen pääsy tilitoimiston tunnuksiin käsiksi. Tämä on hyvä seikka,

joka toivon mukaan toimii viitteenä sille että salasanojen kirjoittaminen paperille ja säilyttäminen työpaikan tiloissa näkösällä on vähemmän yleinen ilmiö kuin pelätään.

b) **Kuinka usein päivitätte salasanoja?** Tiheä ja säännöllinen salasanojen uusiminen on tietoturvan peruspilareita, ja tämän suhteen tilitoimistot toimivat varsin vaihtelevasti. Neljä vastaajaa kertoo päivittävänsä salasanojansa (hyvin) harvoin tai ei säännöllisesti, kolme ilmoittaa tekevänsä näin muutaman kerran vuodessa, ja kaksi vastaajista kertoo luottavansa ohjelmien ja laitteiden muistutuksiin. Positiivisena ilmiönä kolme tilitoimistoista nostaa esille mobiili-/vahvan tunnistautumisen käytön ainakin joissain toiminnoissaan. Näitä metodeja harvoin päivitetään, mutta ne takaavat paljon normaalia turvallisemman kirjautumismetodin kuin pelkkien salasanojen varassa toimimisen. Eli kokonaisuudessaan joillakin tilitoimistoilla on parantamisen varaa, mutta toisaalta selkeitä toimenpiteitä salasanojen säännölliseen päivittämiseen ja kirjautumistietojen vahventamiseen on havaittavissa.

25) **Onko yrityksenne käytössä pilvipalveluita?** Kaikki haastatellut tilitoimistot kertovat käyttävänsä pilvipalveluja ainakin jossain muodossa, eli digitalisaatio on tältäkin osin vahvasti omaksuttu. Seuraava kysymys tulee siis koskettamaan kaikkia tutkimukseen osallistuneita.

a) **Jos on, miten huolehditte näiden tietoturvasta?** Haastatellut tilitoimistot ovat yksimielisiä siitä, että pilvipalvelujen tietoturva on parempi jättää palveluntarjoajan harteille. Oletuksena kuitenkin on, että yritykset noudattavat työpaikan normaaleja turvallisuuskäytänteitä pilvipalvelujen käytössä, sillä ohjelmistojen tekninen puoli on vain yksi osa tietoturvaa. Lopulta tietoturva on vain niin tehokas kuin niiden käyttäjien omat toimet ja ymmärrys turvallisuuskäytänteistä. Yksi vastaajista tarkentaa, ettei heillä pilveen tallenneta mitään arkaluontoista saatikka arvokasta dataa, joten tältä osin tietynlaisia varovaisuutta ylläpidetään. Myös työpaikan verkon koskemattomuus korostuu, jottei pilvipalveluihin päästä käsiksi yrityksen sisältä käsin hakkeroinnin keinoin. Tällaisissa asioissa olisi siis huomioitavaa.

26) **Turvaudutteko tietojenkäsittelyssä ulkopuolisiin toimijoihin?** Tilitoimistot vaikuttavat pitävän aktiivisesti liiketoimensa langat omissa käsissään, ainakin mitä tulee tiedonkäsittelyyn ja IT:hen yrityksen sisällä. Seitsemän vastaajaa antaa kysymykseen kielteisen vastauksen, yksi mieltää ainoastaan pilvipalvelujen toimittajan tällaiseksi ulkopuoliseksi tahoksi, ja yksi tilitoimisto nostaa esille atk-tuen ja ostetut toiminnanohjauspalvelut. Kyberturvallisuuden kannalta tämä on varsin hyvä merkki, tilitoimistojen käyttämää dataa ei vaikuttaisi jaettavan juurikaan yrityksen ulkopuolelle lukuun ottamatta tilanteita, joissa huoltoa tai IT-tukea tarvitaan tai dataa annetaan palveluntarjoajien säilytettäväksi. Tällainen on luonnollisesti luottamuk-

seen perustuvaa toimintaa kuten mikä tahansa liiketoiminta, eli katsotaan että pilvipalvelut ja muut yritykset omaavat riittävät turvallisuustoimet tiedonhallinnan suhteen ja nämä eivät käytä mahdollisia käsiinsä saamia tietoja hyväkseen.

27) **Onko yrityksellänne kotisivuja?** Kaikki tutkimukseen osallistuneet tilitoimistot omaavat kotisivut, joten näillä on siis yksi kyberturvallisuuden elementti huolehdittavanaan.

   a) **Jos on, annatteko julkaista sivustollanne mainoksia?** Yksikään vastaajista ei kertomansa mukaan mainosta kotisivuillaan mitään, joten huoli mainosten kaappaamisesta on sikäli aiheeton – ainakin tutkimukseen osallistuneiden yritysten tapauksessa. Lisäksi odottamattomien mainosten ilmaantuminen on nopea merkki siitä että kaikki ei ole kohdallaan, mutta vain mikäli kotisivuja tarkastetaan ja päivitetään riittävän tiheästi.

   b) **Milloin olette viimeksi päivittäneet kotisivunne?** Vastaukset tähän kysymykseen osoittavat, että tilitoimistoilla on melkoisia eroja mitä tulee verkkosivujen päivitystahtiin. Neljä vastaajista myöntää edellisestä päivityksestä olevan vähintään vuosi, jopa kolme vuotta; kolmen vastaajan tapauksessa päivityksiä on tehty viimeksi alle kuukausi sitten, eli ero edelliseen ryhmään on huomattava. Yksi tutkimukseen osallistunut kertoo päivityksille olevan yleisesti hyvin harvoin tarvetta, ja yksi kertoo, ettei muista edellisen päivityksen ajankohtaa. On sikäli ymmärrettävää, että yrityksen kotisivuilla ei ole välttämätöntä säännöllistä päivitystarvetta, mikäli tilitoimiston toiminnassa ei tapahdu merkittäviä muutoksia, mutta vähintään sivuston sisällön tarkastaminen säännöllisin väliajoin auttaisi ehkäisemään sille mahdollisesti pesiytyvien haittaohjelmien aiheuttamia ongelmia.

   c) **Onko sivustollanne paljon linkkejä ja/tai yhteystietoja, joita voi kopioida?** Kaikki tutkimukseen osallistuneet toteavat, ettei heidän kotisivuillaan ole paljon linkkejä, yhteystietoja tms., jotka ovat kopioitavissa. On tietenkin subjektiivista, miten itse kukin määrittelee sen mikä on ”paljon”, mutta oletusarvoisesti kaikki mikä ei ole välttämätöntä yrityksen yhteystietojen ja toiminnan välittämiseksi on tällaiseksi miellettävissä. Viime kädessä se, ettei esillä olevaa tietoa voida yhdistää jonkun yksityistietoihin on tärkeintä.

   d) **Onko domaininne tarjoaja maksullinen toimija vai ilmaisen verkkotunnuksen tarjoava taho?** Yksikään vastaajista ei kerro turvautuneensa kotisivujensa isännöinnissä ilmaisen verkkosivuston tarjoavaan toimijaan, vaan on vuokrannut maksullisen domainin. Vaikka jälkimmäisissä toimijoissakin voi olla merkittäviä eroja palvelun laajuuden ym. suhteen, on ajatus siitä, että palveluntuottajalla on vähintään taloudelliset

motiivit tuottaa turvalliset puitteet asiakkaan verkkosivuille yleisesti hyvä kyberturvan kannalta.

28) **Saatteko sähköpostin kautta usein roskapostia?** Roskaposti vaikuttaa nykyään olevan ilmiönä sellainen, että on harvinaisempaa jos sähköpostiosoite ei sellaista vastaanota. Tilitoimistotkin vaikuttavat saavan roskapostia vaihtelevin määrin: neljä vastaajaa sanoo suoraan, ettei roskapostia ole (juurikaan) ongelmaksi asti; kolmen vastaajan mukaan sähköpostiin ilmestyy roskapostia hyvin vähän tai jonkin verran; ja kaksi tilitoimistoa saa kertomansa mukaan roskapostia usein. Yksittäistä syytä siihen, miten roskapostin määrä kullekin määräytyy tai miten sitä levittävät tahot ovat saaneet käsiinsä tilitoimistojen sähköpostiosoitteita ei liene olemassa, mutta on osoitettava selkeää varovaisuutta siinä, missä ja kenelle sähköpostiosoitettaan jakaa. On kaiken kaikkiaan kokonaisuudessaan hyvä seikka, että vain harva kokee roskapostiongelman huomattavaksi.

