LAB University of Applied Sciences

Suomalaisten mikroyrittäjien käsitykset tieto-turvariskeistä

LAB-ammattikorkeakoulu
Tradenomi (AMK)
2022
Kati Palm

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Palm, Kati	Opinnäytetyö, AMK	2022
	Sivumäärä	
	35	

Työn nimi

Suomalaisten mikroyrittäjien käsitykset tietoturvariskeistä

Tutkinto ja koulutusala

Tradenomi (AMK), Tietojenkäsittely

Toimeksiantajan nimi, titteli ja organisaatio

Avosorsa Oy

Tiivistelmä

Työssä tutkittiin suomalaisten mikroyrittäjien käsityksiä tietoturvariskeistä ja mihin tietoturvariskeihin heidän olisi hyvä kiinnittää huomiota enemmän. Työn tavoitteena oli saada suomalaiset mikroyrittäjät ymmärtämään tietoturvan merkitys yritystoiminnassa ja minkälaisia tietoturvariskejä on olemassa. Työn toimeksiantajana toimi suomalainen mikroyritys, Avosorsa Oy.

Tutkimusmenetelmänä käytettiin laadullista tutkimusta ja aineisto kerättiin teemahaastatteluilla. Haastateltavana oli 10 suomalaista mikroyrittäjää. Haastattelut antoivat runsaasti tietoa mikroyrittäjien tietoturvan käsityksistä sekä tietoturvariskien tunnistamisesta. Mikroyrittäjien lisäksi haastateltiin kuutta asiantuntijaa, jotka antoivat ajankohtaisia näkemyksiä ja tulevaisuuden trendejä tietoturvan ja tietoturvariskien suhteen.

Työn tuloksena todettiin suomalaisten mikroyrittäjien käsitykset tietoturvariskeistä olevan niukat ja keskittyvän enemmänkin jokapäiväisten toimintojen ympärille.

Asiasanat

Tietoturva, tietoturvariski, mikroyrittäjä

Abstract

Author(s)	Type of Publication	Published
Palm, Kati	Thesis, UAS	2022
	Number of Pages	
	35	

Title of Publication

Finnish micro entrepreneurs' perceptions of information security risks

Degree and field of study

Bachelor of Business Administration, Information Technology

Name, title and organisation of the client

Avosorsa Ltd

Abstract

The work explored the Finnish micro entrepreneurs' perceptions of information security risks and what information security risks they should pay more attention to. The aim of the work was to get Finnish micro entrepreneurs to understand the importance of information security in business and what kind of information security risks exist. As an operator at this work was a Finnish micro enterprise, Avosorsa Oy.

As a research method, qualitative research was used, and the material was collected with theme interviews. The interviewee had 10 Finnish micro entrepreneurs. Interviews gave a lot of information on the concepts of information security and identifying information security risks. In addition to micro entrepreneurs', six experts were interviewed, which provided topical views and future trends in relation to information security and information security risks.

As a result, the perceptions of Finnish micro entrepreneurs were found to be scarce for information security risks and concentrating more around everyday activities.

Keywords

Information security, information security risk, micro entrepreneur

Sisällys

Liitteet

1 Johdanto

1.1 Opinnäytetyön aihe ja tausta

Tässä opinnäytetyössä selvitetään suomalaisten mikroyrittäjien käsityksiä tietoturvariskeistä ja mitä tietoturvariskejä heidän olisi hyvä huomioida enemmän. Aihevalinnassa on kiinnitetty huomioita tietoturvan merkitykseen, toimialasta riippumatta, uutisoinnin ja mediassa ilmenevien keskusteluiden pohjalta. Nykyisin yhteiskunnan, henkilöiden ja yritysten on mahdoton toimia ilman teknisiä järjestelmiä ja toimintaedellytykset riippuvat siitä, kuinka hyvin nämä voidaan turvata (Limnéll ym. 2014, 95, 106). Lisäksi aihevalintaan on vaikuttanut toimeksiantajan havainnot, tutkijan kiinnostus aiheeseen sekä tutkimukseen tarvittavan materiaalin saatavuus ja pätevyys. Aihevalinnassa on otettu myös huomioon tutkimustuloksen hyödynnettävyys.

Tietoturva on ajankohtainen aihe jatkuvasti muuttuvassa toimintaympäristössä ja tietoturvaan liittyvien riskien yleistyessä. Yhteiskunnan digitalisaatio, sekä työn ja yksityiselämän yhdistämisen luoma niin sanottu hybriditila, osaltaan tuo tietoturvaan ja tietoturvariskien havainnointiin uusia ulottuvuuksia. Mitä enemmän työympäristö siirtyy hybriditilaan, sitä suuremmiksi riskit muodostuvat (Limnéll ym. 2014, 107).

Tutkimus tullaan rajaamaan tietoturvan määritelmään, joka kertoo tietoturvan olevan tiedon luotettavuuden, eheyden ja saatavuuden ylläpitoa (Liikenne- ja viestintävirasto Traficom 2020). Lisäksi tutkimuksen aikana tullaan käsittelemään tietoturvan osa-alueita, joita ovat: Hallinnollinen tietoturva, fyysinen tietoturva, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus, tietoliikenneturvallisuus, henkilöstöturvallisuus ja käyttöturvallisuus. (Andreasson ym. 2013, 52.) Tutkimuksessa ei tulla ottamaan kantaa lainsäädäntöihin tai asetuksiin, koska tutkimus käsittelee puhtaasti suomalaisten mikroyrittäjien käsityksiä tietoturvariskeistä.

Oma kiinnostukseni tietoturvaa kohtaan on syventynyt viimeisten vuosien aikana, sekä työni puolesta, että yksityiselämässäkin. Havaintojeni mukaan on mahdollista minimoida tietoturvariskejä pelkästään omalla tekemisellään ja tiedostamalla riskien mahdollisuus, sekä seuraamalla ajankohtaista uutisointia.

1.2 Tutkimuksen tavoite ja tutkimusmenetelmä

Tutkimuksen tavoitteena on saada suomalaiset mikroyrittäjät ymmärtämään tietoturvan merkitys, mitä tietoturvariskejä on olemassa ja mitä tietoturvariskejä heidän olisi hyvä huomioida enemmän. Tietoturvariskien havaitseminen ja tietoturvan kehittäminen olisi hyvä

saada osaksi mikroyrittäjien toimintoja ja tietoturvasta huolehtimisen tulisi olla osana mikroyritysten riskienhallintaa.

Toimeksiantaja voi hyödyntää tutkimustuloksia asiakkaidensa parissa, esimerkiksi miettien mahdollisia kehitystoimenpiteitä, joilla parantaa heidän tietoturvatasoansa erilaisilla toimenpiteillä tai kuinka he voisivat havaita tietoturvariskejä aiempaa paremmin. Tämän lisäksi julkiset tutkimustulokset ovat muidenkin hyödynnettävissä.

Tutkimuksessa tullaan käyttämään laadullista tutkimusmenetelmää, jonka materiaali kerätään teemahaastatteluilla. Teemahaastattelu mahdollistaa varsin vapaan puheenvuoron haastateltavalle ennakkoon määritellystä teemasta. Teemahaastattelun merkitys korostuu tilanteessa, jossa on tarve saada tietoa vähemmän tunnetusta asiasta tai ilmiöstä. Teemahaastattelulla kerätään kokonaisvaltaista tietoa todellisesta tilanteesta, saaden samalla laadullinen metodi aineiston hankintaan. Mittausvälineenä tulee olemaan havainnot perustuen teemahaastatteluiden materiaaliin. (Tampereen yliopisto.)

Tutkimuksen aineiston luotettavuus varmistetaan toistettavuudella eli reliaabeliuksella. Mikäli vastaajat, toisistaan riippumatta, antavat samankaltaista tietoa, voidaan aineiston olevan ei-sattumanvaraista ja täten luotettavaa. Aineiston pätevyys, validius, määrittelee kuinka hyvin analysointimenetelmä vastaa aineistoa. (Jyväskylän yliopisto 2009.)

Teemahaastatteluissa haastateltiin 10 suomalaista mikroyrittäjää. Haastattelut suoritettiin verkon välityksellä ja tallennettiin tätä tutkimusta ja tulosten analysointia varten. Tämän lisäksi aiheeseen lähdettiin hakemaan ajankohtaista näkemystä ja tulevaisuuden trendejä seuraavilta asiantuntijoilta: Hannu Huttunen (turvallisuusasiantuntija), Petteri Järvinen (IT-asiantuntija, tietokirjailija), Niko Marjomaa (tietoturva-asiantuntija), Heikki Paananen (tietohallintoyksikön päällikkö), Kimmo Rousku (Tietoturva ry:n hallituksen jäsen, digiturva-asiantuntija), Jani Räty (tietoturva-asiantuntija, FT).

Tutkimuskysymyksellä saadaan tietoa, jolla tutkimusongelmaan hankitaan analysoitavaa materiaalia ja tutkimus on mahdollista toteuttaa. Tämän tutkimuksen pääkysymys on:

- Mitkä ovat suomalaisten mikroyrittäjien käsitykset tietoturvariskeistä?

Pääkysymyksen lisäksi tutkimuksella on alakysymys, jonka tehtävänä on tukea pääkysymystä. Tämän tutkimuksen alakysymys on:

- Mitä tietoturvariskejä suomalaisten mikroyrittäjien tulisi huomioida enemmän?

1.3 Toimeksiantaja

Toimeksiantajana toimii suomalainen mikroyritys Avosorsa Oy. Yritys on perustettu vuonna 2015, yrityksen kotipaikka on Hollola ja toiminta-alueenaan yritys kertoo olevan internet. Yritys on keskittynyt auttamaan etenkin suomalaisia mikroyrityksiä verkkoliiketoiminnassa, muun muassa verkkosivujen, verkkokaupan, hakukonenäkyvyyden ja hakukonemainonnan osalta. Yrityksen tuotevalikoimassa on maailman yleisimmin käytettyjä, avoimen lähdekoodin ohjelmia ja tästä juontaa yrityksen nimi (open source, avoin lähdekoodi, ”sorsakoodi”). Yritys mainitsee keskittäneensä osaamisen WordPress-ohjelman hyödyntämiseen Google-ympäristössä. Lisäksi yritys tarjoaa digitaalisia markkina- ja kilpailijakartoituksia. (Avosorsa Oy 2021.)

Toimeksiantajan asiakaskunta muodostuu pääsääntöisesti suomalaisista, yrittäjävetoisista mikroyrityksistä. Toimeksiantajan havaintojen mukaan kohderyhmällä on osittain vaikeuksia tunnistaa tietoturvariskejä tai tehdä niiden minimoimiseksi toimenpiteitä. Toisinaan tietoturvariski on havaittu, mutta asian edistämiseksi ei tehdä toimenpiteitä.

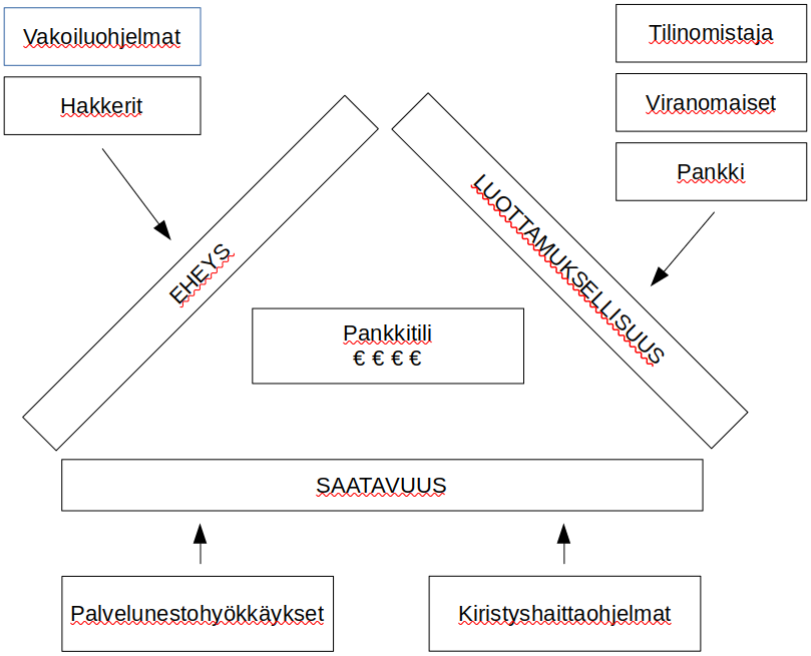
2 Tietoturva

2.1 Määritelmä

Tietoturvan määritelmän mukaan tietoturva on tiedon luottamuksellisuuden, eheyden ja saatavuuden ylläpitoa (Bell & La Padula 1976, 13, 40, 70–71; Clark & Wilson 1987, 185–186). Nämä kolme elementtiä tunnetaan CIA-kolmiona, jossa lyhenne tulee englanninkielisistä sanoista confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Nämä kolme tietoturvan perusperiaatetta määrittelevät erilaisia vaatimuksia tiedon käsittelyssä käytettäville prosesseille ja järjestelmille. (Karsisto 2007, 5.)

Tietoturvassa on siis kyse toimenpiteistä, joilla tavoitellaan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamista (Tieteen termipankki 2022a). Luottamuksellisuudella huolehditaan tietojen olevan vain niiden käytössä, joilla tiedon kuuluukin olla käytettävissä. Eheydellä huolehditaan tietojen muuttumattomuus, sekä tietojen oikeanlainen hävittäminen. Saatavuudella huolehditaan tietoihin pääsystä silloin kun tietoon on tarkoitus päästä. (Kyberturvallisuuskeskus 2020.) Esimerkkinä näihin voisi ajatella kysymyksiä: Kenellä tietoon on pääsy, milloin tietoon on päästävä käsiksi, onko tieto edelleen siinä muodossa kuin sen kuuluukin olla, onko tiedon määrä oikea.

Otetaan esimerkkinä yrityksen pankkitili. Tässä tapauksessa yrittäjällä on pääsy kyseiseen tiliin eli tietoon. Tämän lisäksi tilitiedot ovat pankin ja joidenkin viranomaisten saatavilla. Tieto säilyy kuitenkin luottamuksellisena, koska tietoon pääsevät käsiksi vain ne, joilla on oikeus siihen. Luottamuksellisuus on siis kunnossa, mutta tässä vaiheessa esimerkkiä astuu kuvaan eheys. Eheyttä eli tiedon muuttumattomuutta yrittävät horjuttaa esimerkiksi erilaiset vakoiluohjelmat ja hakkerit. Mikäli eheys murtuu ja nämä haitalliset tahot pääsevät tiliin eli tietoon käsiksi, on sekä luottamuksellisuus, että eheys menetetty. Kolmantena asiana on saatavuus. Saatavuus antaa tilin eli tiedon käyttöön silloin kuin käyttäjä sitä tarvitsee. Tätä saatavuutta yritetään estää esimerkiksi palvelunestohyökkäyksillä ja kiristyshaittaohjelmilla. Mikäli nämä onnistuvat heikentämään saatavuutta, on luottamuksellisuus ja eheys edelleen tallessa. Toisaalta tietoon oikeutettu käyttäjä ei tällöin pääse tietoon käsiksi eli luottamuksellisuus on mennyt. Lisäksi voidaan huomioida, että saatavuuden voi estää myös jokin haitallinen taho eheyden murtumisen myötä.



