Markus Hölsä

KYMENLAAKSON KYBERTURVAKAR-TOITUS

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Markus Hölsä
Työn nimi	Kymenlaakson kyberturvakartoitus
Toimeksiantaja	Kyberturvallisuuden tulevaisuus Kymenlaaksossa -hanke
Vuosi	2024
Sivut	66 sivua
Työn ohjaaja(t)	Kimmo Kääriäinen, Vesa Kankare

TIIVISTELMÄ

Maailmassa tapahtuneet geopoliittiset muutokset ja koronaviruspandemia toivat kyberturvallisuuden median kautta yleisön tietoon. Useat kyberhyökkäykset ja huijausten määrän lisääntyminen yrityksiä kohtaan ovat luoneet huolen yritysten kyberturvasta. Tässä tutkimuksessa pyritään saamaan selville Kymenlaakson yritysten kyber- ja tietoturvatoimien tilanne sekä yrittäjien oma käsitys yrityksiensä kyber- ja tietoturvaan. Tutkimuksessa pyritään myös saamaan selko siitä, täsmääkö yrittäjien käsitys yrityksen tilanteesta konkreettisten toimien kanssa. Tutkimuksen toimeksiantajana toimii Kyberturvan tulevaisuus Kymenlaaksossa -hanke, jota rahoittaa Kymenlaakson oikeudenmukaisen siirtymän rahasto (JTF).

Teoriaosassa käytiin läpi yleisimpiä yritysten uhkia, joiden pohjalta luotiin hyvien kyber- ja tietoturvien käytännöt. Käytännöt luotiin yleisimpien uhkien pohjalta ja niiden tarkoitus on tarjota tukea aineiston analyysiin tarvittavan tasotaulukkotyökalun luomisessa. Uhkien ja hyvien käytäntöjen osiot laadittiin kattavalla määrällä alan sekundääriaineistoa, jonka pohjalta pystyttiin tasotaulukon lisäksi myös luomaan yrityskysely.

Tutkimus toteutettiin pääsääntöisesti määrällisenä tutkimuksena. Tutkimusaineisto kerättiin yrityksille tehdyn puhelinhaastattelun avulla, jonka suoritti Taloustutkimus Oy. Haastattelu suoritettiin kyselymuotoisena 432 Kymenlaaksolaiselle yritykselle, jossa vastaajana toimi joko yrityksen toimitusjohtaja tai vastaava tekninen päällikkö. Kyselyn teoreettiset tulokset muutettiin empiiriseen muotoon operationalisoinnin avulla. Tämän avulla aineistoanalyysi pystyttiin analysoimaan määrällisen tutkimusotteen mukaisesti.

Tutkimustulosten perusteella yritysten kyber- ja tietoturvatilanne on tietosuojan, asiakastietojen ja jatkuvuuden kannalta heikko. Tulokset toivat vahvasti esille myös mahdolliset ongelmat yrittäjien käsityksen ja konkreettisten toimien välillä. Kuitenkin suuressa osassa yrityksistä on käytössään suojausohjelmistoja ja monivaiheinen tunnistautuminen.

Tutkimus toi esille Kymenlaakson yritysten kyberturvatilanteen ja loi selkoa yrittäjien tietoisuuteen aiheeseen. Tutkimus korostaa tietoisuuden lisäämistä varsinkin Kymenlaakson yrittäjien keskuuteen. Tämä voidaan saavuttaa mahdollisten tiedotuskampanjoiden avulla sekä kyberturvaan liittyvällä hanketoiminnalla.

Asiasanat: Kymenlaakso, kyberturva, tietoturva, yrityskysely

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Markus Hölsä
Thesis title	Cybersecurity mapping of Kymenlaakso
Commissioned by	Cyber resilient Kymenlaakso -project
Time	2024
Pages	66 pages
Supervisor	Kimmo Kääriäinen, Vesa Kankare

ABSTRACT

Geopolitical changes in the world and the coronavirus pandemic brought cybersecurity to the public's attention through the media. Several cyber-attacks and an increase in the number of scams against companies have created concerns about the cybersecurity in companies. The objective of the study was to examine the situation of companies in Kymenlaakso in terms of cyber and information security measures, as well as the entrepreneurs' own perception of their company's cyber security. The study also aimed to find out whether the entrepreneurs' perception of their company's situation matches the concrete actions taken. The study was commissioned by the Cyber resilient Kymenlaakso project, funded by the Kymenlaakso Just Transition Fund (JTF).