29) **Toimiiko yrityksenne aktiivisesti sosiaalisessa mediassa?** Huolimatta sosiaalisen median kasvavasta läsnäolosta sekä ihmisten arjessa että yritysten toiminnassa, mikrokokoiset tilitoimistot vaikuttavat pääsääntöisesti jättäytyvän tämän digitaalisen maailman ulkopuolelle. Kaikki vastaajat kertovat yrityksensä läsnäolon olevan joko olematonta (3 vastaajaa) tai vähäistä (kuusi vastaajaa). Ilmeisesti tilitoimistot onnistuvat ylläpitämään liiketoimintaansa ilman aktiivista osallistumista sosiaalisen median pyörteisiin, ja kyberturvallisuuden kannalta näin vältytään myös mahdolliselta eitoivotulta huomiolta, kuten petoksilta ja sosiaaliselta manipuloinnilta.

30) **Käytättekö työpaikkanne laitteita muuhun kuin työntekoon, esim. yksityisten asioiden hoitamiseen?** Koska kaikki internetissä toimiminen jättää jälkensä, olisi siksi suositeltavaa pitää työ ja yksityiselämä erillään toisistaan ihan yleisen yksityisyyden ja turvallisuuden kannalta. Valitettavasti jotkut haastatelluista tilitoimistoista (3 vastaajaa) käyttävät työpaikan koneita työn ulkopuoliseen toimintaan, muiden (4 vastaajaa) tehden näin harvemmin tai jonkin verran. Yksi vastaaja kieltää tekevänsä näin alkuunkaan, ja yksi kertoo käyttävänsä omaa konettaan muttei toimiston konetta henkilökohtaisten asioiden hoitoon. Tässä olisi kieltämättä parantamisen varaa, sillä kuten aiemmin todettu, työpaikan verkkoon kytketyt laitteet voivat helposti levittää haittaohjelmia muiden laitteiden välillä. Ei vaadita kuin yksi varomaton vahinkoklikkaus väärässä paikassa niin koko toimisto saattaa olla altis hakkereille. Luonnollisesti vain murto-osa internetissä asioimisista johtaa mihinkään negatiiviseen ilmiöön, mutta kuten muissakin tilanteissa, turvallisuudentunteeseen ei kannata tuudittautua.

31) **Minkä miellätte tällä hetkellä tärkeimmäksi digitalisaation aiheuttamaksi uhkatekijäksi?** Digitalisaation yleistymisen aiheuttamat lieveilmiöt ovat hyvin mikrokokoisten tilitoimistojen tiedossa, vastaukset kysymykseen vaihtelevat ja kaikki ovat huomioitavia seikkoja tietoturvan kannalta. Ylei-

senä vastauksena mainitaan identiteettivarkaudet/-vuodot (2 vastaajaa) tai tietomurrot (2 vastaajaa), erityisesti tilitoimiston toiminnan kannalta erittäin vaarallisia tilanteita ottaen huomioon tilitoimistojen työnkuvan ja käsiteltävän tiedon sensitiivisyyden. Myös digitaalisen (asiakas)tiedon ja työkalujen katoaminen tai käytön estyminen mainittiin (1 vastaaja), vahvistaen tilitoimistojen kokemaa huolta oman toiminnan ja luottamuksellisuuden kokemasta vahingosta kyberuhkien edessä. Muita mainittuja kyberturvallisuuden ainaisia uhkatekijöitä ovat hakkerit ja kyberrikollisuus yleisesti (1 vastaaja), verkon kautta ilmenevät hyökkäykset/kaappaukset/virukset (1 vastaaja) ja verkossa ilmenevät huijaukset (1 vastaaja). Vaikka nämä ovat varsin yleistäviä vastauksia, osoittaa tämä että tilitoimistot osaavat tunnistaa potentiaalisia vaaratekijöitä. Yksi erityisesti digitalisaation varjopuolia korostava vastaus annettiin myös, ”yleinen riippuvuus internetistä”. On totta, että internet on tuonut mukanaan käteviä työkaluja ja metodeja moniin tilanteisiin sekä luonut puitteet tehokkaalle työskentelylle, mutta lieveilmiöt ovat seuranneet nopeasti perässä. On siksi mielenkiintoista huomata, että koko internetin konseptin aiheuttamat ongelmat noteerataan ja yleistä riippuvuutta tätä kohtaan osataan kritisoida. Siinä missä hakkeroinnit, virukset ym. kyberuhat ovat pikemminkin digitalisaation seurauksia, internetiä voisi monella tapaa pitää aiheuttavana tekijänä.

32) **Onko yrityksenne joutunut kyberrikollisuuden tai hakkeroinnin kohteeksi?** Kolme yhdeksästä vastanneesta tilitoimistosta kertoo joutuneensa kohdennettujen kyberuhkien kohteeksi, mikä on vähemmän kuin voisi odottaa, kyberrikollisuuden yleistyessä jatkuvasti. On toisaalta huomioitava tutkimuksen kannalta erittäin tärkeä seikka: kuudesta vastaajasta, jotka vastasivat kysymykseen ”ei”, neljä korostaa ettei ole *tiedostetusti* kokenut tällaista ilmiötä. Tämä on äärimmäisen hyvä huomio, sillä monet hakkeroinnit tai sellaisen yritykset jäävät helposti huomiotta – tähänhän ne useimmiten pyrkivät, huomaamattomaan matalan profiilin soluttautumiseen ja tietojen kalasteluun. Vain siksi, ettei kyberrikollisuudesta tai hakkeroinnista ole kokemusta, ei tarkoita etteikö tällaisia yrityksiä ole tapahtunut kaikessa hiljaisuudessa – tai peräti onnistunutkin murtamaan yrityksen suojaukset jättämättä mitään jälkiä.

   a) **Mihin isku(t) on kohdistunut?** Ne **k**olme tilitoimistoa, jotka vastasivat myöntävästi edelliseen kysymykseen, antavat kolme hyvin erilaista kokemusta. Yksi vastaajista kertoo hakkerointiyrityksen kohdistuneen yrityksen kotisivuihin ja työsähköpostiin. Tarkentavaa tietoa tilanteesta ei ole, mutta oletettavasti näiden kohteiden tietoliikennettä on yritetty hyödyntää joko tietojen keräämiseen tai käyttäjien ohjaamiseen hakkerin määrittelemille teille. Toisen tapauksessa vastaajan maksukortin tiedot oli hakkeroitu, oletettavasti varastamalla pankkikorttitiedot joltakin tätä säilyttäneeltä palvelulta. Tämä on yksi yleisimmistä hakkeroinnin ilmiöistä. Kolmannen vastaajan kohdalla työntekijöiden sähkö-

postiosoitteita oli käytetty huijausviestien lähettämiseen yrityksen sisällä, klassinen esimerkki phishing-ilmiöstä eli tietojenkalastelusta.

b) **Koitteko taloudellisia tappioita tämän/näiden takia?** Näistä kolmesta tapauksesta ainoastaan yksi ehti johtaa taloudellisiin menetyksiin, eli ei niinkään yllättävästi maksukortin hakkerointiin johtanut tapahtumaketju. Valitettavasti maksukortin tietojen päätyminen ulkopuolisten käsiin selviää usein vasta silloin, kun korttiin kytketyltä tililtä on jo tehty rikollisen toimesta maksutapahtumia ja joko kortin omistaja tai korttiyhtiö huomaa väärinkäytökset. Jäljelle jää tällöin vain jälkipyykin hoito, eli vahinkojen korjaamien ja tilanteen pahenemisen estäminen. Tätä on luonnollisesti vaikea ennakoida muuten kuin olemalla jakamatta maksukortin tietoja internetissä muuten kuin ehdottoman välttämättömissä tilanteissa ja luotettavien palvelujen yhteydessä – ja silloinkin on aina olemassa ainakin häviävän pieni mahdollisuus, että uusi tietomurto saattaa paljastaa käyttäjä- tai maksutiedot rikollisille. Kaksi muuta tapausta ei onneksi aiheuttanut taloudellisia menetyksiä, mutta on vaikea arvioida, olisiko tilanteen eskaloituminen lopulta johtanut siihen vai olisiko lopputuloksena ollut hiljainen tietojen keräys ja tästä johtuvat arvaamattomat seuraukset. On myös pohdittava, ehtivätkö hakkerit saamaan käsiinsä jotain dataa ennen kuin heidän toimintansa paljastui: jos he saivat käsiinsä sähköpostiosoitteita ja kotisivutietoja, kuka tietää mitä muuta heillä saattaa vielä olla hallussaan?