Kuva 1. Tiedon luottamuksellisuuden, eheyden ja saatavuuden esimerkki

Tietoturvan määritelmän kolme peruspilaria, tiedon luottamuksellisuus, eheys ja saatavuus, ovat siis itsessään melko yksinkertaisia, mutta niiden vaikuttavuus moniin asioihin on huomattavasti monimutkaisempi. Lähtökohtaisesti kaikki tiedon käsittelyyn liittyvä toiminta tulisi olla yhteydessä näihin tietoturvan peruspilareihin ja kaiken tietoturvallisen toiminnan tulisi pyrkiä toimimaan näiden vaatimalla tavalla.

Tiedon luottamuksellisuus

Tiedon luottamuksellisuus käsittää toimenpiteet, joilla tiedot suojataan luvattoman käytön riskeiltä. Tietojen tulee olla käytettävissä vain henkilöillä tai tahoilla, jotka tietoa tarvitsevat. (Miettinen 2002, 129.) Tiedon luottamuksellisuudella varmistetaan myös tietojen paljastamattomuus henkilöille, toiminnoille tai laitteille, joille tieto ei kuulu, sekä estetään sivullisten pääsy tietoon (Pollari 2021, 13; Tieteen termipankki 2022b). Luottamuksellisuudella pyritään varmistamaan esimerkiksi oikeiden henkilöiden pääsy tietoon ja estämään tiedon tahallinen tai tahaton paljastuminen. Luottamuksellisuus pitää sisällään muun muassa käyttöoikeudet ja roolit eri käyttäjille, salasanojen hallinnan ja niistä huolehtimisen. (Rautiainen 2013a; Rousku 2014, 48.)

Tiedon eheys

Tiedon eheydellä varmistetaan tietojen muuttumattomuus. Tiedon tulee pysyä virheettömänä, tallennetun tiedon määrän ei pidä muuttua itsestään, ja tietojen tulee pysyä siinä muodossa kuin niiden on alun perinkin kuulunut olla. (Miettinen 2002, 129.) Lisäksi

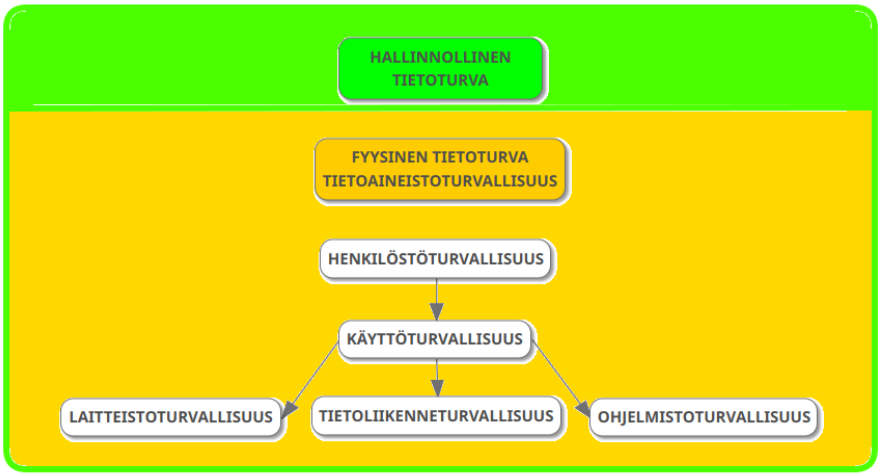
eheydellä suojataan tiedot luvattomalta perustamiselta, käsittelyltä ja poistamiselta (Pollari 2021, 13). Tietojen mahdolliset muutokset tulee voida todentaa ja tiedon tulee olla keskinäisesti yhdenmukaista alkuperäisen tiedon kanssa (Tieteen termipankki 2022c). Eheydellä pyritään varmistamaan tiedon pysyminen siinä muodossa kuin sen kuuluukin olla ja mahdolliset muutokset on tehty valtuutettuina kyseiseen tietoon. Varmuuskopiointi ja tarvittaessa tiedon palauttaminen on yksi merkittävä tiedon eheyden varmistaja. (Rautiainen 2013b).

Tiedon saatavuus

Tiedon saatavuudella varmistetaan tiedon käytettävyys. Tiedon tulee olla saatavilla oikeaaikaisesti, koko sen ajan kuin tietoa on tarve käyttää. (Miettinen 2002, 129.) Saatavuudella turvataan tietojen käytettävyys kyseiseen tietoon valtuutetuille henkilöille, laitteille tai osapuolille ja niihin tulee päästä käsiksi aina kun kyseiseen tietoon valtuutetuilla on tarve. Saatavuutta voi horjuttaa esimerkiksi palvelunestohyökkäykset, joiden tehtävä on kuormittaa voimakkaasti palvelimia ja estää näin käyttäjän pääsy tietoon haluttuna aikana. (Rousku 2014, 50.) Tähän ei kuitenkaan kuulu mahdolliset huoltokatkot. Tiedon tulee siis olla käytettävissä haluttuna aikana ja tarpeen edellyttämällä tavalla (Tieteen termipankki 2022d).

2.2 Tietoturvan osa-alueet

Tietoturvaa voidaan tarkastella jakamalla se osa-alueisiin. Näiden osa-alueiden tehtävänä on helpottaa tietoturvan hahmottamista ja tiedostamista. (Ruohonen 2002, 4–5.) Hallinnollinen osa-alue määrittelee yrityksen toiminnat ja suunnitelmat tietoturvan suhteen. Fyysinen osa-alue sisältää yrityksen tilojen, laitteiden ja materiaalien fyysisen suojauksen. Tietoaineiston osa-alue turvaa yrityksen asiakirjat ja tiedostot. Henkilöstön osa-alue muodostaa toimenkuvien ja käyttöoikeuksien määrittelyt sekä tarvittavat koulutukset. Käytön osa-alue kattaa käyttöperiaatteet ja -ympäristön, salasanat ja varmuuskopiot. Laitteistojen osa-alue kattaa laiteturvallisuuden ja ohjelmistojen osa-alue vastaavasti käytettävien ohjelmien turvallisuuden. Tietoliikenteen osa-alue sisältää toimenpiteet, joilla pyritään varmistamaan välitettävien tietojen luottamuksellisuus, eheys ja saatavuus. (Helsingin yliopisto 2011.)



Kuva 2. Tietoturvan osa-alueet ja niiden sijoittuminen suhteessa toisiinsa

Hallinnollinen tietoturva

Hallinnollinen tietoturva pitää sisällään tietoturvajohtamisen ja siihen liittyvät tietoturvasuunnitelman, -linjauksen ja -vastuunjaon. Edellä mainittu yhdistää tietoturvan osa-alueet kokonaisuudeksi, mahdollistaen tietoturvan kehittämis- ja ylläpidon toimintaedellytykset ja antaen perusteet yrityksen tietoturvapolitiikkaan (Laaksonen ym. 2006, 123–124, 128.) Hallinnollinen tietoturva määrittelee yrityksen näkemykset tietoturvan periaatteisiin ja toimintatapoihin. Siihen lukeutuu myös tietoisuus mahdollisista tietoturvariskeistä ja näiden mukaiset menettelyt sekä henkilöstön tietoturvakoulutuksen ja riskien havainnoinnit. (Karsisto 2007, 9.)

Fyysinen tietoturva

Fyysinen tietoturva sisältää yrityksen tuotanto-, varasto- ja toimitilat, tilojen tärkeysluokitukset sekä näissä olevien laitteiden suojaamisen esimerkiksi lämpötila-, kosteus-, palo-, vesi- ja sähkövahingoilta. Näiden lisäksi tulee ottaa huomioon varkauden ja ilkivallan uhat, kulunvalvonta sekä valvontakamerat ja murtosuojaukset. (Andreasson ym. 2013, 52–64.) Fyysisen tietoturvan toteutuminen on hyvä varmistaa säännöllisesti, ja jo suunnitteluvaiheessa on hyvä huomioida eri tilojen ja laitteiden vaatimukset (Karsisto 2007, 11).

Tietoaineistoturvallisuus

Tietoaineistoturvallisuus kattaa yrityksen strategiset tiedot, asiakas- ja henkilöstötiedot, talous- ja hallintotiedot sekä tuotekehitys-, tuote- ja palvelutiedot. Tähän sisältyy myös tietoaineiston oikeanlainen poisto ja hävittäminen. (Laaksonen ym. 2006, 156–158, 161.)

Tietoaineistoturvallisuuden tehtävänä on myös luokitella suojattavat tiedot ja määritellä tietoaineistoluokan mukainen suojaustaso (Karsisto 2007, 12).

Henkilöstöturvallisuus

Henkilöstöturvallisuus kattaa kaiken missä on osapuolena henkilö. Merkittävä tekijä on henkilön käytös, toiminta ja huolellisuus, inhimilliset virheet sekä tietoturvaosaaminen tai osaamisen puute. Henkilöstöturvallisuuteen liittyy myös henkilövaihtuvuus, yhteistyökumppanit ja alihankkijat sekä palveluntarjoajat digitaalisiin palveluihin. (Laaksonen ym. 2006, 138–139.)

Käyttöturvallisuus

Käyttöturvallisuus käsittää normaalit käyttötoiminnot. Näitä ovat esimerkiksi käyttöoikeuksien määrittely, laitteiden ja järjestelmien käyttäminen ja käytön valvonta sekä salasanojen hallinta ja varmuuskopiointi. (Laaksonen ym. 2006, 162–171.) Käyttöturvallisuus mahdollistaa tiedon käsittelyn ja käytön jatkuvuuden sekä laitteiden ja ohjelmien turvallisen käytön koko niiden elinkaaren ajan (Karsisto 2007, 12).

Laitteistoturvallisuus

Laitteistoturvallisuus käsittää laitteiden pääsynvalvonnan ja tapahtumatiedot, laitteiston yleisen toimivuuden, laitedokumentoinnin, laitteen varmentamisen (varalaite) sekä varaosien saatavuuden, ylläpito- ja huoltosopimukset. Lisäksi laitteiden ylläpidon osalta tulee huolehtia tarvittavien tietojen palauttaminen, mikäli jokin haittaava poikkeama esiintyy. (Andreasson ym. 2013, 65–68.)

Ohjelmistoturvallisuus

Ohjelmistoturvallisuus tarkoittaa käytettävien ohjelmien ja sovellusten suojaamista (ml. Käyttöjärjestelmä, tietokannat). Suojaaminen tapahtuu esimerkiksi ohjelmien päivitysten ylläpidolla, pääsynvalvonnalla, tapahtumalokilla, varmuuskopioinnilla ja dokumentoinnilla. (Laaksonen ym. 2006, 151–153, 156, 159.) Lisäksi ohjelmistojen luotettavuus on hyvä ottaa huomioon (Karsisto 2007, 12).

Tietoliikenneturvallisuus

Tietoliikenneturvallisuus sisältää kaiken, joka liittyy tiedon välittämiseen käyttäjältä toiselle. Tietoliikenneturvallisuudessa tulee estää väärinkäytöt tietoliikenneyhteyksissä (ml. mobiiliverkko), lähiverkossa ja verkkoon liitetyissä laitteissa. Siihen sisältyy myös tietoliikenneverkon välityksellä toimivat haittaohjelmat, sekä esimerkiksi palvelunestohyökkäykset. (Andreasson ym. 2013, 69–76.) Tietoliikenneturvallisuuteen katsotaan sisältyvän myös

tietoliikennelaitteiden hallinnan ja ylläpidon, ongelmatilanteiden tiedostamisen ja niiden kirjaukset, käytönvalvonnan, tietoliikenteen salauksen ja valvonnan sekä verkon hallinnan (Karsisto 2007, 11).

2.3 Tietoturvan rooli mikroyrityksessä

Tilastokeskuksen määrittelyn mukaan mikroyritys on kyseessä silloin, mikäli henkilökuntamäärä on alle 10 työntekijää ja vuosittainen liikevaihto tai taseen loppusumma on enintään 2 miljoonaa euroa. Yrityksen tulee täyttää myös riippumattomuuden määrittely; 25 prosenttia tai enemmän pääomasta tai äänivaltaisista osakkeista ei ole yhden yrityksen omistuksessa tai sellaisten yritysten yhteisomistuksessa, joihin ei voi soveltaa Pk-yrityksen tai pienen yrityksen määritelmää. (Tilastokeskus.) Suomessa vuonna 2021 kaikista toiminnassa olevista yrityksistä 93 prosenttia on ollut mikroyrityksiä (Elinkeinoelämän keskusliitto 2021).

Yrityksessä tietoturva saatetaan mieltää monimutkaiseksi ja hankalaksi, lähes mahdottomaksi toteuttaa, ilman tarvittavaa osaamista ja tietoa. Tietoturva voidaan kokea hyvin tekniseksi, vaikkakin suurin tekijä tietoturvariskin toteutumiseen on henkilön käyttäytyminen. Näin ollen, yrityksellä tulisi olla hallinnassa teknisen puolen lisäksi henkilöstön tietoturvallinen toiminta. (Pollari 2021, 7.) Tietoturvan tulisi kattaa yrityksen kaikki ne toiminnot ja osa-alueet, joissa käsitellään tietoa. Myös ajanpuute on mikroyritysten yleinen ongelma ja tämä saattaa vaikuttaa tietoturvan toteuttamiseen (Journal 2014, 192). Koska tavoitetila on tiedonturvaaminen, tulisi sen eteen tehdä toimenpiteitä (Limnéll ym. 2014, 60).

Vaikka tietoturva saatetaankin mieltää omaksi osa-alueeksi ja sitä varten tulisi olla vastaava henkilö nimettynä, sen ei tulisi olla vain yhden henkilön varassa. Yrityksen koko ajattelutavan tulisi olla kannustava tietoturvaan. Tietoturva olisi suositeltavaa olla osana jokapäiväistä tekemistä ja kuuluvan jokaisen työntekijän tapaan työskennellä. Yrityksessä olisi hyvä olla laadittuna oma tietoturvapolitiikka ja sitä voidaan toteuttaa, ilman erillistä tietoturvaorganisaatiota tai nimettyä vastuuhenkilöä, johdon sitoutumisella ja liittämällä tietoturva osaksi riskienhallintaa (Karsisto 2007, 15–16). Tietoturvallinen toiminta vaatii yritykseltä jatkuvaa huomioita (Pollari 2021, 7). Yrityksellä tulisi olla kokonaiskäsitys yrityksen toiminnasta ja siihen vaikuttavista tekijöistä. Näiden tulisi ohjata yritystä kohti aktiivista turvallisuusjohtamista ja riskienhallintaa. (Limnéll ym. 2014, 114.)