The theoretical part covered the most common threats to businesses, based on which good cyber and information security practices were created. The practices were intended to serve as a tool for creating a spreadsheet for the analysis of the data. The threats and good practices were created using the relevant literature of the subject, which allowed not only the creation of a spreadsheet for the analysis but also a business survey.

The survey was mainly conducted as a quantitative study. The survey data was collected through a telephone interview with companies, conducted by Taloustutkimus Oy. The interview was conducted in the form of a questionnaire for 432 companies in Kymenlaakso, where the respondent was either the chairman or the responsible technical manager of the company. The theoretical results of the survey were transformed into an empirical form by operationalization. This enabled the data analysis to be analyzed in accordance with the quantitative research approach.

The survey results show that companies’ cyber and information security situation in terms of data protection, customer data and continuity is weak. The results also strongly reveal potential problems between entrepreneurs' perceptions and concrete actions. However, the vast majority of companies have security software and multi-factor authentication in place. The study highlights the importance of increasing entrepreneurs’ awareness of cybersecurity issues in Kymenlaakso. This can be achieved through possible awareness campaigns and project activities related to cybersecurity.

Keywords: Kymenlaakso, cybersecurity, information security, survey

SISÄLLYS

1 JOHDANTO

Kyberturvallisuus terminä on luonut pelkoa ja epävarmuutta yrittäjissä sekä organisaatioissa niin pitkään kun aiheesta on puhuttu mediassa. Maailmalla yritykset näkevät oman digitaalisen ympäristönsä suojaamisen usein edelleenkin kuluna, joka täytyy vain hoitaa alta pois. Kuitenkin nykymaailman tilannekuva on muuttunut merkittävästi politiikan sekä erityisesti kyberturvan kannalta, jonka takia digitaalisten ja tietoteknisten laitteiden sekä ohjelmistojen turvallisuuden selvittäminen yrityksissä on erittäin ajankohtainen aihe. Jyväskylän yliopiston artikkelissa Kyberhyökkäysten määrä kasvaa vuosittain – yritysten osaamisessa ja varautumisessa suurta vaihtelua (2022) mukaan suomalaisiin yrityksiin ja organisaatioihin kohdistuvat kyberhyökkäykset ovat nousussa ja varautuminen niihin on vaihtelevaa. Mattila ym. (2020, 22) huomauttivat selvityksessään pienten, keskisuurten ja suurien yritysten kyberturvavaikeuksista verrattuna eurooppalaiseen keskiarvoon. Yleisimmät syyt yrityksen koosta riippumatta olivat tietojen tuhoutuminen, joko inhimillisestä virheestä tai haitta/kiristyshaittaohjelman seurauksena, tietojen päätyminen vääriin käsiin ja palvelunestohyökkäykset. Myös tietovuodot aiheuttivat vahinkoa enemmän suomalaisille yrityksille kuin Euroopassa yleensä.

Vuosien 2022 ja 2023 aikana tehty Kyberturvan ABC -hanke toi ilmi yrittäjien vaikeudet ymmärtää kaikkea, mitä oman yrityksen kyber- ja tietoturvaan liittyy. Tätä huomiota tukee myös Digital Innovation Hub -selvitys, jossa on käynyt osittain ilmi monet puutteet yritysten sekä yritysjärjestöjen kyber- ja tietoturva osa- sekä vastuualueista. DIH-hankkeen aikana tehdyssä selvityksessä yrityskonsultit tiedottivat, että heidän asiakkaillaan on erittäin hyvää osaamista vain neljällä digitalisaation osaamista mittaavalla alalla kahdestakymmenestä kysytystä taidosta. Yrityskonsultit myös epäilivät yrittäjien heikkoa osaamista tai taitojen puuttumista niissä taidoissa, joita yrittäjät itse uskovat olevan erinomaisella tai hyvällä tasolla (Digital Innovation Hub Kymenlaakso -hanke 2022.) Tämä voi olla merkki siitä, että yritykset eivät välttämättä tiedä kaikkea sitä vastuuta, joka niille kuuluu ja yritysjärjestöt eivät ole syystä tai toisesta yrittäjille näistä myöskään tiedottaneet tai opastaneet. Myöskään Kymenlaakson seudulla ei ole otettu selvää yritysten yleisestä kyber- ja tietoturvatasosta, joka luo epätietoisuutta tulevaisuudessa.