c) **Miten ratkaisitte hakkeroinnin aiheuttamat ongelmat?** Ensimmäisessä tapauksessa, hakkerointiyrityksen paljastuttua tilitoimisto vaihtoi kotisivunsa ja palveluntarjoajan ja aloitti näin puhtaalta pöydältä. Maksukortin hakkerointi ratkaistiin odotetulla tavalla: kortinhaltija sopi luottoyhtiön ja pankin kanssa kortin jäädyttämisestä ja korvaamisesta uudella, ja väärinkäytöstä aiheutuneet menetykset saatiin korvattua. Valitettavasti tekijä tuskin tulee koskaan jäämään kiinni. Kolmannen tilitoimiston tietojenkalasteluun yritys vastasi hiljaisuudella, jättämällä huijarin viestit huomiotta tämä lopetti ennen pitkää ja siirtyi oletettavasti huijaamaan jotakuta muuta. Näissä kolmessa tapauksessa toimittiin varsin esimerkillisesti, nopea reagointi ilmenneeseen ongelmaan vahinkojen minimoimiseksi tai verkkohuijarin huomiotta jättäminen ovat juuri oikeita metodeja kamppailussa kyberrikollisuutta vastaan. Tämä antaa positiivisen kuvan tilitoimistojen valmiustasosta kyberuhkien edessä. Oletettavasti näissä tapauksissa tapahtuneesta on ilmoitettu poliisille, tai mikäli näin ei ole tehty olisi se suositeltavaa, Suomen poliisi kehottaa tekemään rikosilmoituksen jo petoksen yrityksistä (Poliisi, 2020).

6.2 Haastatteluvastaukset tutkimuskysymysten valossa

Mikrokokoisten tilitoimistojen antamat vastaukset haastattelukysymyksiin antavat vaihtelevan mutta viime kädessä jokseenkin lupaavan kuvan ko. yritysten kyberturvallisuuskompetenssista. Digitalisaatio on otettu kaikissa tutkimukseen osallistuneissa yrityksissä avosylin vastaan, mutta omaksuminen ei ole jäänyt pinnalliseksi virran mukana ajelehtimiseksi, jossa tekniikka määrää suunnan ja käyttäjät luottavat tähän sokeasti. Tilitoimistojen työntekijät vaikuttavat saavuttaneen ainakin jonkinasteisen otteen digitaalisen tekniikan toiminnasta ja ymmärtävät sen selkeimpien ongelmien päälle.

Seuraavaksi käydään läpi tutkimuksen alussa esitetyt tutkimuskysymykset ja etsitään haastatteluvastauksista ilmiöitä, joilla voimme vastata näihin kysymyksiin.

6.2.1 Mitä on kyberturvallisuus ja kyberturvallisuussuunnitelma ja mitä ne pitävät sisällään?

Kyberturvallisuuden määritelmä, niin lavea kuin se onkin, on kaikilla yrityksillä tiedossa. Myös tietoturvariskin käsitteeseen on kaikilla antaa sovelias vastaus, joka kertoo ymmärryksestä. Yleisimmät riskit ja uhat ovat tilitoimistojen tiedossa ja joitakin ratkaisuja esitetään.

Kyberturvallisuussuunnitelman määrittely jää haastattelun puitteissa avoimeksi valtaosan yrityksistä jättäneen sen virallisen käyttöönoton kokonaan pois ja vain osan pyrkiessä perehtymään aiheeseen tulevaisuudessa. Näin ollen kyberturvallisuussuunnitelman/kyberstrategian käsitettä avataan lähinnä aiemman tutkimuksen valossa.

6.2.2 Millä tavalla mikrokokoiset tilitoimistot huolehtivat yrityksensä ja asiakkaidensa tietoturvasta?

Tietoturvan ylläpitämiseen on valikoitunut kussakin organisaatiossa ainakin joku vastuuhenkilö ja ammattitaitoiseen IT-tukeen osataan turvautua tarvittaessa. Toisaalta yrityksen ydintoimintaa tai tietojenkäsittelyä ei juurikaan ulkoisteta, eli mm. asiakastiedot säilyvät yrityksen käsissä.

Monilta osin tilitoimistot luottavat käytössään olevien ohjelmien ja järjestelmien toimintakykyyn ja turvallisuuteen, jättäen muun muassa ohjelmapäivitykset niiden huoleksi. Sama pätee hyvin yleisessä käytössä oleviin pilvipalveluihin. Mikäli ohjelmat ja palvelut ovat tunnettuja ja luotettavia toimijoita, asiassa ei sikäli ole mitään sellaista ongelmaa mikä ei koskisi kaikkia palvelun käyttäjiä samanaikaisesti.

Positiivista on, että tilitoimistot osaavat tunnistaa työskentelytavoissaan ja digitaalisessa toimintaympäristössä piileviä uhkia. Vaikka omakohtainen kokemus tai ymmärrys kyberturvallisuudesta tilitoimistojen työntekijöiden kes-

kuudessa vaihtelee, perusasioiden tietämys on merkittävä askel tietoturvan toteuttamisessa

Tietoturvasuunnitelman puute on toinen valitettavan yleinen ilmiö ja itsessään ongelmallinen tilanne, sillä kuten aiemmin todettu suunnitelmallinen ja ennakoiva kyberturvallisuuden toteutus tarjoaa ehdottomasti tehokkaan tavan järjestää organisaation tietoturva. Ilman selkeää tietoturvasuunnitelmaa ja kattavaa riskienarviointia yritys jää helposti pimentoon omassa organisaatiossa vallitsevista riskeistä ja tietoturvan valuvioista, mikä on havaittavissa osassa tilitoimistojen antamista vastauksista: puolet tilitoimistoista ei tunnista ilmeisiä riskejä toiminnassaan, mikä kertoo joko vahvasta osaamisesta tai liiallisesta itsevarmuudesta.

6.2.3 Onko mikrokokoisilla tilitoimistoilla joitain huomioitavia erityispiirteitä kyberturvan ja sen kehittämisen suhteen?

Kyberturvallisuuteen liittyvän koulutuksen puute on yksi heikko lenkki, joka toistuu haastatelluilla tilitoimistoilla. Vaikka monet IT-ammattilaiset saattavatkin olla itseoppineita, jo jonkinlainen tietoturvan peruskoulutus auttaisi vastuuhenkilöä ja koko henkilökuntaa sisäistämään kyberturvallisuuden perusteet paremmin, ja ottaen huomioon kuinka alati muuttuvia kybermaailma ja siihen liittyvät uhkat ovat, aktiivinen ajan tasalla pysyminen jatkokoulutuksen muodossa on toivottavaa.

Etätyöskentely on jokseenkin yleinen ilmiö tilitoimistojen keskuudessa ainakin tutkimuksen toteuttamisen aikana, ja siihen liittyvät toimenpiteet vievät jonkin verran huomiota. Tämä on toisaalta osa työskentelykulttuurin murrosta, ilmiötä, joka on yleistynyt merkittävästi viime vuosina muutenkin (Leskinen, 2021). Oli miten oli, tämä tuo mukanaan haasteita, tilitoimistojen etätyöskentelymetodeissa on parantamisen arvoisia seikkoja ja muutostarpeita erityisesti yhteisten toimintatapojen ja suunnitelmien kehittämiseksi.

Muutoin mikrokokoisten tilitoimistojen kompetenssi kyberturvan suhteen vaihtelee: yrityksen internetsivujen, sähköpostin sekä muun digitaalisen tietojenkäsittelyn ylläpitämisessä joko noudatetaan oikeaoppisia turvallisuuskäytänteitä tai tehdään pieniä, yleensä ei-kriittisiä virheitä. Sama pätee työpaikan työskentelyolosuhteisiin: toimintametodit vaihtelevat toimiston ulkopuolisten laitteiden käytöstä yhteisten salasanojen jakamiseen. Eri yrityksillä on luonnollisesti erilaiset tulkinnat työpaikan kuriin ja yhteisten pelisääntöjen noudattamiseen, mutta olisi suotavaa, että näitä asioita suunnitellaan ja toteutetaan kyberturvallisuus edellä.

Huomioitavaa on myös, että laitteistoihin ja IT-tukeen liittyvissä asioissa resurssipula korostuu erinäisin tavoin: palvelujen ulkoistaminen ja luotto ohjelmien/järjestelmien automatisaatioon kielivät siitä, että joitakin toimintoja jätetään palveluntarjoajien vastuulle joko työasioiden helpottamiseksi/oman toiminnan nopeuttamiseksi.