Yrityksen olisi hyvä pitää tiedon suojaamista eräänlaisena mittarina toimintavarmuudesta ja huomioida tiedon luoma liiketoiminnallinen arvo yritykselle (Pollari 2021, 14). Liiketoimintaa tukevien, keskeisten tietojen tulisi olla yrityksen hallinnassa, muussa tapauksessa yrityksen toiminta voi vaarantua. Yritystoiminnan ja päätöksenteon suhteen tietojen tulee olla

virheettömiä. Luvattomasti muuttuneet tiedot voivat aiheuttaa yritykselle mainehaitan ja tämän kautta vaarantaa liiketoiminnan. (Andreasson ym. 2013, 32.)

3 Tietoturvariski

3.1 Määritelmä

Tietoturvariski on kokonaisuus, joka alkaa uhasta, käyttää välineenä haavoittuvuutta ja päättyy riskiin. On siis olemassa oleva, suojausta vaativa tieto, tuote, oikeus, osaaminen tai laite, ja uhka on toiminto tai taho, mikä saattaa vaarantaa tämän suojauksen. (Neittaanmäki ym. 2021, 136, 142.) Haavoittuvuus muuntaa uhan riskiksi. Haavoittuvuus sisältää heikkouksia esimerkiksi tietojärjestelmissä, yrityksen toimintatavoissa tai henkilöstön toiminnoissa. (Tieteen termipankki 2018.)

Tietoturvariski voidaan käsittää uhan toteutumisen mahdollisuutena ja sen myötä tulevan mahdollisen vahingon arvona. Tietoturvariskin koko määrittyy sen myötä tulevan vahingon laajuudesta ja tapahtuneen vahingon todennäköisyydestä (Tieteen termipankki 2004). Uhka on siis toiminto, joka pakottaa tekemään toimenpiteitä. Näillä toimenpiteillä pyritään ehkäisemään uhan toteutuminen ja sen myötä mahdollisesti tuleva negatiivinen vaikutus. (Limnéll ym. 2014, 230.)

Tietoturvaan vahvasti liittyvät riskiarviot ja -analyysit ovat erilaisia uhkien tunnistusmenetelmiä. Näiden avulla voidaan luoda uhkien vaikutusten tilannekuva mikroyrityksen kriittisiin toimintaedellytyksiin. Tietoturvariski sisältää kolme ala-aihetta: Tietoturvariskin uhka, epävarmuus ja mahdollisuus. (Karsisto 2007, 32.) Tietoturvariskin epävarmuus kuvastaa uhan, ja täten itse riskin näkymän todennäköisyyttä. Tietoturvariskin mahdollisuus antaa yritykselle kehitysedellytykset, joiden avulla riskiä voidaan hallita. Perimmäisenä tarkoituksena on taata yrityksen toiminnan jatkuvuus, myös riskien toteutuessa. Tietoturvallinen toiminta auttaa riskien hallitsemista ja kaikki nämä kuvastavat valmiuksia kohdata tietoturvariski. (Karsisto 2007, 32.) Riskin mahdollisuus sisältyy kuitenkin kaikkeen toimintaan, ja riski itsessään ei ole ongelma. Ongelma on riskin toteutumisen myötä tullut ei-toivottu tapahtuma. (Limnéll ym. 2014, 236.)

Tietotekniikka liittyy jokaisen yrityksen jokapäiväiseen liiketoimintaan, joko suoranaisesti yrityksen toimintojen kautta, välillisesti yhteiskunnan tai henkilön kautta ja tämän on havaittu lisäävän erilaisia tietoturvariskejä. Tietotekniikan käyttämisen myötä olisi hyvä ymmärtää siihen kohdistuvia riskejä (Pollari 2021, 7, 10). Koska tavoitetila on turvallinen toimintaympäristö, myös tietotekniikan suhteen, tulisi arvioida erilaisia uhkia ja näiden myötä vahvistaa turvallisuutta (Limnéll ym. 2014, 60).

Vaikka itse tietoturvariski näyttäisi olevan määrittelemätön, erilaisilla tulkinnoilla voidaan hahmottaa sen määritelmä ja monesti puhutaan riskin sijaan riskien hallinnasta.

Tietoturvariskin voidaan ajatella pitävän sisällään riskien hallinnan, niihin liittyvien luottamuksellisten, kriittisten tietojen ja resurssien hallinnan sekä mahdollisen tapahtuman mikä vaarantaa nämä tiedot ja resurssit. Mahdollisten tapahtumien myötä tulevat odottamattomat, negatiiviset seuraukset ovat vahvasti sidoksissa tietoturvariskeihin. Riskistä puhuessa voidaan siis ajatella tietyn uhan toteutuminen jollakin tietyllä haavoittuvuudella ja tapahtuman tulos on haitallinen tai poikkeava odotetusta. (Pollari 2021, 10.) Tämä poikkeama voi vaarantaa tiedon luottamuksellisuuden, eheyden tai saatavuuden (Suomidigi 2020).

Joistakin tietoturvariskeistä on helppo saada ajantasaista tietoa. Esimerkiksi Liikenne- ja viestintävirasto Traficomin alaisuudessa toimiva Kyberturvallisuuskeskus tuottaa Kybersää uutiskarttaa. Kyseinen uutiskartta kertoo kuukausittain erilaisia tietoturvaa uhkaavia ilmiöitä ja näihin mahdollisesti olemassa olevia suojautumiskeinoja. Tietoturvailmiöitä ovat esimerkiksi tietomurrot ja tietovuodot, huijaukset ja tietojenkalastelut, haittaohjelmat ja haavoittuvuudet, palvelunestohyökkäykset ja kybervakoilu. (Kyberturvallisuuskeskus 2022.)

Tietoturvan hinta on vaikeasti määriteltävissä ja tietoturvan investointeihin ei koeta halukkuutta. Tietoturva koetaan usein menoeränä siihen saakka, kunnes tietoturvariski toteutuu. Näin ollen, tietoturvan hinnan määrittely voidaan laskea mahdollisen rahallisen menetyksen kautta riskin toteutuessa. Kustannusten kokonaisuuteen katsotaan kuuluvan esimerkiksi mahdolliset ongelmat tuotannossa, selvittelyyn ja korjaukseen menevä aika, yrityksen luottamuskuvan heikentyminen ja yrityksen arvon alentuminen. Tiedon luottamuksellisuuden, eheyden ja saatavuuden menetyksen kannalta ei ole merkitystä tapahtuuko riskin toteutuminen esimerkiksi luonnonilmiön vai inhimillisen erehdyksen kautta. (Pollari 2021, 12–14.) Sen sijaan, tietoturvallisen toiminnan hintaan vaikuttavat esimerkiksi yrityksen koko, toimintaympäristö, turvattavan tiedon laatu ja määrä ja henkilöstön osaaminen. Tietoturvallisen toiminnan hinta on kaksivaiheinen; alkukustannus, joka perustuu lähtötasoon sekä ylläpitokustannus. (Suomen Yrittäjät 2020.)

3.2 Tietoturvariskin aihealueet

Kantar TNS Oy:n, Pk-yritykselle suunnatun Yrittäjägallupin mukaan (Kauppalehti 2022) 34 % vastaajista koki tietomurrot suurena tai melko suurena riskinä liiketoiminnalle ja 7 % ei nähnyt riskejä ollenkaan. Tietoturvasta huolehtimisen erittäin tärkeänä asiana piti 58 % vastaajista ja melko tärkeäksi 31 %. Vastaajista 56 % koki tietoturvan tason hyväksi, 15 % erinomaiseksi ja 29 % heikommaksi. Esteitä tietoturvan toteuttamiseen koki 61 %. Osaamisen puute (35 %), tietoturvan kustannukset (22 %) ja ajan puute (18 %) olivat merkittävimmät esteet tietoturvan toteuttamiseen. Lisäksi 39 % oli vastannut, että ei esteitä tietoturvan

toteuttamiselle. Kyselyyn osallistuneista vastaajista 80 % työllistivät alle 10 henkilöä, mutta erikseen ei mainittu, täyttivätkö ne muilta osin mikroyrityksen määritelmän.

Deloitte Touche Tohmatsu Limitedin (2017) maailmanlaajuisen tutkimuksen mukaan yrityksillä on haasteita hallita riskejä. Vastaajista 42 % piti yritystään tehokkaana tai erittäin tehokkaana kyberturvallisuusriskien hallinnassa. Haasteina olivat kyberturvallisuusasiantuntijoiden palkkaaminen (58 %) ja lähes reaaliaikaisen, käyttökelpoisen uhkatiedon saaminen (57 %). Vastaajista 26 % piti yritystään tiedonhallinnan suhteen tehokkaana tai erittäin tehokkaana. Haasteita koettiin yrityksen johtamismallista (40 %), kolmansista osapuolista (37 %) ja tietojen eheydestä (32 %).

Pollarin (2021, 42) mukaan henkilön omalla toiminnalla aiheutetut tietoturvariskit ovat merkittävässä roolissa, vaikkakin inhimillisiin tekoihin ja toimintoihin liittyviä tietoturvariskejä ei ole tutkittu tarpeeksi. Henkilön toimintaan vaikuttavat huolimattomuus ja tietämättömyys. Näiden myötä erilaiset tietoturvariskit ja tietoturvaloukkaukset tulevat mahdollisiksi. Tietoturvariskejä voidaan vähentää henkilöstön valmiudella kohdata ne; tiedostamalla riskit, hallitsemalla perusasiat ja käyttämällä järkeä (Limnéll ym. 2014, 97).

Tunnistaakseen tietoturvariskit yleensäkin, yrityksen tulisi tunnistaa liiketoimintaansa vaikuttavat keskeiset riskit. Riskien jatkuvan muodonmuutoksen vuoksi tulisi niiden hallinnasta tehdä jatkuva prosessi osana yrityksen toimintaa. (Pollari 2021, 21.) Riskejä ei kuitenkaan voida täysin poistaa, vaan niitä tulee tarkastella vähentämisen ja varautumisen kannalta. Merkittävää hyötyä ei myöskään saavuteta kaikkien riskien minimoinnilla, koska tällöin tehtävät toimenpiteet ovat suhteettoman suuria saavutettuun hyötyyn nähden. Riskinhallinta tulisi suhteuttaa sopivan kokoiseksi ja hyväksyä, että riskejä ei voi poistaa täysin. (Pollari 2021, 22–23.) Täyttä turvallisuutta ilman minkäänlaisia uhkia ei ole, turvallisuuden tasoon voi vaikuttaa järjestelemällä turvattavat asiat tärkeysjärjestykseen ja tehden niiden mukaisia turvatoimia (Limnéll ym. 2014, 45).

Pollarin (2021, 46) tutkimuksessa todetaan tietoturvariskien hallinnan oleellisimman seikan olevan tietoturvariskin tunnistaminen ja sen vaikutuksen merkitys. Lisäksi henkilöstön rooli, yrityksen määrittelemät tietoturvakäytännöt ja johdon sitoutuneisuus vaikuttavat riskien hallintaan.

Tietoturvariskin inhimilliset tekijät

Tietoturvariskin inhimilliset tekijät käsittävät henkilön ja tämän tekemät toimenpiteet. Merkittävä osa inhimillisistä tekijöistä on tahatonta ja niihin sisältyy vahvasti henkilön kiire, huolimattomuus ja osaamattomuus. Nämä voivat ilmetä esimerkiksi yhden salasanan käyttämisenä monessa paikassa, tietojen vääränlaisena poistamisena tai laitteen hävittämisenä.

Lisäksi työnteossa käytetyt ohjelmat voivat olla hankalia käyttää ja mahdollista koulutuksen tuomaa tietoa ei ole sisäistetty ja otettu käyttöön. Lisäksi riskinä ovat perheenjäsenien jakamat laitteet, mikäli näitä samoja laitteita käytetään työntekemiseen. (Järvinen 2012, 19.) Myös toimintatavat ja tiedonpuute ovat merkittävässä asemassa inhimillisissä tekijöissä (Pollari 2021, 44).

Tietoturvariskin hallinnolliset tekijät

Hallinnolliset tekijät muodostavat tietoturvariskin yrityksen johdon suhtautumistavalla tietoturvan tavoitteiden, prosessien ja koulutuksen sekä näihin liittyvien toimien tukemisella (Hakala ym. 2006, 114). Myös yrityksen johdon sitoutuneisuus, henkilöstön hallinta ja henkilöstön mukaan ottaminen päätöksentekoon on osana hallinnollisia tekijöitä (Pollari 2021 44). Hallinnollisilla toimenpiteillä on mahdollista vähentää inhimillisiä uhkia ja se kattaa myös henkilöstön vaihtuvuuden myötä tulevia riskejä (Laaksonen ym. 2006, 139).

Tietoturvariskin ohjelmisto- ja laitteistotekijät

Ohjelmisto- ja laitteistotekijät luovat riskin esimerkiksi päivitysten laiminlyönnin seurauksena. Ajantasaisilla päivityksillä minimoidaan ohjelmistovirheitä, yhteensopimattomuusongelmia ja tietoturva-aukkojen tuomia riskejä. (Järvinen 2006, 15–17.) On hyvä myös huomioida käytettävien laitteiden käyttöikä ja mahdollinen elinkaari. Ohjelmapäivityksiä tulisi olla saatavilla laitteen koko käyttöajan ja niiden puute vaikuttaa merkittävästi laitteen elinkaareen. (STT Viestintäpalvelut 2021.)

Tietoturvariskin ympäristötekijät

Ympäristötekijöihin voidaan lukea tietojenkalastelu ja fyysinen uhka. Tietojenkalastelu on rikollista toimintaa ja sen tarkoituksena on päästä käsiksi luottamuksellisiin tietoihin esimerkiksi verkon välityksellä, puhelimitse tai tapaamisella. (Järvinen 2006, 273–274.) Fyysinen uhka voi kohdistua myös sähköiseen materiaaliin, esimerkiksi sen säilytykseen ja laitteisiin sekä tapahtumiin, jotka voivat tuhota olemassa olevat varmuuskopiot (Tirronen 2003).

4 Tutkimus mikroyrittäjien tietoturvariskien käsityksistä

4.1 Kohderyhmä

Tutkimuksen kohteena olivat suomalaiset mikroyrittäjät. Haastatteluryhmän koko oli 10 mikroyrittäjää, edustaen eri sukupuolia ja eri toimialoja. Osallistujat valittiin toimeksiantajan asiakasrekisteristä seuraavien kriteereiden mukaisesti: Osallistuvan yrityksen tuli täyttää Tilastokeskuksen mukainen mikroyrityksen määritelmä, yrittäjän tuli olla päätoiminen yrittäjä, yrityksen kotipaikan tuli olla Suomessa ja heidän tuli olla aktiivisia oman verkkopalvelunsa kehittämisen suhteen. Mikroyrityksen määritelmä on käsitelty teoriaosuuden luvussa 2.3 Tietoturvan rooli mikroyrityksessä.

Suostumus tutkimukseen osallistumisesta kysyttiin henkilökohtaisesti suoraan mikroyrittäjältä sähköpostin välityksellä marraskuussa 2021 ja mikroyrityksen määritelmä tuotiin ilmi tässä yhteydessä. Tutkimuksessa, ja sen tuloksissa, ei tulla julkaisemaan vastaajien, eikä heidän yritystensä nimiä asian arkaluontoisuuden vuoksi.

4.2 Tiedon kerääminen ja analysointi

Teemahaastattelut toteutettiin sekä asiantuntijoille, että mikroyrittäjille verkon välityksellä Teams -etäkokousohjelmalla joulukuu 2021 – tammikuu 2022 välisellä ajalla. Kaikkia osallistujia haastateltiin kerran, haastattelun pituus oli 30–60 minuuttia. Mahdolliset häiriötekijät esimerkiksi asiakaspalvelutilanne, puhelu tai muu yllättävä tilanne pyrittiin minimoimaan, eikä näitä havaittu haastattelujen aikana.

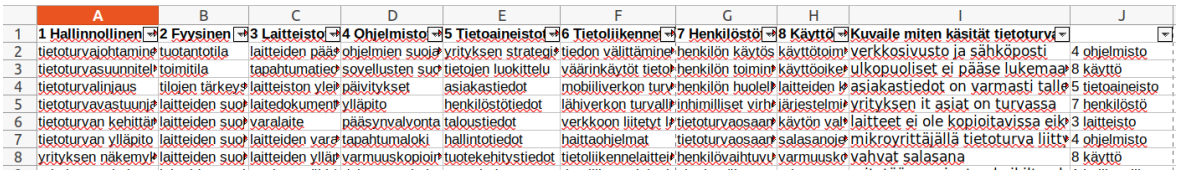
Asiantuntijoiden suostumus haastatteluun tapahtui LinkedIn -verkostoitumisohjelman välityksellä marraskuussa 2021. Asiantuntijoille toimitettiin kysymykset etukäteen sähköpostitse, ja samalla toimitettiin tieto mitä käsite suomalainen mikroyrittäjä pitää sisällään tässä tutkimuksessa: Suomalaisella mikroyrittäjällä tarkoitetaan tässä tapauksessa mikroyrityksen yrittäjää, jonka päätulonlähde on ko. yritystoiminta ja yrityksen kotipaikka on Suomessa. Lisäksi yrityksen tulee täyttää Tilastokeskuksen mikroyrityksen määritelmä.

Asiantuntijahaastatteluilla lähdettiin selvittämään tuoreimpia tietoja tietoturvasta ja tietoturvariskeistä sekä näkökulmia näihin liittyvistä tulevaisuudennäkymistä. Asiantuntijahaastatteluun osallistui kuusi asiantuntijaa ja haastattelut analysoitiin käyttämällä jaottelua tietoturva, tietoturvariskit ja tulevaisuudennäkymät. Näiden jaotteluiden pohjalta muodostettiin kooste asiantuntijoiden näkemyksistä.

Jotta mikroyrittäjien käsitys tietoturvariskeistä saatiin haastatteluiden yhteydessä esille, heille ei toimitettu kysymyksiä tai tietoturvaan liittyvää materiaalia etukäteen. Haastattelijan

näkemyksiä ei tuotu esille, vaan haastattelut keskittyivät ennalta laadittuihin kysymyksiin, joihin haastateltava vastasi vapaamuotoisesti, ilman haastattelijan täydentävää tietoa tai kommentointia.

Mikroyrittäjien haastatteluiden vastaukset purettiin Excel -taulukkoon. Taulukkoon oli lisätty ennalta tietoturvan osa-alueet (8 kpl) ja niiden sisältö sen mukaisesti kuin tämän tutkimuksen teoriaosuudessa on mainittu. Lisäksi taulukkoon lisättiin asiantuntijoiden mainitsemat seikat, joita ei teoriaosuudessa tullut ilmi. Tämän jälkeen mikroyrittäjien mainitsemat asiat linkitettiin tietoturvan eri osa-alueisiin.



	A	B	C	D	E	F	G	H	I	J
1	1 Hallinnollinen	2 Fyysinen	3 Laitteisto	4 Ohjelmisto	5 Tietoaineisto	6 Tietoliikenne	7 Henkilöstö	8 Käyttö	Kuvaile miten käsität tietoturva	
2	tietoturvajohtamine	tuotantotila	laitteiden pää	ohjelmien suoja	yrityksen strategi	tiedon välittämine	henkilön käytös	käyttötoim	verkkosivusto ja sähköposti	4 ohjelmisto
3	tietoturvasuunnitel	toimitila	tapahtumatie	sovellusten suo	tietojen luokittelu	väärinkäytöt tieto	henkilön toimin	käyttöoike	ulkopuoliset ei pääse lukemaa	8 käyttö
4	tietoturvalinjaus	tilojen tärkeys	laitteiston yle	päivitykset	asiakastiedot	mobiiliverkon tury	henkilön huolell	laitteiden k	asiakastiedot on varmasti talle	5 tietoaineisto
5	tietoturvavastuunja	laitteiden suo	laitedokument	ylläpito	henkilöstötiedot	lähiverkon turvalli	inhimilliset virh	järjestelmi	yrityksen it asiat on turvassa	7 henkilöstö
6	tietoturvan kehittär	laitteiden suo	varalaite	pääsynvalvonta	taloustiedot	verkkoon liitetyt l	tietoturvaosaar	käytön val	laitteet ei ole kopioitavissa eik	3 laitteisto
7	tietoturvan ylläpito	laitteiden suo	laitteiden vara	tapahtumaloki	hallintotiedot	haittaohjelmat	tietoturvaosaar	salasanoje	mikroyrittäjällä tietoturva liitty	4 ohjelmisto
8	yrityksen näkemyk	laitteiden suo	laitteiden yllä	varmuuskopioir	tuotekehitystiedot	tietoliikennelaitteir	henkilövaihtuvu	varmuusko	vahvat salasana	8 käyttö

Kuva 3. Mikroyrittäjien haastatteluvastauksia jaoteltuna tietoturvan osa-alueiden mukaisesti

Näin saatiin käsitys, mistä tietoturvan osa-alueista, niiden sisällöstä ja tietoturvariskeistä mikroyrittäjillä oli tietoa haastattelun aikana. Loppujen lopuksi tuli kokonaisymmärrys suomalaisten mikroyrittäjien käsityksistä liittyen tietoturvariskeihin.

4.3 Asiantuntijoiden haastattelu

Tietoturva

Asiantuntijoiden käsitykset tietoturvasta liittyivät CIA-määritelmään, tietojen jatkuvuuden huolehtimiseen sekä yritys- ja kokonaisturvallisuuteen. Näiden lisäksi tietoturvan tulee varmistaa digitaalisten palveluiden toimivuus ja huomioida sen kattavan myös kyberturvan.

Se on puhtaasti riskien hallintaa oman yrityksen jatkuvuuden varmistamiseksi.

Mainittiin myös tietoturvassa monesti korostettavan liikaa teknistä puolta; kaikki toiminta lähtee kuitenkin ihmisestä ja ihmisen toiminnasta. Teknisten järjestelmien tulisi kuitenkin täyttää niihin kohdistetut odotukset ja vaatimukset.

Asiantuntijoiden mukaan mikroyrittäjien suurimmat esteet tietoturvan parantamiseen olivat tietämättömyys, motivaation puute, välinpitämättömyys, resurssit ja kumppaniverkostot. Tietämättömyydessä ei tiedetä mitä tulisi parantaa tai että jotakin tulisi parantaa, eikä myöskään välttämättä nähdä niitä riskejä mitkä tietoturvaan liittyvät. Myöskään riippuvuutta tietotekniikan riskeistä ei tiedetä, esimerkiksi onko liiketoimintaa mahdollista tehdä, jos verkkoyhteys ei toimi, mitä tehdä, jos kiristysohjelma on koneella tai ulkoinen levyasema varmuuskopioita varten on kiinni työasemassa, mutta haittaohjelma tuhoaa myös sen sisällön.

Ei voi varautua kaikkiin riskeihin, mutta monet yllättää se minkälaiset riskit on olemassa.

Motivaation puute estää edistämästä tietoturvaa. Lisäksi kiinnostuksen puute vähentää motivaatiota. Monesti tietoturvariskin pitää ensin toteutua, jotta asiaan havahdutaan ja sille tehdään jotakin. Tietoturvan tarve tulisi tunnistaa.

Kaikki lähtee siitä, että on motivaatio tietoturvan edistämiseen.

Välinpitämättömyys ilmenee esimerkiksi käytettäessä samoja laitteita ja ohjelmia niin yksityis- kuin työelämässäkin tai käytetään samoja tunnuksia eri palveluissa, eikä huolehdita varmuuskopioista. Resurssien kannalta koetaan puutteita ajassa, rahassa ja taidoissa. Tietoturvapalveluiden ostamista pidetään kalliina, vaikkakaan oma aika ja taito ei riitä parantamaan sitä.

Kun ei ole tapahtunut mitään, niin ei ole tarvetta tehdä mitään.

Resurssit on rajalliset, mihin eurot laitetaan.

Kumppaniverkostoon luotetaan liikaa. Olisi hyvä tietää mitä sopimus sisältää ja mitä se tarkoittaa käytännössä. Luotettava kumppaniverkosto auttaa varmistamaan liiketoiminnan jatkuvuuden mahdollisessa häiriötilanteessa, joka on saattanut tulla tietoturvariskin seurauksena.

Tietoturvariski

Asiantuntijoiden mukaan tietoturvariski on mikä tahansa häiriö, joka johtaa vaikeuksiin tai heikentäisi liiketoiminnan jatkuvuutta. Tietoturvariskit ovat moninaisia ja mikroyritysten tulisi selvittää mitkä ovat todellisia liiketoimintariskejä.

Niin pientä yritystä ei olekaan, etteikö tietoturva koskisi heitä.

Strategiset, hallinnolliset ja taktiset tietoturvariskit ovat hyvin usein samankaltaisia. Strategiset tietoturvariskit vaikuttavat kykyyn tehdä ydinliiketoimintaa. Hallinnollinen tietoturvariski näyttäytyy ongelmatilanteissa ja kuinka yritys on varautunut tietoturvariskeihin. Taktiset tietoturvariskit voivat olla esimerkiksi väärinkäyttöä, verkkorikollisuutta, tahatonta tai tahallista toiminnan lamauttamista.

Mikroyrityksen tulee fokusoida mitä voi tehdä.

Suurimmat riskit tulevat ihmisten toiminnasta, pääosin vahingoista ja inhimillisistä virheistä, vaikkakin käytettävässä tekniikassakin on haavoittuvuuksia. Lisäksi erilaiset verkkorikollisuuden toimijat aiheuttavat tietoturvariskejä, tietoisesti ja vahingoittaen toimintaa. Näiden

lisäksi ilmeni valtiolliset toimijat, kybervakoilu sekä fyysisen maailman uhat digitaalisuuteen ja erilaiset luonnonilmiöt.

Asiantuntijoiden mielestä tietoturvariskeistä mikroyrittäjän tulisi ottaa huomioon ensinnäkin toiminnan jatkuvuuden hallinta. Tieto on aina liiketoiminnan taustalla, riskien havainnointiin tulisi olla mietitty prosessi, jota noudatetaan ja jonka avulla parannetaan havainnointia. Myös läheltä piti -raportointi tulisi ottaa osaksi toimintoja. Kokonaisuutena tulisi kiinnittää huomiota tiedon luotettavuuden, eheyden ja käytettävyyden varmistamiseen. Mikäli tilannetta ei ole hahmotettu, on vaikea varautua erilaisiin tietoturvariskeihin. Asiantuntemus tietoturva-asioihin puuttuu tai tietoturvariskejä ei koeta ajankohtaisiksi omassa yritystoiminnassa.

Kaikkiin riskeihin tulisi kiinnittää huomiota, mutta se ei ole mahdollista.

Lisäksi tulisi miettiä tietotekniikan tuomat riskit, laitteiden rikkoutumiset ja mahdollisen varalaitteen saatavuuden varmistaminen. Ohjelmien tuomia riskejä on mahdollista pienentää pitämällä ohjelmapäivitykset ajan tasalla ja hankkimalla vain luotettavia ohjelmia luotettavilta toimijoilta. Lisäksi tulee huolehtia säännölliset varmuuskopioinnit, lokitietojen saatavuus, eri tunnukset eri palveluihin ja huomioida mahdollinen toisen osapuolen tietovuoto. Näiden lisäksi on erilaisia verkosta tulevia uhkia; virukset, kiristysyritykset ja muut haittaohjelmat, huijaukset ja hyökkäykset ja tiedostamattomat tapahtumat tietoverkossa.

Asiantuntijoiden mukaan tietoturvariskien havainnointi lähtee tunnistamalla oman yrityksen tavoitteet liiketoiminnalle ja ymmärryksellä, että joku haluaa tähän toimintaan iskeä jollakin tavalla. Jokaisen tulisi tunnistaa mistä oma liiketoiminta muodostuu. Yrityksen henkilöluku ei kerro yrityksen tietoturvatasoa. Tietoturvariskit voivat aiheuttaa myös sopimussanktion.

Miten voi havaita? Kysele ja mieti mitä pitäisi ottaa tietoturvasta huomioon.

Mikroyrittäjän tulisi miettiä minkälaisia keinoja on havaita tietoturvariskejä ennakoivasti. Monet keinot vaativat teknistä osaamista, eikä ole erikseen olemassa helppoja tietoturvaratkaisuja mikroyrittäjille. Mikroyrittäjän olisi hyvä selvittää kuinka tietoturva näkyy omalla toimialalla ja tehdä sen mukaiset toimenpiteet. Pitäisi pyrkiä pois ajattelutavasta, jossa mitään ei ole tarvetta tehdä koska mitään ei ole tapahtunut.

Mieti ennakolta miten tietyissä tilanteissa toimitaan.

Usein havainnointi tulee ulkopuoliselta toimijalta ja tällöin mikroyrittäjä on jo niin sanotussa kriisitilanteessa eikä jatkuvuussuunnitelma ole välttämättä valmiina. Tämän vuoksi asiantuntijoiden mukaan olisi suositeltavaa valmistautua ennalta kriisitilanteessa toimimiseen.

Valitettavan usein mikroyrittäjän on helppo tehdä havainto myös itse, esimerkiksi koneet tai ohjelmat eivät käynnisty ja kiristysohjelma on jo koneella.

Tee jotain ennen kuin jotain tapahtuu.

Asiantuntijoiden näkemysten mukaan tulisi kiinnittää huomio outoihin ja normaalista poikkeaviin tapahtumiin vaikkakin esimerkiksi kiireessä ei osata yhdistää poikkeamaa, joka saattaa aiheuttaa tietoturvaongelman. Havainnointi voi on hankalaa ja tulisi enemmän luottaa omaan intuitioonsa. Erilaisista tietoturvauhkista on mahdollista saada tietoa myös kuuntelemalla säännöllisesti tietoturvaa tarjoavan yrityksen edustajaa: tietoturvan myyjät elävät tietoturvauhkia esittämällä.