7 POHDINTA

Tutkimus toteutettiin ja viimeisteltiin poikkeuksellisissa olosuhteissa. Vuoden 2020 alussa alkanut koronaviruspandemia teki erityisesti haastattelujen toteuttamisesta haastavaa. Turvallisuussyistä päädyin toteuttamaan haastattelut puhelimitse, mikä ei allekirjoittaneen mielestä soveltunut teemahaastattelun puitteisiin niin hyvin kuin olisin toivonut. Luontevan dialogin puuttuminen ei tuonut esiin potentiaalisia vahvuuksiani.

Haastattelujen suhteen jäi melkoisesti parantamisen varaa: vain yhdeksän tilitoimistoa neljästäkymmenestä vastasi myöntävästi haastattelupyyntöön. Tutkimuksen otanta jäi siksi varsin suppeaksi, ja kenties tutkimuksen validiteetti kärsii tämän johdosta

Tarkentavia kysymyksiä olisi voinut esittää tilanteissa, joissa haastateltavan vastaukset jäivät laveaksi tai pahimmillaan epävarmoiksi, mikä jätti joissakin tapauksissa tulkinnanvaraisuuksia. Haastattelujen toteuttaminen kasvotusten antaisi paljon paremmat puitteet pohdiskelevaan, taustailmiöitä tarkentavaan tiedonkeruuseen ja analyysiin. Samaan lopputulokseen on kuitenkin mahdollista päästä muidenkin haastattelumetodien avulla, joten tässä tapauksessa kokemattomuus puhelinhaastattelujen toteuttamisesta käy selväksi, ja tässä olisi tutkijan osalta opeteltavaa, mikäli uusia akateemisia toimeksiantoja on tulevaisuudessa odotettavissa.

Toisaalta kysymysten puutteellisuus voidaan kenties nähdä positiivisena puutteena. Kysymyksen 17 puitteissa tiedusteltiin tilitoimistojen kyvystä varautua poikkeustilanteisiin, ja vaikka vastaukset saattavatkin jäädä vaatimattomiksi johtuen kysymyksenasettelusta tai haastattelijan kokemattomuudesta, nostaa tämä esille mielenkiintoisen idean potentiaalista uutta tutkimusta varten. Tilitoimistojen – tai muiden mikroyritysten – kriisinsietokyky/kyberkompetenssi digitaalisten ydintoimintojen keskeytyessä voisi olla seuraava luonnollinen vaihe tutkimuksen jatkoa ajatellen.

Toinen jatkotutkimuksen aihe voidaan kehitellä kybersuunnitelman/kyberstrategian käyttöönotosta mikrokokoisten yritysten parissa. Koska vain harva haastateltu yritys oli perehtynyt aiheeseen tai omaksunut kyber-

suunnitelman osaksi yrityksen toimintaa, on aihe selvästi ajankohtainen ainakin tilitoimistojen keskuudessa.

Tutkimuksen painopiste on alusta lähtien ollut haastateltavien tilitoimistojen kokemukset ja näiden omakohtaiset näkemykset kyberturvallisuudesta. Kyberturvallisuudesta on kirjoitettu satoja artikkeleita, kirjoja ja tutkimuksia, mutta viime kädessä koen kulloisenkin tutkimuksen kohderyhmän äänen olevan tuore ja mielenkiintoisempi. Luonnollisesti tämä on akateemisen tutkimuksen merkittävä painopiste yleisesti, mutta omassa työssäni tämä korostuu entisestään. Olen pyrkinyt kokemattomuudestani huolimatta avaamaan ja punnitsemaan annettuja vastauksia objektiivisesti ja antamaan tilitoimistojen äänelle riittävästi sijaa. Kenties otannan pienuus antaa siksi jokseenkin hyvin tilaa punnita ja analysoida eri vastauksia tarpeen mukaan.

Edellä mainittu seikka näkyy kenties merkittävimmin suppean teoriaosuuden/kirjallisuuskatsauksen muodossa, prioriteettien kallistuessa haastattelujen aineiston käsittelyyn. Kyberturvallisuutta koskeva osuus jää jokseenkin pinnalliseksi, mikä voi osaltaan johtua aihetta käsittelevän tutkittavan aineiston massiivisesta määrästä: kyberturvallisuudesta on kirjoitettu jo niin paljon, että lukijan on jo suositeltavaa perehtyä johonkin aihetta puivaan kirjaan tai artikkeliin ja ammentaa perustieto suoraan sieltä.

Tutkimuksen teoriaosuus kuitenkin onnistuu nähdäkseni tukemaan haastattelua, vertailukohtia haastattelun ja aiempien tutkimuksien välillä on mahdollista tehdä. Muun muassa toistuvuutta pienyritysten liiketoiminnan ja digitaalisen työskentelyn resurssiongelmista on havaittavissa.

Tutkimusmetodi kokonaisuudessaan vastasi odotuksia. Teemahaastattelu, vaikka olosuhteet ja kokemattomuus vaikuttivat osaltaan sen toteuttamiseen, osoittautui soveliaaksi tavaksi kerätä tietoa kohderyhmänä olevien yritysten omista kokemuksista kyberturvallisuuden saralla ja näkemyksistä toimintametodeistaan.

8 YHTEENVETO

Tilitoimistojen informaatioturvallisuus on äärimmäisen huomionarvoinen seikka. Kyberturvallisuuden soveltaminen paitsi takaa paremman suojan tietovarkauksia vastaan, myös luo pohjaa tehokkaammalle liiketoiminnalle.

Yleisellä tasolla kyberturvallisuuden suunnittelu ja toteuttaminen vaatii ymmärrystä internetin keskeisistä uhkakuvista sekä IT:hen ja organisaation liiketoimintaan kohdistuvista riskeistä. Tämä vaatii kattavan kyberturvallisuussuunnitelman toteuttamista, joka nojaa vahvasti haavoittuvuuksien kartoittamiseen ja sopivien vastatoimenpiteiden ja korjausliikkeiden kehittämiseen.

Valitettavasti pienyritysten kyberturvallisuudessa on jonkin verran korjaamisen varaa. Kyberiin liittyvät odotukset ja informaatio on monella yrityksellä heikolla tolalla, ja tiedon puute luo haavoittuvuuksia, joita opportunistinen hakkeri voi käyttää hyväkseen.

Kyberturvatietoisuuden kasvattaminen on siis arvokas ensiaskel, koska monet ongelmatekijät saataisiin ratkaistua jo soveliaalla valmennuksella. Pienyritys voi sikäli olla edullisessa asemassa, sillä pieni joukko työntekijöitä on teoriassa helpompi opettaa kyberturvallisuuden saloihin. Toisaalta kaikissa pienyrityksissä henkilökunta ei ole missään määrin yhtäläisen taitavaa tietotekniikan käytössä, joten yksilölliset erot on otettava huomioon.

Resurssipula on myös huomioitava tekijä, joka yhdistää monia pienyrityksiä ja joka on vaikeasti korjattavissa. Pienyritysten käytössä oleva pääoma on usein suhteellisen vähäinen verrattuna tehokkaan ja luotettavan tietojärjestelmän vaatimuksiin. Tämän korjaaminen vaatisi laajaa muutosta yritysten investointihalukkuuteen.

Lisäksi pienyritysten huomiota vievät liiketoiminnan muut osa-alueet, ja tätä pahentaa IT:n puolella vallitseva luottamus siihen, ettei oma yritys ole jatkossakaan rikollisten kohteena. Passiivisuus kostautuu helposti organisaatioille, jotka eivät ole aloitteellisia.

Tutkimuksen kohteena olevat mikrokokoiset tilitoimistot osoittavat edellä esitellyistä haasteista huolimatta lupaavia merkkejä kyberturvallisuuden ja sen toteutuksen ymmärtämisestä. Selkeää kompetenssia on havaittavissa, vaikka olosuhteet loisivatkin keskimääräistä huonommat puitteet aiheeseen perehty-

miseen. On sikälikin toivottavaa, että kyberturvallisuudesta kehkeytyy tulevaisuudessa yleisempi aihe yhteiskunnallisessa keskustelussa. Täten valveutuneisuus lisääntyisi ja sitä myöten myös yritykset hyötyisivät koko yhteiskunnan kattavan kompetenssin kehittymisestä.