Tulevaisuudennäkymät

Asiantuntijoiden mukaan seuraavan vuoden aikana tietoturvaan liittyvät huijaukset tulevat lisääntymään ja kehittymään. Tietoturvariskit tulevat kasvamaan ja yleistymään sekä niitä käytetään hyökkäysvälineenä entistä enemmän. Tietoturvariskien kentän laajuus tulee olemaan konkreettinen uhka. Toimitusketjuhyökkäykset tulevat kohdistumaan myös mikroyrityksiin. Pilvipalvelut mahdollistavat riskien kannalta merkittävää parannusta, esimerkiksi muutaman euron kuukausimaksulla saa turvallisemman sähköpostin.

Tulee myös huomata ajanjaksoja taaksepäin; moni ongelma on poistunut.

Tietoturvariskeistä tulee entistä suurempia kokonaisuuksia ja ne laajenevat myös globaalisti, massamäärät tulevat kasvamaan, erilaisia haavoittuvuuksia tullaan yhdistämään kuin myös avointa tietoa. Olisi hyvä huomioida käytettävien kassajärjestelmien, teollisuuskoneiden ja myös autojen tietoturva sekä esineiden internet.

Asiantuntijat havaitsivat tietoturvaan vaikuttavia trendejä olevan etätyö, työsuhteiden muuttuminen, yhteistyökumppanit ja verkostot sekä valtioiden toiminta ja verkkorikollisuus. Etätyöstä mainittiin työtilan järjestäminen (ml. äänieristykset), kotiverkon turvallisuus ja muiden laitteiden käyttäminen sekä työn organisointi. Nostoina ilmeni varjo-IT eli työntekijä ottaa käyttöönsä jonkin muun ohjelman kuin työnantajan tarjoaman esimerkiksi sen helppokäyttöisyyden vuoksi. Lisäksi ilmeni rajan vetämisen puute yksityis- ja työympäristöön.

Työsuhteissa tullaan menemään entistä enemmän Y-tunnuksellisiin suhteisiin eli mikroyrittäjien määrä tulee kasvamaan. Ihmiset oppivat hinnoittelemaan osaamisensa, vapaa-aikansa ja tietonsa.

Alihankinta-, palvelu- ja verkostoketjut tulevat muuttumaan, koska uhka voi tulla myös näiden kautta. Uhka ei siis välttämättä tulekaan verkosta vaan esimerkiksi joltakin tutulta ja luotetulta taholta.

Trendeinä mainittiin myös valtioiden toiminta ja verkkorikollisuus. Verkkorikokset ja -huijaukset tulevat muuttumaan ammattimaisemmiksi, niitä tullaan tekemään myös sattumanvaraisesti, eivätkä ne katso yrityksen kokoa. Verkkorikollisuus tulee kasvamaan, yleistymään ja jengiytymään. Nämä rikollisjengit ja niiden käyttämät alihankintaketjut saattavat olla valtioiden suojeluksessa.

Asiantuntijoiden näkemyksen mukaan seuraavan vuoden aikana mikroyrittäjän tulisi tiedostaa riskit, tehdä oma riskiarvio sekä miettiä mikä olisi pahinta mitä voisi tapahtua ja mikä on yrityksen varasuunnitelma. Lisäksi tulisi tunnistaa omat kriittiset kohdat ja miettiä missä yrityksen toiminnoissa tietotekniikka on välttämätön. Koska tietoturvariski ei katso aikaa, tulisi miettiä mihin asioihin voi yleensäkin varautua etukäteen ja osallistua näitä tukeviin harjoituksiin.

Hyökkäykset, kiristysohjelmat ja haavoittuvuudet tulevat muuttumaan monimuotoisemmiksi ja lisääntyvät myös mikroyrityksiin. Tietoturvan tulisi muuttua olisi kiva olla -muodosta täytyy olla -muotoon.

Etätyö tuo omat haasteensa myös seuraavan vuoden aikana. Etätyössä käytettävät laitteet ja ohjelmat saattavat olla ajan tasalla, mutta esimerkiksi modeemi voi olla vanha ja päivittämätön. Lisäksi kynnys havaintojen mainintaan voi olla korkeampi, koska työyhteisö ei ole välittömässä läheisyydessä.

Etätyö tuo omat haasteensa, kynnys havaintojen mainintaan on korkeampi.

Lisäksi mikroyritysten olisi hyvä käyttää asiantuntijoita. Tietoturvaa tarjoavia asiantuntijoita ei tarvitse välttämättä ostaa isoilta toimijoilta. Olisi hyvä kiinnittää huomiota myös olemassa oleviin yhteistyökumppaneihin ja alihankkijoihin sekä selvittää mistä palveluista tällä hetkellä maksetaan ja mitä sillä saadaan.

Monet asiat mitä pitää itse tehdä, jää todennäköisesti tekemättä.

4.4 Asiantuntijahaastatteluiden tulokset

Asiantuntijahaastatteluiden pohjalta tietoturva tulisi tiedostaa ja tunnistaa osaksi liiketoimintaa. Tulisi miettiä etukäteen mitä tehdä, jos palvelut ei olekaan saatavilla ja mitä jos liiketoiminta ei onnistu kyseisen häiriön vuoksi sekä mitä voi tehdä kokonaisvaltaisen toiminnan

lamauttamisen ehkäisemiseksi. Mikroyrityksen on suositeltava tunnistaa oman liiketoimintansa kannalta tärkeät asiat ja mistä asioista liiketoiminta muodostuu.

Tietoturva on riskien hallintaa yrityksen toiminnan jatkuvuuden varmistamiseksi. Tietoturva on yrityksen kaikkeen tekemiseen liittyvää prosessien ja liiketoiminnan arvon säilyttävää turvatyötä.

Tietoturva nähdään kulueränä yrityksen liiketoiminnassa aina siihen saakka, kunnes jotain tapahtuu. Tulisi osata ymmärtää tietoturvaan vaikuttavan kokonaisketjun merkitys ja ihmisen rooli siinä.

Asiantuntijat suosittelivat mikroyrittäjiä miettimään tilannetta, jossa tiedon luottamuksellisuus, eheys ja saatavuus on menetetty ja mitä sen jälkeen tapahtuu. Mikroyrittäjä voi parantaa kokonaisturvallisuusriskien havainnointia esimerkiksi käyttämällä asiantuntijoita, hyödyntämällä valmiita kyselylistoja, selvittämällä asioita ja seuraamalla uutisointia aiheesta.

Tietoturvariski voi johtaa pahimmillaan siihen, että mikroyrityksellä ei ole enää mitä laskuttaa, ketä laskuttaa tai millä perusteella laskuttaa. Tähän mikroyrittäjän tulisi kiinnittää huomiota. Monesti mikroyrittäjä hankkii elantonsa yritystoiminnalla ja mikäli palvelua ei voida tuottaa, asiakas vaihtaa palveluntarjoajaa. Myös mahdollisen misinformaation tai mahdollisesti jo tapahtuneen tietovuodon tuoma mainehaitta olisi hyvä osata huomioida.

Kaikkiin riskeihin ei voi varautua ja monet mikroyrittäjät yllättyvät siitä minkälaisia riskejä on olemassa. Mikroyrittäjän oma asenne vaikuttaa moneen asiaan ja sitä muuttamalla voi parantaa tietoturvaa. Tietoturvariskit saatetaan havaita, vaikkakin niille ei välttämättä tehdä mitään. Monesti vasta siinä vaiheessa, kun jotakin tapahtuu, ymmärretään miksi tietoturvaan olisi ollut hyvä panostaa jo aiemmin. Todennäköisesti tapahtuma tulee yllätyksenä ja se voi lamauttaa koko liiketoiminnan.

On suositeltavaa huomioida myös tiedon elinkaari; tiedon hävittäminen on yhtä tärkeä asia kuin tiedon säilyttäminenkin. Tulisi osata tiedostaa kokonaisuus ja mitä kaikkea siihen kuuluu.

Tulevaisuudessa tietoverkkorikollisten uhka tulee nousemaan merkittävästi ja rikolliset kehittävät jatkuvasti uusia keinoja. Mikroyritysten tulisi miettiä kiinnostavuus tietoverkkorikollisten kannalta sekä ottaa huomioon valtiolliset toimijat ja esimerkiksi kybervakoilu. Myös mikroyritys voi olla kybervakoilulle kohde, mikäli yritys toimii esimerkiksi alihankkijana verkkorikollista kiinnostavalle suuryritykselle. Myös mikroyrityksen tuotanto voi olla erittäin erikoistunutta ja sen myötä kiinnostaa rikollisia.

Digitalisaatio ja pilvipalveluiden mahdollisuudet tuovat myös hyviä seikkoja tietoturvaan, vaikkakin tulee edelleen muistaa esimerkiksi fyysinen kulunvalvonta, paloturvallisuus ja tietovuodon riski tahattomasti. Lisäksi on hyvä huomioida digitalisaation yleistyminen esimerkiksi kodinkoneissa, vaatteissa, autoissa ja huomioida niiden käyttämä tekniikka.

Mikroyrittäjien tulisi tiedostaa, että tietoturva on osa liiketoimintaa ja sen tulisi olla mukana yrityksen jatkuvassa toiminnassa. Jos tietoturva ei ole kunnossa, on rikollisten helppo tarttua siihen kiinni. Koska tietoturva ja digitaalisuus on kaikessa läsnä, olisi hyvä miettiä mitä ilman ei ole liiketoimintaa, miten tietoturva liittyy niihin ja mitä niille asioille voi tehdä. Itse tekemällä voi vaikuttaa yrityksensä tietoturvaan, vaikkakin monet asiat mitä pitäisi itse tehdä, jää todennäköisesti tekemättä. Loppujen lopuksi ihminen ei välttämättä olekaan se heikoin lenkki; koulutuksella, tiedostamisella, tiedotuksilla ja uutisoinnilla saadaan heikointakin kohtaa vahvistettua.

Tietoturva kannattaa nähdä laajempana kokonaisuutena; se on osa riskienhallintaa ja toiminnan jatkuvuuden varmistamista. Tietoturvaa kannattaa lähestyä kriittisesti, mutta innostuneesti. Yrityksen tietoturvasta ei vastaa yhteistyökumppani, se lähtee aina yrityksen sisältä.

Ennaltaehkäisy on edullisin vaihtoehto aina ja vastuunjako tulisi ymmärtää. Loppupelissä vastuu on aina mikroyrittäjällä, toimitusjohtajalla, hallituksen puheenjohtajalla. Kaikki liiketoiminta pyörii tiedon varassa.

Tietoturva on myös myönteistä kehitystä ja helppoja asioita. Asian huomioiminen on jo hyvä alku ja voi aloittaa perusasioista. Tietoa on maksutta saatavilla, olisi hyvä seurata tietoturvauutisia edes otsikkotasolla. Lisäksi havainnoista olisi syytä kertoa aina jollekin toiselle ja käydä avointa keskustelua. Näiden lisäksi olisi suositeltavaa käyttää asiantuntijoita sekä hankkia tietoa ja palveluita vastaavan kokoiselta mikroyritykseltä.

Tulee muistaa, että tietomurron kohteeksi joutuminen ei ole hävettävä asia, eikä sitä tule peitellä. Mikäli kohtaa minkä tahansa tietomurtoasian, tulee aina tehdä rikosilmoitus. Ja on hyvä huomioida, että tämä koskee niin mikroyritystä, suuryritystä kuin valtion hallintoakin.

Jokaisen mikroyrittäjän tulisi havahtua tietoturvan suhteen; tapahtuma tulee monesti yllättäen, shokkina. Etukäteen kannattaa kartoittaa tilanne, miettiä mitä kaikkea voisi tapahtua, katsoa kriittisimmät riskit ja luoda varasuunnitelma.

Lisäksi kaikkiin yrityksen kannalta kriittisiin toimintoihin tulisi olla aina kahden työntekijän hyväksyntä sekä tulisi hyödyntää kaksivaiheista varmennusta, oli kyseessä sitten henkilö

tai ohjelma. Koko liiketoiminta ei saisi olla kiinni yhdestä työntekijästä ja kaikki sopimukset tulee tehdä kirjallisina sekä huomioida myös alihankintaketjut osana riskejä.

> *Suomessa tarvitaan kaikenlaista yritystoimintaa; jokaisen pitäisi olla mikroyrittäjä Suomessa.*

4.5 Mikroyrittäjien haastattelu

Haastattelun runko

Teemahaastattelujen sisältö noudatti samaa linjaa kaikille mikroyrittäjille.

- Alkusanat, joissa pyydettiin vastaamaan nimenomaan mikroyrittäjän näkökulmasta, eikä niinkään yksityishenkilön sekä vastaamaan rehellisesti ja mikäli ei tiedä vastausta, sekin on suotavaa sanoa. Mainittiin myös mahdollisten vastausten mieleen tuleminen haastattelun eri vaiheissa ja että on sallittua kertoa myös nämä, vaikka kyseinen kysymys olisi jo aikaisemmin käsitelty. Lisäksi kerrottiin haastattelun runko.
- Haastattelussa kysyttiin ensin neljä kysymystä, jonka jälkeen kerrottiin tietoturvan yleinen määritelmä lyhyesti. Tämän jälkeen esitettiin yksi kysymys ja kerrottiin tietoturvan osa-alueista lyhyesti. Tämän jälkeen tuli vielä neljä kysymystä.

Kysymykset oli laadittu ilman ammattisanastoa ja tietoturvan termejä, jotta haastateltaville ei tulisi epävarmuutta kysytystä asiasta ja haastattelutilanne olisi mahdollisimman luonteva. Tietoturvan määritelmän ja osa-alueiden kertomisella haastattelun edetessä pyrittiin avartamaan mikroyrittäjän näkemystä hieman laajemmalle tietoturvan suhteen ja näin varmistamaan, että saadaan esille heidän näkemyksensä aiheesta mahdollisimman kattavasti.

Haastattelu

Kysymykseen kuvaile miten käsität tietoturvan, tietoturvaa pidettiin tärkeänä ja monipuolisena asiana yrityksille. Tietojen ei haluta menevän ulkopuolisille ja niiden tulee pysyä rajatussa käyttötarkoituksessa. Tietoturvan koettiin suojelevan yksityisyyttä ja omaisuutta. Tietoturvatarpeiden koettiin muuttuvan nopeasti.

Tietoturva koettiin olevan vahvasti kytköksissä yrityksen käyttämään tietoturvaohjelmaan sekä salasanojen ja pankkitunnusten suojaamiseen. Myös laitteiden, tietojen ja tilien ei tule olla kopioitavissa tai kaapattavissa ja yrityksen tietotekniikka tulee olla turvattu.

Rikollisuuden koettiin siirtyneen verkkoon ja verkon kautta tulevia uhkia vastaan tulee pyrkiä suojautumaan. Ulkoisten tekijöiden ei tule päästä käsiksi tietoon, käsittäen

verkkosivun/verkkokaupan, sähköpostit, käytettävät tilit ja asiakastiedot, mainittiin myös toimitilat ja työpöytä. Arkaluontoiset tiedot tulee suojata verkossa ja yleensäkin kaikki tulee järjestää siten, että tieto ei joudu vääriin käsiin. Lisäksi mainittiin yhteistyökumppaneiden tietoturva.

Henkilö- ja henkilöllisyystietojen, pankki- ja luottokorttitietojen ilmoittamiset pidettiin tarkkoina, salassa ja turvassa pidettävinä asioina. Näin koettiin myös asiakastietojen ja asiakkaiden henkilötietojen suhteen.

Ulkopuoliset ei pääse lukemaan asioita mitkä ei ole tarkoitettu muiden käsiin.

Tietoturva suojaa mun yksityisyyttä ja omaisuutta.

Tietoturva on melko tärkeä asia nykypäivänä, ehdoton pakko.

Yritetään suojautua kaikilta uhkilta mitä verkosta tulee.

Kysyttäessä erilaisia tietoturvariskejä mainittiin tekemättömät ohjelmistojen ja laitteiden ajantasaiset päivitykset sekä yleensäkin suojautuminen murtautumisia, soluttautumisia ja hakkerointeja vastaan niin verkossa, laitteissa kuin toimitiloissakin. Myös kulkuluvan tai yrityksen henkilöstökortin käyttämättömyys mainittiin. Tietovuodot ja tiedon oikeanlainen hävittäminen sekä kolmannen osapuolen luotettavuus ja niiden tuomat tietoturvariskit koettiin myös riskeiksi. Tästä mainittiin esimerkiksi Facebook; voiko siihen luottaa ja tuleeko sitä kautta tietoturvaongelmia. Myös tiedon jakaminen tai päätyminen väärälle henkilölle verkossa, sähköpostilla tai kirjepostilla, huonot tietoturvaohjelmat ja erilaiset virukset sekä vierailut haitallisilla sivuilla koettiin tietoturvariskeiksi.

Lisäksi mainittiin salasanojen kalastelu, varastaminen tai yleensäkin salasanojen joutuminen vääriin käsiin, liian helpot salasanat ja säilyttäminen esimerkiksi paperilla tai tallennettuina valmiina selaimeen ja puhelimeen. Myös saman salasanan käyttäminen yhdessä palvelussa liian kauan koettiin tietoturvariskiksi. Riskeiksi koettiin myös mahdollinen pankki- ja luottokorttien kopioiminen tai niiden huoleton käyttö sekä yleensäkin pankkiasioihin liittyvät toiminnot.

Identiteettivarkaudet, niin yrityksen kuin henkilönkin, sekä toisen tahon tekemän valeverkkokaupan vaikutus oman liiketoiminnan luotettavuuteen mainittiin riskeinä. Valeverkkokaupalla tarkoitettiin ulkopuolisen tahon tekemää kopiota mikroyrittäjän verkkokaupasta huijausmielessä. Yleensäkin mainittiin myös pienen yrityksen vaara joutua verkkoilkivallan kohteeksi, verkkorikollisuus on tehty helpoksi.

Päästetään ihmisiä paikkoihin mihin niiden ei kuulu päästä, esimerkiksi mun työpöydän ääreen.

Tieto jaetaan vain tarvittaville henkilöille.

Salasanat pitää vaihtaa tietyin väliajoin, salasanojen pitää täyttää tietyt vaatimukset.

Pankki- ja luottokorttitunnusten sekä pinkoodien yms. keräämiset.

Nimen väärin käyttö, yksityisyys häviää.

Tämän jälkeen kysyttiin, mihin tietoturvariskeihin kiinnitetään huomioita nykyisessä toiminnassa ja miten. Tietoturvariskeistä ohjelmistopäivitykset, virustorjunta ja tietoturvaohjelmat pyritään pitämään kunnossa ja ajan tasalla. Niin ikään mainittiin salasanojen vaihtaminen riittävän usein, vahvojen salasanojen suosiminen ja yhden salasanan käytön välttäminen, salasanaohjelman käyttöönottaminen niin sanotun salasanavihkon tilalle sekä kaksinkertaisen varmennuksen suosiminen kirjautumisten yhteydessä.

Huomiota kiinnitettiin myös käyttöoikeuksiin, tiedon jakamiseen ja tiedon päätymiseen ulkopuolisille. Myös mahdolliset tietovuodot, omien henkilötietojen antaminen eri paikkoihin sekä tiedon oikeanlainen säilyttäminen ja hävittäminen tiedostettiin. Kriittisten tietojen säilyttäminen lukollisessa palokaapissa mainittiin sekä paperisilppurin käyttäminen, hälytysjärjestelmä toimipaikassa ja lukollinen postilaatikko.

Sähköpostiin ja puhelimen käyttöön kiinnitettiin huomioita. Tuntemattomilta tulevia sähköposteja ja sähköpostin mukana tulevia linkkejä ei avata. Sähköpostien palvelimet mainittiin turvallisina. Puhelimen käytössä pyrittiin olemaan varuillaan; verkossa rikollinen saattaa päästä tietoihin käsiksi esimerkiksi onkimalla. Tietokone ja kannettava tietokone koettiin turvallisemmaksi käyttää kuin puhelin. Mobiilissa koettiin tapahtuvan paljon rikoksia ja sen myötä pankkiasioita vieroksutaan hoidettavan puhelimella. Tosin, joskus kiireessä asiat hoidetaan puhelimella. Mainittiin myös puhelimen suojaamattomuus, näytön lukituskin saattoi olla pois päältä.

Muista pankkiasioista tietoturvariskejä vältetään pitämällä luottotili pienenä, yrityksen luottokortin käyttöoikeus on vain luotetuilla henkilöillä. Riskeinä nähtiin myös oman luottokortin käyttäminen sen sijaan, että yrityksellä olisi luottokortti.

Näiden lisäksi mainittiin yksin toimimisen riskittömyys; pienessä yrityksessä tietää mitä tapahtuu ja osaa epäillä, vaikkakin koko ajan pitää olla tarkkaavainen.

Kaikkiin palveluihin on eri salasanat salasanavihkossa.

Tietoja pääsee katsomaan vain se kenelle tieto kuuluu.

Sähköpostit menee turvallisesti, turvallisen palvelimen kautta.

Joku sanoi joskus, että mobiilissa voi joutua helpommin uhriksi pankkiasioissa.

Kysyttäessä mitä tietoturvariskin havaitseminen vaatii mikroyrittäjältä, mainittiin kriittisyys sähköposteja ja tekstiviestejä kohtaan, etenkin tuntemattomilta lähettäjiltä. Epäilyttäviin sähköposti- ja tekstiviesteihin suhtauduttiin varauksella ja ne jäävät monesti avaamatta. Toisinaan tarkistetaan lähettäjältä viestin aitous. Siltikin mahdollisia huijausviestien linkkejä välillä klikataan kokeilumielessä.

Myös näkyvät poikkeamat yrityksen verkkosivulla/verkkokaupassa ja sosiaalisessa mediassa, sekä jos joku tulee mainitsemaan poikkeamista, mainittiin. Ja esimerkiksi salasanojen vuotamiseen liittyvien uutisten lukeminen sai mikroyrittäjät havahtumaan kyseiseen asiaan.

Olemassa olevat, vanhat tietokoneet oli osittain poistettu, tai ainakin pyritty poistamaan, yritystoiminnan käytöstä. Luotettava ja maksullinen tietoturva- ja virusohjelma koettiin hyödylliseksi hankkia kaikkiin käytettäviin laitteisiin. Toisinaan käytettävät laitteet skannattiin virusten varalta.

Tietoturvariskin havaitseminen käsitti myös valmiiksi tallennetut salasanat ohjelmiin sekä huomion, ettei kaikkialle olisi valmiiksi jo kirjauduttu sisään. Myös päivitykset olisi ajettava säännöllisesti, mieluiten automaattiajolla.

Lisäksi mainittiin omaan käyttäytymiseen liittyviä seikkoja: Koko ajan tulee olla valppaana ja hereillä asian suhteen. Mihinkään ei voi luottaa ja tietynlainen vainoharhaisuus tulee olla. Näiden lisäksi henkilökohtaisen verkoston hyöty eli kysytään muilta, mikäli on jotain arveluttavaa.

Ei se ole joka päivä ajatuksissa, mikään tietoturvariski.

Jos ei ole poikkeavaa näkyvillä verkkosivulla tai somessa, niin jää huomaamatta.

Ehkä joku virustorjunta pitäs läppärillä olla, mulla ei oo kyllä mitään, ehkä tos koneen mukana tulee joku valmiina.

Ehkä jos läppärille ponnahtaa joku ikkuna, niin sille pitäs varmaan jotain tehdä.

Haastattelun tässä vaiheessa mikroyrittäjälle kerrottiin tietoturvan yleinen määritelmä tämän mukaisesti: Tietoturva on tiedon luottamuksellisuuden, eheyden ja saatavuuden ylläpitoa. Tiedon luottamuksellisuus käsittää toimenpiteet, joilla tiedot suojataan luvattoman käytön riskeiltä. Tietojen tulee olla käytettävissä vain henkilöillä ja tahoilla, jotka tietoa tarvitsevat. Tiedon eheydellä varmistetaan tietojen muuttumattomuus. Tiedon tulee pysyä virheettömänä, tiedon määrän ei pidä muuttua itsestään, ja tietojen tulee pysyä siinä

muodossa kuin niiden on alkuperinkin kuulunut olla. Tiedon saatavuudella varmistetaan tiedon käytettävyys. Tiedon tulee olla saatavilla aina tarvittaessa sekä koko sen ajan kuin tietoa on tarve käyttää.

Mikroyrittäjien yleinen kommentointi aiheeseen oli, että tietoturvan määritelmä tulisi sisäistää kokonaan ja se on tärkeä asia, joka jää monta kertaa liian pienelle huomiolle. Mainittiin myös ymmärrys, mistä tietoturvassa on kyse sekä salassapitovelvollisuudet ja mietittiin kirjanpitäjän oikeuksia yrityksen tietoihin. Uutena asiana mainittiin tulleen tietoturvan eheys, jota olikin pidetty itsestään selvänä asiana tähän saakka.

Tietoturva on niin tärkeä, että se jää monta kertaa suhteettoman pienelle huomiolle.

Tämän jälkeen pyydettiin mainitsemaan erilaisia tietoturvan osa-alueita. Mikroyrittäjät mainitsivat laitteet (puhelin, tietokone, muut mobiililaitteet), ohjelmat laitteissa, salasanojen ja erilaisten tunnusten hallinta ja säilytys sekä sähköposti ja sosiaalinen media.

Mainittiin myös käyttäjäturvallisuus, laiteturvallisuus, toimintatavat ja ohjeiden noudattaminen, asiakkaiden, henkilöstön ja pankkien tietoturva. Mainittiin yhteistyökumppanit ja muut verkoston yritykset, yleinen luottamus ja salassapitovelvollisuus. Näiden lisäksi ilmi tuli pankki- ja luottokorttitiedot, asiakastietojen säilytys ja millä luvalla tietoa käytetään sekä tiedon vastaanottaminen, tallentaminen ja säilytys.

Tietokoneella pitää olla turvallisuus kunnossa.

Mikä on oikeasti todellinen, akuutti riski ja mikä vaan harmittaisi, jos se vuotaisi.

Tässä vaiheessa mikroyrittäjille kerrottiin tietoturvan osa-alueista tämän mukaisesti: Hallinnollinen tietoturva pitää sisällään tietoturvajohtamisen ja siihen liittyvät tietoturvasuunnitelman, -linjauksen ja -vastuunjaon. Se yhdistää tietoturvan osa-alueet kokonaisuudeksi, mahdollistaen tietoturvan kehittämis- ja ylläpidolliset toimintaedellytykset. Fyysinen tietoturva sisältää yrityksen toimitilat ja tilojen tärkeysluokitukset, näissä olevien laitteiden suojaamisen lämpötila-, kosteus-, palo-, vesi- ja sähkövahingoilta. Näiden lisäksi tulee ottaa huomioon muun muassa varkauden ja ilkivallan uhat, kulunvalvonta sekä valvontakamerat ja murtosuojaukset. Laitteistoturvallisuus käsittää laitteiden pääsynvalvonnan ja tapahtumatiedot, laitteiston yleisen toimivuuden, laitedokumentoinnin, laitteen varmentamisen (varalaite) sekä varaosien saatavuuden, ylläpito- ja huoltosopimukset. Ohjelmistoturvallisuus tarkoittaa käytettävien ohjelmien ja sovellusten suojaamista (ml. käyttöjärjestelmä ja tietokannat). Suojaaminen tapahtuu muun muassa ohjelmien päivitysten ylläpidolla, pääsynvalvonnalla, tapahtumalokilla, varmuuskopioinnilla ja dokumentoinnilla. Tietoaineistoturvallisuus kattaa yrityksen strategiset tiedot, asiakas- ja henkilöstötiedot, talous- ja hallintotiedot sekä

tuotekehitys-, tuote- ja palvelutiedot. Tähän sisältyy myös tietoaineiston oikeanlainen poisto ja hävittäminen. Tietoliikenneturvallisuus sisältää kaiken mikä liittyy tiedon eli datan välittämiseen käyttäjältä toiselle. Tietoliikenneturvallisuudessa tulee estää väärinkäytöt tietoliikenneyhteyksissä (ml. mobiiliverkko), lähiverkossa ja verkkoon liitetyissä koneissa. Siihen sisältyy myös tietoliikenneverkon välityksellä toimivat virukset, madot ja palvelunestohyökkäykset. Henkilöstöturvallisuus kattaa kaiken missä on osapuolena henkilö eli henkilön käytös, toiminta ja huolellisuus, inhimilliset virheet sekä tietoturvaosaaminen. Siihen liittyy myös henkilövaihtuvuus, yhteistyökumppanit ja alihankkijat sekä palveluntarjoajat digitaalisiin palveluihin (ml. Pilvipalvelut). Käyttöturvallisuus käsittää normaalit käyttötoiminnot. Näitä voivat olla muun muassa käyttöoikeudet, laitteiden ja järjestelmien käyttäminen ja käytön valvonta sekä salasanojen hallinta ja varmuuskopiointi.

Tämän jälkeen mikroyrittäjät havahtuivat näkemään tietoturvan laajempana asiana kuin mitä olivat ajatelleet aikaisemmin ja tietoturvan olevan mukana lähes kaikessa toiminnassa. Huomiona tuli myös kaikkien tietoturvan osa-alueiden liittyvän jokapäiväiseen elämään. Kohtuullinen huolellisuus tulisi olla, etteivät tiedot häviä tai välity ulkopuolisille sekä varmuuskopiointiin tulisi kiinnittää entistä enemmän huomiota.

Sehän on totta, että se on kamalan laaja käsite. mulla oli mielessä vaan laitteet.

Kysymykseen mihin tietoturvariskeihin sinun tulisi kiinnittää huomioita jatkossa, mikroyrittäjät mainitsivat tietokoneen, käyttöoikeudet, päivitykset, salasanat ja varmuuskopiointi. Näiden lisäksi esille nousivat tietoturvapalaverin, -strategian ja -koulutuksen tarpeellisuus ja tiedon jakamisen välineet. Huomiota kiinnitettiin myös toimitilaan ja sen turvallisuuteen. Myös sähköpostihuijaukset, sosiaalinen media ja Google mainittiin.