LÄHTEET

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Akhgar, B., Staniforth, A., & Bosco, F. (Eds.). (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Saint Louis, US: Syngress.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 1-24.

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy, 224*(1), 75.

Barrie, J., & Pace, R. W. (1997). Competence, efficiency, and organizational learning. *Human Resource Development Quarterly*, *8*(4), 335.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security, 19*(5), 300-312.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology*, *8*(1), 1-20.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

Damenu, T. K., & Balakrishna, C. (2015). Cloud security risk management: A critical review. *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies* (370-375). IEEE.

Demir, N., Urban, T., Wittek, K., & Pohlmann, N. (2021). Our (in) Secure Web: Understanding Update Behavior of Websites and Its Impact on Security. In *International Conference on Passive and Active Network Measurement* (76-92). Springer, Cham.

Dhir, S., & Dhir, S. (2017). Adoption of open-source software versus proprietary software: An exploratory study. *Strategic Change*, *26*(4), 363-371.

Eling, M., McShane, M. & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125.

Falkner, E. M., & Hiebl, M. R. (2015). Risk management in SMEs: a systematic review of available evidence. *The Journal of Risk Finance*.

Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2021). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, 1-27.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7).

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, *2016*(6), 9-10.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

Hayes, J., & Bodhani, A. (2013). Cyber security small firms under fire [InformatIon Technology Professionalism]. *Engineering & Technology, 8*(6), 80-83.

Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Iguer, H., Medromi, H., Sayouti, A., Elhasnaoui, S., & Faris, S. (2014). The impact of cyber security issues on businesses and governments: A framework for implementing a cyber security plan. *2014 International Conference on Future Internet of Things and Cloud*, 316-321. IEEE.

Jain, J., & Pal, P. R. (2017). A recent study over cyber security and its elements. *International Journal of Advanced Research in Computer Science*, *8*(3), 791-793.

Järvinen, P. & Rousku, K. (2017). *Työpaikan tietoturvaopas: Tunnista uhat, hallitse riskit*. Helsinki: Alma Talent.

Karjalainen, M. (2010). *Large-scale migration to an open source office suite: An innovation adoption study in Finland*. Tampere University Press.

Kettunen, J., Vuori, J., tutkimuslaitos, K. & Research, F. I. f. E. (2021). *Fenomenografia*. Yhteiskuntatieteellinen tietoarkisto.

Kizza, J. M. k. (2013). *Guide to Computer Network Security (2nd ed. 2013.)*. Springer London.

Kleij, R. V. D., & Leukfeldt, R. (2019). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *International conference on applied human factors and ergonomics* (16-27). Springer, Cham.

Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533-7538.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5-7.

Lehto, M., Neittaanmäki, P., Lehto, M., Kuusisto, T., Ollila, R., Ottis, R., . . . Kiperberg, M. (2015). *Cyber security: Analytics, technology and automation*. Springer International Publishing.

Leskinen, T. (2021). Etätyö yleistyi eniten aloilla ja alueilla, joilla sitä ennen tehtiin vähiten. *Tieto & Trendit.* Haettu 23.3.2022 osoitteesta https://www.tilastokeskus.fi/tietotrendit/artikkelit/2021/etatyo-yleistyi-eniten-aloilla-ja-alueilla-joilla-sita-ennen-tehtiin-vahiten/

Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.

Lowe, M. (2014). Defending against cyber-criminals targeting business websites. *Network Security*, *2014*(8), 11-13.

Maayan, G. D. (2019). The Dangers of Open-Source Vulnerabilities, and What You Can Do About It. *Security Today.* Haettu 28.3.2022 osoitteesta https://securitytoday.com/Articles/2019/08/19/The-Dangers-of-OpenSource-Vulnerabilities-and-What-You-Can-Do-About-It.aspx

MacDonald, D., Clements, S. L., Patrick, S. W., Perkins, C., Muller, G., Lancaster, M. J., & Hutton, W. (2013, February). Cyber/physical security vulnerability assessment integration. *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-6). IEEE.

Mandritsa, I. V., Peleshenko, V. I., Mandritsa, O. V., Fensel, A., Tebueva, F. B., Petrenko, V. I., ... & Mecella, M. (2018). Defining a cybersecurity strategy of an organization: criteria, objectives and functions. *В сборнике: Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe*,199-205.

Microsoft (2014). *Don't be exposed when support for Windows XP Ends on April 8 2014.* Haettu 30.3.2022 osoitteesta https://news.microsoft.com/en-hk/2014/03/09/20140310/

Min, K. S., Chai, S. W., & Han, M. (2015). An international comparative study on cyber security strategy. *International Journal of Security and Its Applications*, *9*(2), 13-20.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *Sage Open*, *5*(2), 2158244015580372.

Osborn, E., & Simpson, A. (2015). Small-scale cyber security. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing,* 247-252. IEEE.

Parkin, S., Fielder, A., & Ashby, A. (2016). Pragmatic security: modelling IT security management responsibilities for SME archetypes. *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, 69-80.

Parkkari, J. (2017). Kolme miljardia Yahoon käyttäjätiliä todennäköisesti hakkeroitiin 2013. *Yle Uutiset 4.10.2017.* Haettu 28.3.2022 osoitteesta https://yle.fi/uutiset/3-9864859

Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). A detailed review of Cloud Security: Issues, Threats & Attacks. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA),* 758-764. IEEE.

Poliisi. (2020). *Petosrikokset.* Haettu 11.4.2022 osoitteesta https://poliisi.fi/petosrikokset

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253-259. IEEE.

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017). A state of the art survey-Impact of cyber attacks on SME's. *Proceedings of the International Conference on Future Networks and Distributed Systems*.

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica*, *16*(2), 58-71.

Schryen, G. (2011). Is open source security a myth?. *Communications of the ACM*, *54*(5), 130-140.

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, 1-5. IEEE.

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *The 16th International Conference on Availability, Reliability and Security*, 1-7.

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. No Starch Press.

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber security in social media: challenges and the way forward. *IT Professional*, *21*(2), 41-49.

Thompson, R. (2014). The small business cybersecurity blindspot. *Risk Management, 61*(5), 8-9.

Tilastokeskus. *Käsitteet.* Haettu 30.3.2022 osoitteesta https://www.stat.fi/meta/kas/index.html

Tilastokeskus (2020). Yritykset toimialoittain (yritysyksikkö) 2017-2020. *Tilastokeskuksen maksuttomat tilastotietokannat.* Haettu 1.4.2022 osoitteesta https://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin__yri__yrti__yri/statfin_yrti_pxt_11d5.px/table/tableViewLayout1/

Toulas, B. (2021). It's Windows XP's 20th birthday and way too many still use it. *Bleeping Computers.* Haettu 30.3.2022 osoitteesta https://www.bleepingcomputer.com/news/microsoft/its-windows-xps-20th-birthday-and-way-too-many-still-use-it/

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Turvallisuuskomitea. (2019). *Suomen kyberturvallisuusstrategia* [sähköinen tietoaineisto]. Haettu 31.3.2022 osoitteesta: https://turvallisuuskomitea.fi/wp-

content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Turvallisuuskomitea. (2018). *Kyberturvallisuuden sanasto* [sähköinen tietoaineisto]. Haettu 20.3.2022 osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *The 16th International Conference on Availability, Reliability and Security*, 1-12.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

Wangen, G. (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*, *6*(2), 183-211.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. Sage.

Yrittäjät. (2021). *Yrittäjyystilastot* [sähköinen tietoaineisto]. Haettu 31.3.2022 osoitteesta https://www.yrittajat.fi/wp-content/uploads/2021/07/yritttajyystilasto_2021_su.pdf

Yrittäjät. (2020). *Pk-yritysbarometri. Syksy 2020* [sähköinen tietoaineisto]. Haettu 31.3.2022 osoitteesta https://www.yrittajat.fi/wp-content/uploads/2021/09/pk-yritysbarometri_syksy_2020_vk_kalvosarja.pdf

Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014). The dark alleys of madison avenue: Understanding malicious advertisements. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (pp. 373-380).