Tietokoneesta tulisi huolehtia myös silloin kun työskentelee kotoa käsin ja estää ulkopuolisten (ml. Perheenjäsenten) pääsy koneelle. Tietokoneen rikkoutumisen vaara on hyvä tiedostaa ja siinä ei tulisi säilyttää mitään yritystoiminnan kannalta kriittistä tietoa. Lisäksi yrityksen avainhenkilöillä tulisi olla varakone.

Käyttöoikeuksiin tulisi kiinnittää huomiota ja huomioida yrityksen avainhenkilöiden pääsy kaikkeen yritystoiminnan tietoon. Lisäksi tulisi huolehtia, ettei ylimääräisillä henkilöillä ole pääsyä tietoihin. Yleisesti suojeltavina tietoina mainittiin asiakastiedot, henkilökunnan tiedot sekä yrityksen tunnistautumis- ja tilitiedot.

Päivitykset tulisi tarkistaa viikoittain tietokoneelle ja puhelimelle. Tämän lisäksi olisi hyvä olla jokin maksullinen tietoturva- ja virusohjelma kaikkiin käytettäviin laitteisiin. Salasanojen suhteen tulisi huolehtia eri salasana eri palveluihin. Huomio tulisi kiinnittää myös varmuuskopioihin sekä huolehtia ulkoiselle kiintolevylle kopio tietokoneelle tallennetusta tiedosta.

Tietoturvapalavereja tulisi pitää yrityksen henkilöstölle ja tietoturvastrategia tulisi luoda. Lisäksi olisi mietittävä tiedon jakamisen välineitä ja ohjelmia sekä tiedon tallentamista. Myös se, mitä verkossa tehdään, olisi hyvä käydä läpi henkilöstön kanssa. Lisäksi uusien henkilöiden kouluttaminen siihen miten tietoturvan kanssa tulee toimia.

Toimitilaan kohdistuvia riskejä oli murtautumisen mahdollisuus ja valvontakameroiden puute. Lisäksi yrityksen papereiden säilyttäminen työpöydällä ja tietokoneiden fyysinen lukitsemattomuus.

Verkossa toimimisen suhteen Facebook ja muu sosiaalinen media sekä sähköpostiin tulevat huijaukset. Kaksivaiheinen kirjautuminen kaikkialle käyttöön ja esimerkiksi pankin sivuille ei mentäisi selaimen kautta. Lisäksi mietinnässä oli henkilön oma toiminta verkossa ja mistä tietää esimerkiksi, milloin tieto siirtyy pois EU:sta.

Mitä tietoja voi lähettää milläkin lailla?

Kaikki tieto on paperilla, koneella ei ole mitään sellaista tietoa, että jos kone menee rikki.

Miten voi vaikuttaa toisaalta hankittuun palveluun tai ohjelmaan?

Palomuurit on hoidossa, ostettu palvelu.

Mitä on tietojen oikeanlainen hävittäminen, kauanko tietoa tulee säilyttää?

Murron mahdollisuus on olemassa.

Merkittävimmät tekijät tietoturvariskien havaitsemiseen olivat mikroyrittäjien mielestä huomio siitä, että tietoihin on tullut muutos aikaisempaan tai on normaalista poikkeava tapahtuma. Henkilön oma toiminta, inhimilliset tekijät ja virheenmahdollisuudet mainittiin sekä koulutustarve riskeihin ja yleensäkin ohjeiden noudattaminen työssä. Maalaisjärkeä tulisi käyttää ja olla pieni epäilys kaikkeen. Epäilyttäviin asioihin ei pidä lähteä mukaan ja valveillaolo rikollisten toimintaan verkossa tulee huomioida jatkuvasti. Näiden lisäksi tuli ilmi käytettävissä olevien tietoturvaohjelmien ilmoitukset havaituista tietoturvariskeistä sekä reagointi Suomen Yrittäjien julkaisemiin vinkkeihin silloin kun jotakin yritystä on huijattu.

Kukaan ei ole esimerkiksi nostanut mun tililtä rahaa.

Tietojen oikeanlainen hävittäminen pitää olla kunnossa. Tietoturva pitää muistaa päivittäisessä työnteossa.

Jos en näe mitään erikoista, niin en välttämättä edes huomaa.

Mikroyrittäjien mukaan tietoturvan parantaminen vaatii heiltä viitseliäisyyttä ja aikaa sekä yhteistyötä sellaisten tahojen ja yritysten kanssa, jotka tekevät sitä jatkuvasti. Tietoturva tulisi käydä omassa yrityksessä kaikkien kanssa läpi ja luoda toimintatavat, jotka suojaavat yrityksen toimintaa.

Tulisi ottaa salasanaohjelma käyttöön ja varmuuskopioihin kiinnittää huomiota. Ymmärrystä tietotekniikasta pitäisi olla enemmän ja huolehtia, ettei kenelläkään ulkopuolisella (ml. perheenjäsenet) ole pääsyä työkoneelle; voivat esimerkiksi ladata haitallisen ohjelman.

Olisi mietittävä turvalliset keinot ja ohjelmat lähettää tietoa, säilöttyjen tietojen läpikäynti, tarpeettomien tietojen hävittäminen sekä salassa pidettävien tietojen oikeanlainen tuhoaminen. Tulisi huolehtia myös paperilla säilytettävä tieto lukolliseen kaappiin.

Tietoturvaohjelmien ajantasaiset päivitykset tulisi hoitaa sekä varmistaa, että käytettävä tietoturvaohjelma on hyvä ja siihen tulee parannuksia jatkuvasti. Tulisi huomioida myös puhelimeen tarvittavat suojaukset. Vanhat laitteet olisivat hyvä uusia ja hankkia mahdolliset varalaitteet.

Keskittyminen ja kiinnostus tietoturva-asioihin sekä tietoisuus mitä tapahtuu tai mitä voi tapahtua parantaisivat myös mikroyrittäjien mielestä tietoturvaa. Aiheeseen liittyviä uutisia tulisi seurata enemmän. Järki tulisi pitää päässä; ei voi luottaa vain virusturvaohjelmaan.

> *Tällaisia haastatteluja, jotka laittavat miettimään asiaa enemmän.*
>
> *Omalla tyhmyydellä voi tehdä paljon tuhoa.*
>
> *Pitäisi ottaa itseään niskasta kiinni ja ruveta hommiin.*
>
> *Kaikessa on paljon parantamisen varaa.*
>
> *Sellainen koulutuspäivä, että ymmärtäisi oikeasti minkälaisia riskejä on olemassa ja miten reagoida, jos huomaa poikkeaman.*

Viimeinen kysymys mikroyrittäjille käsitteli muuta aiheeseen liittyvää, jonka haluavat mainita haastattelussa. Mainittavia asioita olivat:

- Tulee tarkistaa tietoihin pääsyn käyttöoikeudet ja varmistua siitä, että kaikki tieto ei ole vain yhden henkilön takana.
- Tulee uusia laitteet, jotka ovat tulleet tiensä päähän ja tarkistaa myös ohjelmapäivitykset.
- Jatkossa tulee huomioida pankki- tai luottokortin väärinkäytön mahdollisuus ja tarkistaa säännöllisesti tilitapahtumat.

- Tietoturva on laaja ja monimutkainen aihe. Riskit ei tunnu pahoilta, kun niitä ei käsitä.

Miten turvataan laaja tietoaineisto, jossa on koko yrityksen osa-alueet ja tiedot?

Modeemin pitäisi päivittää itsensä päivittäin automaattisesti.

Yksittäinen ihminen ei voi hakkereille mitään, ohjelmien varassa ollaan.

Pitäisi miettiä mikä olisi omassa yrityksessä kuolemanisku, joka lamaannuttaisi kaiken.

4.6 Johtopäätökset mikroyrittäjien haastatteluista

Mikroyrittäjät tunnistivat tietoturvan yleisen määritelmän ja pitivät sitä tärkeänä, mutta tietoturvan osa-alueista jäi paljon huomioimatta. Tietoturva miellettiin tärkeäksi asiaksi, mutta esimerkiksi tietoturvajohtaminen ja riskienarviointi tuntuivat puuttuvan täysin, kuin myös toipumissuunnitelma. Tietoturva oli taka-alalle jäänyt asia, johon ei tuntunut olevan resursseja; aikaa, rahaa, osaamista tai viitseliäisyyttä. Tietoturvan koettiin olevan hyväksyttävällä tasolla maksullisen tietoturvaohjelman sekä salasanojen ja pankkitunnusten suojaamisen avulla. Tietoturvan miellettiin liittyvän yksityisyyteen ja omaisuuteen.

Mikroyrittäjät kokivat, että heidän tulisi itse hallita ja osata tietoturva-asiat. Halua kehittää ja oppia tietoturvasta enemmän oli olemassa. Päällimmäisenä ajatuksena oli tehdä itse parannusta yrityksen tietoturvaan, vaikkakin koettiin, että osaamista ja aikaa ei ole. Vain yksi mikroyrittäjä mainitsi ajan riittämättömyyden johtavan asiantuntijapalvelun hankintaan ostopalveluna tietoturvan suhteen ja jonkinlaisen koulutuspäivän tarpeellisuuden tietoturvariskeistä.

Tietoisuus tietoturvariskeistä kuitenkin mikroyrittäjillä oli, vaikkakin ne liittyivät melko vahvasti laitteiden ja ohjelmien päivityksiin, salasanojen hallintaan, erilaisiin huijausyrityksiin ja viruksiin. Ohjelmapäivitykset huolehdittiin laitteille, salasanojen hallinta oli retuperällä. Huijausyrityksiin suhtauduttiin suurella varauksella, vaikkakin väsymystä huijausyrityksistä oli havaittavissa. Virusten torjunnan suhteen luotto oli nimenomaan maksullisissa virustorjuntaohjelmissa.

Sen sijaan ulkopuolisen mahdollinen pääsy tietoon koettiin jollakin määrin jopa toimintaa lamauttavaksi tekijäksi; painoarvo oli pankki- ja luottokortin sekä pankkitilin väärinkäytössä ja identiteettivarkauksissa (henkilön, yrityksen). Oli kuitenkin merkittävästi havaittavissa mikroyrittäjien huoli siitä, kuinka huolehtia ja varmistaa oikeus tietoon vain siihen kuuluville henkilöille ja tiedon oikeanlainen hävittäminen. Myös ulkopuolisten pääsyn

mahdollisuudesta yrityksen tiloihin tai tietokoneille, ja näiden kautta ulkopuolisen mahdollisuudesta päästä tietoon käsiksi, kannettiin huolta. Näiden lisäksi riskeinä koettiin verkkorikollisuus, verkon kautta tulevien uhkien yleistyminen ja tiedon joutuminen vääriin käsiin. Etenkin arkaluontoiset tiedot, henkilö- ja henkilöllisyystiedot sekä asiakastiedot pyrittiin pitämään turvassa. Sen sijaan mainintaa ei tullut esimerkiksi yrityksen tuotekehitystiedoista, sopimuksista tai muista vastaavista tiedoista.

Se, mihin jatkossa mikroyrittäjät aikovat kiinnittää tietoturvariskien osalta huomiota, ovat laitteet ja päivitykset. Vanhat laitteet uusitaan ja ohjelmapäivitykset pidetään ajan tasalla. Käyttöoikeudet, salasanojen hallinta ja varmuuskopiot nousivat myös vahvasti esille jatkon kannalta. Havahtuminen tuli myös tietoturvapalaverien järjestämiseen ja mahdollinen lisäkoulutus tietoturvan suhteen koko yrityksen henkilöstölle. Lisäksi mikroyrittäjät miettivät tietoturvastrategian luomista omalle yritykselle. Toimitiloissa huomattiin olevan paljon kehitettävää turvallisuuden osalta ja tämä mainittiin myös jatkotoimenpiteenä.

Kaiken kaikkiaan, mikroyrittäjillä oli käsitys tietoturvan tärkeydestä, he hahmottivat sen laajuuden ja osasivat kertoa yleisiä tietoturvariskejä. Vaikkakin tietoturvan osa-alueisiin peilaten riskejä jäi paljon mainitsematta, kokonaisuutena voi kuitenkin katsoa mikroyrittäjien ainakin pyrkivän tietoturvallisempaan toimintaan, jossa pääkohtina olisi tiedon luottamuksellisuus, eheys ja saatavuus. Näiden menettäminen olisi mikroyrittäjien mielestä musertava tapahtuma yritystoiminnalle. Myös riskien tehokkaampi havaitseminen nousi esille tietoturvan tärkeyden rinnalla sekä oman toiminnan merkitys.

5 Yhteenveto ja pohdinta

Tutkimuksen tavoitteena oli saada suomalaiset mikroyrittäjät ymmärtämään tietoturvan merkitys, mitä tietoturvariskejä on olemassa ja mitä tietoturvariskejä heidän olisi hyvä huomioida enemmän. Näiden lisäksi tietoturvariskien havaitseminen ja tietoturvan kehittäminen olisi hyvä saada osaksi mikroyrittäjän toimintoja ja tietoturvasta huolehtiminen tulisi olla osana riskienhallintaa. Tutkimuksen tavoitteena oli myös löytää vastaus tutkimuskysymykseen. Tutkimuskysymys käsitteli suomalaisten mikroyrittäjien käsityksiä tietoturvariskeistä sekä mihin tietoturvariskeihin heidän olisi hyvä kiinnittää huomiota enemmän.

Mikroyrittäjien teemahaastatteluilla hankittu aineisto oli luotettavaa ja tämä varmistui toistettavuudella; mikroyrittäjät, toisistaan riippumatta, antoivat samankaltaisia vastauksia. Aineiston analysointi keskittyi induktiiviseen analyysiin; lähtökohta ei perustunut teoriaan vaan aineiston tarkasteluun ja aineisto oli pätevää, koska analysointimenetelmä vastasi aineistoa. Teoriaosuuden kirjallisuus ja verkkojulkaisut olivat osittain julkaistu 2000-luvun alkupuolella, mutta käsiteltyjen aiheiden muuttumattomuus piti nämäkin lähteet käyttökelpoisina ja luotettavina.

Tutkimuksen tuloksia tarkastellessa on havaittavissa yksinkertaisen teemahaastattelun myötä jokaisen haastatteluun osallistuneen mikroyrittäjän alkavan miettiä tietoturvaa, ainakin hetkellisesti, uudelta kannalta. Mikroyrittäjät miettivät tietoturvaan ja tietoturvariskeihin liittyviä asioita aidosti innostuneena ja he oivalsivat niihin vaikuttavia tekijöitä, vaikkakin maaperä miellettiin oudoksi ja laajaksi. Myös se, että haastattelussa kerrottiin suoraa tietoa (tietoturvan määritelmä, tietoturvan osa-alueet) sai mikroyrittäjät oivaltamaan mihin tietoturvariskeihin heidän olisi hyvä kiinnittää jatkossa huomiota enemmän.

Arvioidessa tutkimuksen tavoitteen ja tuloksen onnistumista, tutkimuskysymystä silmällä pitäen ja omiin havaintoihini vedoten, sanoisin mikroyrittäjien käsityksien tietoturvariskeistä olevan vaillinaiset, jopa niukat. Pääsääntöisesti riskit tiedostetaan jokapäiväisen toiminnan kautta, mutta riskien aihealueet ovat suppeat. Tietoturvariskit tunnistetaan vain niistä toiminnoista, joita käytetään säännöllisesti tai joista uutisoidaan. Liiketoimintaan vaikuttaville tietoturvariskeille ei anneta aikaa, eikä riskien toteutumisen vähentämisestä ja ennaltaehkäisystä olla valmiita maksamaan rahaa. Se, että jokin riski oli aikaisemmin jo toteutunut, oli saanut mikroyrittäjät havahtumaan. Siltikin toteutuneiden tapahtumien myötä tulleet havahtumiset eivät kantaneet kovin pitkälle, eikä niiden eteen tehty merkittäviä toimenpiteitä.

Näin ollen, viitseliäisyys vaikuttaa tietoturvan tasoon ja sen myötä riskien mahdollisuuteen ja niiden hallintaan. Voidaanko jopa ajatella, että mikroyrityksissä on hyväksyttävänä tietoturvalinjauksena ja menettelytapana motivaation puute? Tätä seikkaa tukisi resurssien

puutteista aika ja viitseliäisyys. Mikäli yrityksen johto priorisoisi tietoturvan kehitettävien toimenpiteiden kärkeen, siihen olisi löydyttävä motivaatio, käytettävä aikaa. Motivaation myötä löytyy monesti myös rahaa, mikäli haluttu lopputulos olisi sillä saavutettavissa. Loppujen lopuksi vastuu on aina yrityksen johdolla ja mikroyrityksessä monesti yrityksen johto on sama kuin mikroyrittäjä.

Ehkä se, että mikroyrittäjä kerrankin varasi aikaa tietoturvalle, edes haastattelun verran, voisi luoda jatkumon, jossa mikroyrittäjä ymmärtäisi motivaation merkityksen tietoturvan parantamiseen. Näin toimien mikroyrittäjä loisi yrityksellensä tietoturvapolitiikan, jonka kautta tietoturvaa olisi mahdollista kehittää ja ylläpitää ja näin ollen saada käsitys omaan liiketoimintaan vaikuttavista tietoturvariskeistä ja saada tieto niistä tietoturvariskeistä, joihin olisi hyvä kiinnittää huomio jatkossa.

Teoriaosuuden ja asiantuntijoiden haastatteluiden perusteella voidaan todeta tietoturvan kehittämisen alkavan riskien tunnistamisella ja arvioinnilla sekä tiedostamalla tietoturvan olevan osa laajempaa kokonaisuutta. Kokonaisuutta, jonka tarkoitus on hallita riskit ja sen myötä mahdollistaa liiketoiminnan jatkuvuus.

Mikäli yrityksellä ei ole tietoturvalinjausta, kuinka tietoturvan ylläpito ja kehittäminen on mahdollista? Kuinka tällöin voidaan tiedostaa tietoturvariskit, jotka vaikuttavat juuri oman yrityksen toiminnan jatkuvuuteen? Koska suomalaisilla mikroyrittäjillä ei ole mietittynä kriittisiä riskejä liiketoiminnan jatkuvuuden kannalta, mielestäni tässä saadaan vastaukset tämän tutkimuksen tutkimuskysymykseen: Suomalaisilla mikroyrittäjillä ei ole käsitystä tietoturvariskeistä, eikä siitä, mihin tietoturvariskeihin heidän olisi hyvä kiinnittää huomiota enemmän.

Haastattelun aikana mikroyrittäjille tuli paljon uusia ajatuksia tietoturvan ja tietoturvariskien suhteen ja sai mikroyrittäjän tekemään jonkin toimenpiteen. Toimenpiteitä olivat esimerkiksi käytettävän modeemin päivitysten tarkistaminen tai kannettavalle tietokoneelle salasanan käyttäminen käynnistyksen yhteydessä. Pieniä tekoja, mutta tekoja tietoturvan eteen joka tapauksessa.

Olisi hyvä tutkia enemmän, kuinka mikroyrittäjien motivaatiota saisi nostettua tietoturvan toteuttamiseen tai kuinka esille tulleita suuriakin tietoturvalinjauksia voisi tukea tai esimerkiksi opinnäytetyönä luoda mikroyritykselle tietoturvastrategia. Myös tietoturva ja tietosuoja termit sekoittuivat jonkin verran keskenään mikroyrittäjillä; tätäkin voisi tutkia enemmän ja kuinka termien sekoittuminen vaikuttaa toimintaan. Onko kuvitelma se, että kun tietosuoja on kunnossa, niin silloin myös tietoturva on kunnossa?

Yleinen hyödynnettävyys tälle tutkimustulokselle on merkittävä. Oma toiveeni on, että mikroyrittäjät poimisivat tästä ne itselleen tärkeät seikat ja aloittaisivat jonkin toimenpiteen

tietoturvan eteenpäin viemiseksi. Lisäksi erilaiset palveluntarjoajat voivat hyödyntää kerättyä materiaalia ja tutkimustulosta omassa liiketoiminnassaan. Tulee myös ottaa huomioon se, että vaikka tässä tutkimuksessa kohderyhmänä oli mikroyrittäjät, samat asiat koskettavat myös suurempia yrityksiä sekä henkilöitä.

Kaiken kaikkiaan, tämän tutkimuksen tulos saavutti sille määritellyt tavoitteet. Suomalaisten mikroyrittäjien käsityksissä tietoturvariskien suhteen on parannettavaa, teemahaastattelun myötä mikroyrittäjät saatiin ymmärtämään tietoturvan merkitys. Se mihin tietoturvariskeihin he jatkossa kiinnittävät huomiota, riippuu pitkälti käytettävistä resursseista, vaikkakin niiden puute on suurin syy suomalaisten mikroyritysten tietoturvan kehittymiselle.

Lähteet

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma Oy.

Avosorsa Oy. 2021. Meistä. Viitattu 18.12.2021. Saatavissa: https://www.avosorsa.fi/meista-wordpress-yllapito-osaaja-nettisivujen-kotisivujen-tekija-sisallontuottaja/

Bell, D.E. & La Padula, L. 1976. Secure Computer System: Unified Exposition and MULTICS Interpretation, MTR-2997 Rev. 1. Viitattu 22.2.2022. Saatavissa: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/bell76.pdf

Clark, D.D. & Wilson, D.R. 1987. A comparison of commercial and military computer security policies. Viitattu 22.2.2022. Saatavissa: http://theory.stanford.edu/~ninghui/courses/Fall03/papers/clark_wilson.pdf

Deloitte Touche Tohmatsu Limited. 2017. Global risk management survey, 10th edition. Viitattu 26.2.2022. Saatavissa: https://www2.deloitte.com/global/en/insights/topics/risk-management/global-risk-management-survey.html

Elinkeinoelämän keskusliitto. 2021. Yritykset. Viitattu 24.2.2022. Saatavissa: https://ek.fi/tutkittua-tietoa/tietoa-suomen-taloudesta/yritykset/

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo Finland Oy.

Helsingin yliopisto. 2011. Tietoturvan perusteet. Viitattu 20.2.2022. Saatavissa: https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_11.pdf

Journal. 2014. Mikroyrittäjien työhyvinvointi. Viitattu 24.2.2022. Saatavissa: https://journal.fi/tyoelamantutkimus/article/view/87162

Jyväskylän yliopisto. 2009. Validiteetti ja reliabiliteetti. Viitattu 24.2.2022. Saatavissa: http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo Finland Oy.

Järvinen, P. 2012. Arjen tietoturva – vinkit & ratkaisut. Jyväskylä: Docendo.

Kauppalehti. 2022. Kysely yrittäjille: Tietomurrot ovat liiketoimintariski – osaamisen puute on suurin tietoturvan hidaste. Viitattu 8.4.2022. Saatavissa:

https://www.kauppalehti.fi/uutiset/kysely-yrittajille-tietomurrot-ovat-liiketoimintariski-osaamisen-puute-on-suurin-tietoturvan-hidaste/c25e7cc7-7ecf-4186-bb2f-eae763ac3f13

Karsisto, T. 2007. Tietoturvariskianalyysin tehostaminen työkalun avulla. Helsingin teknillinen korkeakoulu. Viitattu 24.2.2022. Saatavissa: http://lib.tkk.fi/Dipl/2007/urn007703.pdf

Kyberturvallisuuskeskus. 2020. Tietoturva. Viitattu 22.2.2022. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Kyberturvallisuuskeskus. 2022. Kybersää. Viitattu 22.02.2022. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

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

Liikenne- ja viestintävirasto Traficom. 2020. Tietoturva. Viitattu 24.2.2022. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Viitattu 15.4.2022. Saatavissa: https://kirja.elisa.fi/ekirja/kyberturvallisuus

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Jyväskylä: Talentum Media Oy.

Neittaanmäki, P., Lehto, M. & Savonen, M. 2021. Yhteiskunnan digimurros. Jyväskylän yliopisto. Viitattu 24.2.2022. Saatavissa: https://jyx.jyu.fi/bitstream/handle/123456789/75328/Yhteiskunnan%20digimurros.pdf?sequence=1&isAllowed=y

Pollari, E. 2021. Tietoturvariskien hallinta organisaatioissa. Jyväskylän yliopisto. Viitattu 24.2.2022. Saatavissa: https://jyx.jyu.fi/bitstream/handle/123456789/77437/URN%3ANBN%3Afi%3Ajyu-202108204602.pdf?sequence=1&isAllowed=y

Rautiainen. J. 2013a. Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus. Juhan IT-blogi. Viitattu 24.2.2022. Saatavissa: https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/

Rautiainen. J. 2013b. Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus. Juhan IT-blogi. Viitattu 24.2.2022. Saatavissa: https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/

Rousku, K. 2014. Kyberturvaopas - Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

STT Viestintäpalvelut. 2021. Tietoturva-asiantuntija listaa: Kolme tärkeää perusasiaa, joista jokaisen tulisi huolehtia – kodin laitteiden elinkaari luo uusia tietoturvahaasteita. Viitattu 16.4.2022. Saatavissa: https://www.sttinfo.fi/tiedote/tietoturva-asiantuntija-listaa-kolme-tarkeaa-perusasiaa-joista-jokaisen-tulisi-huolehtia-kodin-laitteiden-elinkaari-luo-uusia-tietoturvahaasteita?publisherId=1881&releaseId=69899122

Suomen Yrittäjät. 2020. Miten suojata yrityksen arkaluontoiset tiedot? Mitä tietoturva maksaa? Lue asiantuntijoiden neuvot – ”Tärkeintä olla kiinnostunut”. Viitattu 16.4.2022. Saatavissa: https://www.yrittajat.fi/uutiset/miten-suojata-yrityksen-arkaluontoiset-tiedot-mita-tietoturva-maksaa-lue-asiantuntijoiden-neuvot-tarkeinta-olla-kiinnostunut/

Suomidigi. 2020. Vahti 8/2017 Tietoturvapoikkeamatilanteiden hallinta. Viitattu 14.4.2022. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-82017-tietoturvapoikkeamatilanteiden-hallinta

Tampereen yliopisto. Teemahaastattelu. Viitattu 19.12.2021. Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_2.html

Tieteen termipankki. 2022a. Terminologisen sanastot 2. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/mot/mot.exe?Opt=256&ListWord=@40@40ID@3DTSKTT@2DID1&SearchWord=tietoturva&dic=1&page=results&UI=figr&Source=Record

Tieteen termipankki. 2022b. Terminologiset sanastot 2. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/mot/mot.exe?Opt=256&ListWord=@40@40ID@3DTSKTT@2DID1&SearchWord=tietoturva&dic=1&page=results&UI=figr&Source=Record

Tieteen termipankki. 2022c. Terminologiset sanastot 2. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/mot/mot.exe?Opt=256&ListWord=@40@40ID@3DTSKTT@2DID1&SearchWord=tietoturva&dic=1&page=results&UI=figr&Source=Record

Tieteen termipankki. 2022d. Terminologiset sanastot 2. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/mot/mot.exe?Opt=256&ListWord=@40@40ID@3DTSKTT@2DID1&SearchWord=tietoturva&dic=1&page=results&UI=figr

Tieteen termipankki. 2018. TEPA-termipankki. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/fi/haku/haavoittuvuus

Tieteen termipankki. 2004. TEPA-termipankki. Viitattu 24.2.2022. Saatavissa: https://termipankki.fi/tepa/mot/mot.exe?Opt=256&ListWord=@40@40ID@3D@22TSK@5

F31@2DIDEU7iHytELW0e06t7dybc5w@22&SearchWord=tietoturva&dic=1&page=results&UI=figr&Source=Record

Tilastokeskus. Mikroyritys. Viitattu 24.2.2022. Saatavissa: https://www.stat.fi/meta/kas/mikroyritys.html

Tirronen, H. 2003. Tietoturvan osa-alueet. Viitattu 1.3.2022. Saatavissa: http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html

Liite 1. Asiantuntijahaastatteluiden kysymykset

1. Kuvaile miten käsität tietoturvan.
2. Mainitse erilaisia tietoturvariskejä.
3. Mihin tietoturvariskeihin mielestäsi mikroyrittäjän tulisi kiinnittää huomioita?
4. Kuinka mikroyrittäjä voi havaita tietoturvariskejä?
5. Mitkä ovat mielestäsi mikroyrittäjän suurimmat esteet tietoturvan parantamiseen?
6. Miten näet tietoturvariskien muuttuvan seuraavan vuoden aikana?
7. Onko näkyvissä joitakin trendejä, jotka tulevat vaikuttamaan tietoturvaan?
8. Miten näet, että mikroyrittäjien tulisi varautua tietoturvariskeihin seuraavan vuoden aikana?
9. Haluatko sanoa vielä jotain muuta näihin liittyvää?
10. Mitä terveisiä haluaisit lähettää tietoturvaan liittyen suomalaisille mikroyrittäjille?

Liite 2. Mikroyrittäjähaastatteluiden kysymykset

1. Kuvaile miten käsität tietoturvan.
2. Mainitse erilaisia tietoturvariskejä.
3. Mihin tietoturvariskeihin kiinnität huomioita nykyisessä toiminnassasi? Ja miten?
4. Mitä tietoturvariskin havaitseminen vaatii sinulta?
5. Mainitse erilaisia tietoturvan osa-alueita.
6. Mihin tietoturvariskeihin sinun tulisi kiinnittää huomioita jatkossa?
7. Mitkä sinusta ovat merkittävimmät tekijät tietoturvariskien havaitsemiseen?
8. Mitä tietoturvan parantaminen vaatii sinulta?
9. Onko jotain muuta tähän liittyvää, mitä haluat mainita?