LIITE 1 TILITOIMISTOJEN HAASTATTELUT – VASTAUKSET

1. **Kuinka monta henkilöä työskentelee yrityksessänne?**
    - 2
    - 5
    - 5
    - 7
    - 2
    - 5
    - 2
    - 5 (4 kokoaikaista, 1 osa-aikainen)
    - 4 (2 päätoimista, 1 harjoittelija, 1 osa-aikainen harjoittelija)
2. **Mikä on teidän (vastaajan) asema yrityksessä?**
    - Yrittäjä/omistaja
    - Yrittäjä
    - Toimitusjohtaja
    - Yrittäjä
    - Toimitusjohtaja
    - Yrittäjä/omistaja
    - Yrittäjä/omistaja
    - Toimitusjohtaja
    - Toimitusjohtaja
3. **Nojaako yrityksenne työnteko pääsääntöisesti tietokoneisiin ja digitaalisiin laitteisiin ts. onko digitalisaatiolla ollut selkeä vaikutus yrityksenne toimintaan?**
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
    - Kyllä
4. **Miten määrittelette termin ”kyberturvallisuus”?**
    - Tietoverkoissa tapahtuva suojaus

- Yleinen tietoturva, mm. palomuurit ja virustorjunta
- Tietoturvaan liittyvät yleiset seikat
- Digitaalisesti välittyvän tiedon turvallisuuden takaaminen
- Kattaa yleisesti mm. virustorjunnan ja palomuurit, henkilötietojen koskemattomuuden, verkkohuijaukset
- Oletusarvoisesti (verkossa olevat) tiedostot /materiaali on suojassa väärinkäytöksiltä
- Tietokoneiden ja internetin kautta tuleva uhka, huijaripuhelut
- Yleisesti sähköinen turvallisuus, kattaa tietojen turvaamisen, tärkeän datan käsiksi pääsemisen estämisen ulkopuolisilta, laitteiden hajoamiseen liittyvät uhkatekijät
- Olosuhteet, joissa kukaan vieras/ulkopuolinen taho ei pääse digitaalisiin tietoihin käsiksi

5. **Kuka yrityksessänne huolehtii tietoturvasta?**
    - Yrittäjä itse, ohjelmistojen kohdalla ohjelmiston tarjoaja
    - Ulkoinen it-tuki ostopalveluna
    - Toimitusjohtaja itse
    - Kaikki työntekijät yhteisesti, yrittäjä vastuuhenkilö
    - Toimitusjohtaja itse
    - Yrittäjä/omistaja itse
    - Päävastuu yrittäjällä, atk-alan yritys hoitaa varsinaiset toimet.
    - Toimitusjohtaja vastuussa
    - Toimitusjohtaja itse
6. **Onko yrityksenne ulkoistanut IT-tuen tai tietoturvan toteutuksen jollekin ulkoiselle taholle?**
    - Ei yksittäiselle taholle, kutakin ongelmaa varten järjestetään tarpeen tullen sopiva ammattilainen avuksi
    - Kyllä
    - Ei pysyvästi, mutta tarpeen mukaan turvaudutaan ulkoiseen apuun.
    - Atk-tukihenkilö auttaa tarvittaessa.
    - Yritys kustantanut maksullisen virustorjunnan firman koneille
    - Ei
    - Kyllä, atk-alan yritykselle
    - Kyllä

- Verkkosivujen tietoturva ulkoistettu mainostoimistolle, operaattori hoitaa sähköpostin tietoturvan, maksullinen virustorjuntapalvelu, ohjelmien tallennustila pilvipalveluissa

7. **Onko yrityksenne henkilökunnalla koulutusta tietoturvan saralla?**
   - Ei ole
   - Ei ole
   - Ei varsinaisesti
   - Peruskoulutusta kyllä, muttei mitään erikoisosaamista
   - Ei oikeastaan, joskin keskustelua aiheesta käydään yrityksen sisällä
   - Ei
   - Ei
   - Ei varsinaisesti, yrityksen sisällä on käyty teemaa yhdessä läpi
   - Ei, toimitusjohtaja perehdyttää yleiset käytänteet
     a. **Jos on, järjestetäänkö tämän tiimoilta säännöllistä jatkokoulutusta?**
        - –
        - –
        - –
        - Ei
        - –
        - –
        - –
        - –
        - –
8. **Onko yrityksenne ostanut tietojärjestelmiä, -ohjelmia ja/tai -palveluita (lisenssit)?**
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
   - Kyllä
     a. **Jos on, huolehtivatko näiden palveluiden tarjoajat ohjelmistojen tms. toiminnasta ja päivityksestä?**

- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä

b. Käyttääkö yrityksenne ilmaisia vaihtoehtoja?

- Ei
- Ei
- Ei
- Ei
- Kyllä
- Ei
- Ei
- Kyllä
- Ei omassa liiketoiminnassa, tarjoaa ilmaista palkanlaskentaohjelmaa asiakkaille

9. Miten määrittelette termin ”tietoturvariski”?

- Heikko lenkki tietoturvassa
- Potentiaalinen tietojärjestelmiin kohdistuva vaara
- Verkon kautta tapahtuvat (tieto)varkaudet
- Suojaamaton pääsy henkilötietoihin
- Arkaluontoisiin tietoihin käsiksi pääseminen
- Käsiteltävien tietojen päätyminen ulkopuolisille, joten varmistutaan että tieto käsitellään oikein
- Hahmotetaan salassa pidettävät tiedot, ja miten tietoa voidaan jakaa ja säilyttää turvallisesti
- Heikko tietoturvan suojaustaso yleisesti, tietojen vuotaminen esim. varomattomuuden takia
- Esim. sähköpostin tai henkilötietojen päätyminen vääriin käsiin tai verkkovakoilu

10. Onko yrityksellänne mielestänne ilmeisiä tietoturvariskejä, joihin pitäisi puuttua?

- Samat salasanat käytössä useissa palveluissa
- Ei ilmeisiä riskejä

- Koneiden ja laitteiden salasanasuojaus.
- Fyysinen tai digitaalinen murtautuminen yrityksen tietoihin
- Ei
- Ei
- Ei
- Ei
- Oma valppaus kaikista tärkein elementti, esim. virheellinen sähköpostin lähetys voi aiheuttaa riskin

11. Onko yrityksellänne selkeätä tietoturvasuunnitelmaa?

- Ei
- Kyllä
- Ei
- Ei
- Ei
- Ei
- Ei, tosin keskustelua tietoturvasta käydään yrityksen sisällä
- Ei
- Kyllä: poikkeavat tapahtumat kirjataan ylös, mitään työtehtäviä ei tehdä omalla koneella, suojattu tiedonvälitys arkaluontoisen tiedon suhteen
  - **a. Jos on, milloin se on kehitetty, ja päivitättekö sitä säännöllisesti?**
    - –
    - Alle kaksi vuotta sitten, ei säännöllistä päivitystä
    - –
    - –
    - –
    - –
    - –
    - –
    - Parin viime kuukauden sisällä, kyllä päivitetään ja tietoa jaetaan yrityksen sisällä
  - **b. Jos ei, aiotteko kehittää sellaisen tulevaisuudessa?**
    - Ei ole ollut suunnitelmissa, ei varmuutta mitä se pitäisi sisällään
    - –
    - On tarvetta, joten mahdollisesti
    - Voi olla tarvetta

    - Voi olla tarvetta
    - Ei
    - Ei näin pienellä henkilökunnalla
    - Ei, paitsi mikäli henkilöstön koko kasvaa tulevaisuudessa
    - –

12. Onko yrityksenne toimintaa varten luotu suljettu yksityinen lähiverkko?

- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Ei
- On
- On
- Kyllä
- Kyllä

13. Onko työpaikkanne verkkoon yhteydessä laitteita, joita ei käytetä työntekoon?

- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei

14. Kuinka usein päivitätte käytössänne olevia laitteita tai ohjelmia?

- Ohjelmat pilvessä, päivittyvät automaattisesti
- Ohjelmat päivittyvät aktiivisesti, laitteiden uusiminen muutaman vuoden välein
- Palveluntarjoajan suositusten mukaisesti
- Päivittyvät automaattisesti
- Päivittyvät automaattisesti
- Yleensä ohjelmat/laiteet päivittyvät automaattisesti, muutoin satunnaisesti.

- Ohjelmistot päivittyvät automaattisesti, muutoin harvoin
- Päivittyvät pääsääntöisesti automaattisesti.
- Päivittyvät pääsääntöisesti automaattisesti

15. Käytättekö paljon ulkoisia (muisti)laitteita (puhelimet, ulkoiset USB-kiintolevyt jne.) tiedostojen siirtämisessä koneelta toiselle?

- Ei, tiedostojen siirto tapahtuu pääsääntöisesti pilviympäristössä
- Ei, tiedostojen siirto tapahtuu pääsääntöisesti pilviympäristössä
- Ei, tiedostojen siirto tapahtuu pääsääntöisesti pilviympäristössä
- Ei, tiedostojen siirto tapahtuu pääsääntöisesti pilviympäristössä
- Kyllä, erityisesti varmuuskopioinnin yhteydessä
- Ei
- Hyvin vähän, vain työpaikan käyttöön tarkoitetut muistitikut.
- Vain varmuuskopioinnin yhteydessä.
- Ei

16. Onko työpaikallanne käytössä webkameroita tai mikrofoneja?

- On
- On mikrofoneja
- On
- Kyllä
- Ei
- Ei
- On mikrofoni.
- Ei
- On mikrofoni
  - **a. Jos on, ovatko ne oletusarvoisesti toimintavalmiudessa?**
    - Ei
    - Eivät, kytketään päälle tarvittaessa
    - Kyllä
    - Kyllä
    - –
    - –
    - Ei
    - –

    - Kyllä

17. Onko yrityksenne varautunut tilanteisiin, joissa ette pysty käyttämään tietojärjestelmiä tai Internetiä?

- Ei ole
- Laajakaistakatkoja varten on olemassa mobiilivaihtoehtoja internetyhteyden säilyttämiseksi
- Laajakaistakatkoja varten on olemassa mobiilivaihtoehtoja internetyhteyden säilyttämiseksi
- Mobiilinetin saa nopeasti laajakaistan tilalle
- Kirjanpitojärjestelmä ei riippuvainen internetistä, joten verkkokatkokset eivät haittaa toimintaa
- Ei oikeastaan, mobiiliverkko toimii kiinteän laajakaistan ohessa
- Ei oikeastaan
- Kaikki työskentely ei ole internetin varassa, verkkoyhteyden takaamiseksi löytyy varajärjestelmä
- Ei, joskin joskus ollut varalla mobiilinetti
    - **a. Onko kyseisiä tilanteita tullut vastaan?**
        - Korkeintaan itsestä riippumattomat sähkökatkokset
        - Valokuitu ja palveluntarjoaja ovat aiemmin aiheuttaneet ongelmia
        - Ajoittain valokuituyhteys on katkennut
        - Lähiverkko on aiemmin kaatunut
        - Ei
        - Kiinteä verkko on saattanut kaatua hetkeksi
        - Ei
        - Ei
        - Kyllä
    - **b. Jos vastaava tilanne on tapahtunut, kuinka kauan tilanteen korjaaminen keskimäärin vei?**
        - –
        - Laajakaista pari tuntia poikki, ohjelmistokatkot kestäneet jopa puolitoista päivää
        - Mobiiliverkkoon vaihtaminen ei vie kauaa, muussa tapauksessa riippunut pitkälti laajakaistapalveluntarjoajasta
        - Laajakaistayhteyden palauttaminen vei pari päivää
        - –

    - Muutaman minuutin
    - –
    - –
    - 1-2 tuntia korkeintaan

18. Onko yrityksenne varautunut laitteistoihinne kohdistuviin fyysisiin ongelmatilanteisiin, esim. hajoaminen tai varkaudet?

- Tärkeät tiedot ovat pilvessä, joten laitteiden hajoaminen ei hävitä tärkeitä tietoja
- Tärkeät tiedot ovat tallennettuna pilveen
- Ei juurikaan, tärkeät tiedot tallennettuna pilvessä
- Tärkeät tiedot tallennettuna pilvipalveluihin, atk-tukihenkilö auttaa hajoamistilanteissa
- Liikekiinteistössä kamerat, paikat lukitaan tiukasti, tärkeistä tiedostoista varmuuskopiot
- Kyllä, hälytysjärjestelmät ja kamerat varkauksien ehkäisemiseksi
- Tärkeä data on tallessa pilvipalveluissa
- Varmuuskopiointi huolehtii tietojen säilymisen, tärkeät tiedot ovat salasanoilla suojattu
- Vakuutus kattaa vahingot, varmuuskopiointi tallentaa tärkeät tiedot
    a. **Onko yrityksenne tietojärjestelmistä ja tiedoista olemassa kattavat varmuuskopiot ja säännöllinen varmuuskopiointi?**
        - Kyllä, pilvipalvelut suorittavat varmuuskopioinnit
        - Kyllä, pilvipalvelut suorittavat säännöllisen varmuuskopioinnin
        - Kyllä, pilvipalvelujen kautta
        - Kyllä, pilvipalvelujen kautta
        - Kyllä, viikoittain ulkoisille kovalevyille
        - On, pilvipalvelujen kautta
        - Kyllä, pilvessä
        - Kyllä
        - Kyllä pilvipalvelujen toimesta

19. Tekeekö yrityksenne henkilökunta usein töitä kotoa käsin?

- Kyllä
- Ei usein
- Kyllä

- Normaalioloissa ei juurikaan, poikkeusoloissa kyllä
- Toimitusjohtaja tekee kyllä
- Silloin tällöin
- Ei pääsääntöisesti, mutta jonkin verran
- Normaalisti ei, poikkeusoloissa kyllä
- Kyllä yrityksen kannettavilla tietokoneilla
  - **a. Jos tekee, miten työntekijät huolehtivat tietoturvan ylläpitämisestä työpaikan ulkopuolella?**
    - Kaikki työn kannalta tärkeä on salasanojen takana
    - Työskentely tehdään toimiston koneilla
    - Oman kotiympäristön tarjoamissa puitteissa
    - yrityksen yhteisiä sääntöjä noudattaen, kaikilla työntekijöillä oletusarvoisesti jonkin tasoinen virustorjunta
    - Virustorjunta löytyy, kaikki tärkeä on salasanojen takana, vieraat eivät pääse käsiksi työkoneeseen
    - Työntekoon käytetään pilvipalvelujen/sähköpostin salaamia ja turvaamia materiaaleja.
    - Työntekoon käytetään vain yrityksen omaa kannettavaa tietokonetta
    - Ei ole tietoa, koska ei ole vakiintunut tapa
    - Kodin tietokoneita ei käytetä, erilliset työpuhelimet, suunnitelmissa fyysisistä asiakirjoista luopuminen etätyöskentelyssä
  - **b. Onko kotona työskentelyä varten olemassa oma tietoturvasuunnitelma?**
    - Ei erillistä suunnitelma
    - Ei
    - Ei
    - Ei
    - Ei
    - Ei
    - Samat säännöt pätevät kuin toimistolla
    - Ei
    - Ei, sama kuin työpaikalla
  - **c. Onko työntekijöillä käytössä kattava tietoturvajärjestelmäpaketti kotona?**
    - Virustorjuntaohjelman omat palvelut
    - –

  - –
  - –
  - Sama kattava virustorjunta kuin toimistolla
  - Ei oletusarvoisesti
  - Sama kattava tietoturvapaketti kuin toimistolla
  - Yrityksen koneissa kyllä
  - Laaja maksullinen virustorjunta

20. Teettekö tärkeitä/luottamuksellisia työtehtäviä mobiililaitteilla?

- Kyllä
- Kyllä
- Ei
- Hyvin vähän
- Ei
- Hyvin harvoin
- Ei
- Ei
- Ei asiakkaisiin liittyviä töitä, oman yritykseen liittyviä töitä kyllä

21. Miten toimitte fyysisen tiedostomateriaalin (esim. tulosteet) tietoturvan kanssa? Arkistointi, säilytys, luottamuksellisuuden takaaminen?

- Toimisto lukittu, fyysinen materiaali lukituissa kaapeissa
- Kaikki arkistoidaan, mitään ei julkisesti esillä, asiakas saa tilikauden jälkeen henkilökohtaisen materiaalin takaisin
- Vuodesta 2015 alkaen sähköinen arkistointi, lukot kaapeissa, rajoitettu pääsy ulkopuolisilta
- Hävitetään tietoturvapalvelujen toimesta, dokumentit eivät muiden nähtävillä, henkilökohtainen materiaali palautetaan asiakkaalle
- Hävitetään tietoturvapalvelujen toimesta
- Tärkeimmät materiaalit käsitellään pilvessä, harvat tulosteet poltetaan
- Säilytetään lukkojen takana lukitussa huoneessa
- Toimiston ovet aina lukossa, paperit ovat kaapeissa piilossa ulkopuolisilta, kansiot numeroidut eivätkä nimeä asiakkaita, jos henkilökohtaisia dokumentteja ei palauteta asiakkaalle niin ne päätyvät tietosuojaroskiin

- Asiakirjat eivät lukitussa kaapissa, mutta toimiston ovet pidetään lukittuina aina kun ketään ei ole paikalla

22. Miten yrityksenne hävittää tarpeettoman mutta arkaluontoisen/salassa pidettävän materiaalin?

- Sijoitetaan lukolliseen tietosuojasäiliöön
- Paperidokumentit silputaan
- Paperidokumentit silputaan
- Tietoturvapalvelut hävittää ne
- Tietoturvapalvelut hävittää ne
- Tulosteet poltetaan, kovalevyissä ei säilytetä mitään tärkeää
- Paperit hävitetään paperisilppurilla, kerran vuodessa annetaan jätehuollon käsittelyyn
- Päätyvät tietosuojaroskiin ja sitä kautta hävitettäväksi
- Vanhat asiakirjat poltetaan
  - **a. Entä vanhat ja tarpeettomat laitteet?**
    - Hajotetaan perinpohjaisesti
    - Luovutetaan atk-tuelle hävitettäväksi
    - Hävitetään, kovalevyt säilytetään tallessa
    - Atk-tuki hoitaa turvallisen hävittämisen
    - Kovalevyt hajotetaan itse, muut koneet asiallisiin keräyspisteisiin
    - Toimitetaan asiaankuuluville vastaanottopaikoille, tietokoneiden kovalevyt irrotettuna
    - Ei ole ollut tarvetta hävittää
    - Viedään standardoidulle toimijalle purettavaksi ja hävitettäväksi
    - Ei ole vielä suunnitelmaa niiden varalle, oletettavasti tullaan tyhjentämään tiedoista ja annetaan hävitettäväksi

23. Onko työntekijöillänne yhtäläiset oikeudet kaikkiin tietojärjestelmänne tietoihin?

- Ei
- Ei
- Kyllä lähes kaikkiin
- Ei aivan, oikeudet myönnetään työntekijän roolituksen mukaan
- Pääosin on
- Ei täysin kaikkiin

- Ei
- Ei
- Ei

24. Miten työntekijänne suojaavat salasanoja ja käyttäjätietojaan?

- Kullakin omat tunnukset ja salasanat, joita säilytetään erillään muista
- Kullakin omat salasanat, joita säilytetään erillään muista
- Kullakin omat salasanat, joita ei kirjata ylös
- Tallennetaan turvallisesti salasanojen hallinta- ja tallennusohjelmaan
- Oma salasana tallessa hallinnoivan ohjelman suojissa, toisen työntekijän käyttäjätietoja ei jaeta
- Yhtäläinen sähköpostisalasana iskostetaan muistiin, pääohjelmiin kirjaudutaan vahvalla tunnistautumisella, salasanojen turvallinen säilöntä turvallisella hallintaohjelmalla
- Kullakin omat henkilökohtaiset salasanat
- Osa itse kunkin ulkomuistissa, osa tallessa varmassa paikassa
- Kukin säilyttää omassa muistissa, toimitusjohtaja säilyttää lukitussa tilassa

a. Onko yrityksessänne käyttäjätunnukset tai salasanat jossain fyysisesti näkyvillä?

- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei

b. Kuinka usein päivitätte salasanoja?

- Hyvin harvoin
- Ohjelmistojen salasanat 100 päivän välein, mobiilitunnisteita vaativia salasanoja ei päivitetä
- Harvoin
- Ohjelmiston/laitteen muistutuksen mukaan
- Harvoin

    - Sähköpostin automaattinen muistutus kolmen kuukauden välein
    - Muutaman kerran vuodessa tai ohjelmien suositusten mukaisesti
    - Käytetään paljon vahvaa tunnistautumista, useamman laitteen kirjautumismetodeja
    - Ei säännöllisen usein, osassa toimintaa on käytössä vahva tunnistautuminen

25. Onko yrityksenne käytössä pilvipalveluita?

- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
    - **a. Jos on, miten huolehditte näiden tietoturvasta?**
        - Palveluntarjoaja huolehtii
        - Palveluntarjoaja huolehtii
        - Palveluntarjoaja huolehtii
        - Palveluntarjoaja huolehtii
        - Pilvipalveluihin ei mitään arkaluontoista/arvokasta dataa, luotetaan pilvipalvelun omaan tietoturvaan
        - Ohjelmantoimittajat hoitavat tietoturvan
        - Palveluntarjoajat hoitavat sen
        - Palveluntarjoaja huolehtii
        - Palveluntarjoaja huolehtii

26. Turvaudutteko tietojenkäsittelyssä ulkopuolisiin toimijoihin?

- Ei, yritys hoitaa itse
- Ei, yritys hoitaa itse
- Ei, yritys hoitaa itse
- Atk-tuki auttaa tarvittaessa, toiminnanohjauspalvelut hankittu
- Ei
- Ainoastaan pilvipalveluiden kautta
- Ei
- Ei

- Ei

27. Onko yrityksellänne kotisivuja?

- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä
- Kyllä

a. Jos on, annatteko julkaista sivustollanne mainoksia?

- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei
- Ei

b. Milloin olette viimeksi päivittäneet kotisivunne?

- Ei muista
- Noin kaksi vuotta sitten
- Pari vuotta sitten
- Viikko sitten
- Kolme viikkoa sitten
- Vuosi sitten
- Hyvin harvoin on tarvetta tälle
- Kolme vuotta sitten
- Pari viikkoa sitten

c. Onko sivustollanne paljon linkkejä ja/tai yhteystietoja, joita voi kopioida?

- Ei ole
- Ei
- Ei ole
- Ei ole
- Ei

- Ei
- Ei
- Ei
- Ei

d. Onko domainninne tarjoaja maksullinen toimija vai ilmaisen verkkotunnuksen tarjoava taho?

- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija
- Maksullinen toimija

28. Saatteko sähköpostin kautta usein roskapostia?

- Ei
- Ei
- Kyllä
- Jonkin verran
- Kyllä
- Ei
- Hyvin vähän
- Jonkin verran
- Ei juurikaan

29. Toimiiko yrityksenne aktiivisesti sosiaalisessa mediassa?

- Ei kovinkaan aktiivisesti
- Ei kovinkaan aktiivisesti
- Hyvin vähän
- Hyvin vähän
- Ei
- Ei aktiivisesti
- Ei
- Ei
- Hyvin vähän

30. Käytättekö työpaikkanne laitteita muuhun kuin työntekoon, esim. yksityisten asioiden hoitamiseen?

- Kyllä

- Kyllä
- Kyllä
- Harvoin
- Toimiston koneita ei, henkilökohtaista konetta kyllä
- Hyvin vähän
- Harvakseltaan
- Jonkin verran
- Ei

31. Minkä miellätte tällä hetkellä tärkeimmäksi digitalisaation aiheuttamaksi uhkatekijäksi?

- Yleinen riippuvuus internetistä
- Identiteettivarkaudet
- Asiakkaisiin kohdistuvat tietomurrot
- Etänä toteutettavat tietomurrot
- Hakkerit ja kyberrikollisuuden
- Mahdolliset verkon kautta ilmenevät hyökkäykset/kaappaukset/virukset
- Verkossa ilmenevät huijaukset, joihin liittyen tarvitaan enemmän tietoisuutta/varovaisuutta
- Identiteettitietojen vuodot
- Digitaalisen tiedon/työkalujen/asiakastietojen yhtäkkinen katoaminen tai käytön estyminen

32. Onko yrityksenne joutunut kyberrikollisuuden tai hakkeroinnin kohteeksi?

- Ei ole tiedossa että olisi
- Kyllä
- Kyllä
- Kyllä
- Ei
- Ei tiedostetusti
- Ei tiedostetusti
- Ei tietoisesti
- Ei
    - **a. Mihin isku(t) on kohdistunut?**
        - –
        - Kotisivuihin ja työsähköpostiin.
        - maksukortin tiedot hakkeroitu

- Työntekijöiden sähköpostiosoitteita käytetty huijausviestien lähettelyyn yrityksen sisällä
- –
- –
- –
- –
- –

b. Koitteko taloudellisia tappioita tämän/näiden takia?

- –
- ei
- kyllä
- ei
- –
- –
- –
- –
- –

c. Miten ratkaisitte hakkeroinnin aiheuttamat ongelmat?

- –
- Kotisivut ja palveluntarjoaja vaihtoon.
- Luottoyhtiön ja pankin kautta kortti jäihin ja uusi tilalle, menetykset saatiin korvattua
- Jättämällä huijarin viestit huomiotta, jolloin tämä lopetti pian
- –
- –
- –
- –
- –