Jos yritysten kyber- ja tietoturvatasoa ei saada selville, voi se luoda valheellisen kuvan alueen oikeasta varustautumisesta vakaviin uhkiin tulevaisuudessa. Ilman oikeanlaista tietoa voidaan investointeja sekä hankintoja keskittää muualle jättäen Kymenlaakson varustautumisen huonolle tasolle. Yritykset myös usein vähättelevät kyberturvan merkitystä tai eivät yksinkertaisesti tiedä mitä siihen kuuluu. Näiden asioiden selville saaminen luovat motiivin aiheen tarkemmalle tarkastelulle ja tutkimukselle. Opinnäytetyöllä pyritään selvittämään millä tasolla yritykset ovat omassa kyberturvallisuuden varustautumisessa ja kuinka tosissaan yritykset ottavat tämän osa-alueen. Opinnäytetyössä myös selvitetään Kymenlaakson yritysten oikea kyberturvataso, jota ei peitä pelkät kuulo- ja luulopuheet. Lisäksi saadaan selvityspohja TKI-toiminnalle, jonka tuloksien avulla pyritään lisäämään kyberturva-aiheisia hankkeita Kymenlaaksossa. Työstä hyötyvät täten TKI-toiminnan henkilökunta sekä Kymenlaakson yrittäjäjärjestöt, jotka voivat käyttää opinnäytetyötä pohjana omille kyberturvaan liittyviin ohjeisiinsa Kymenlaaksossa.

2 TUTKIMUSASETELMA

2.1 Tutkimusote

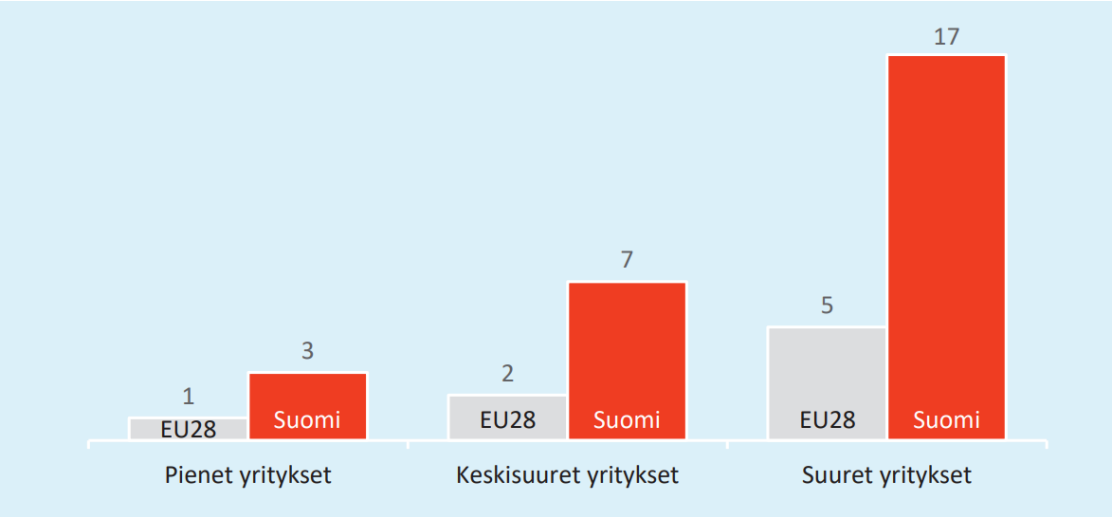
Opinnäytetyön tavoitteena on pyrkiä selvittämään Kymenlaakson yritysten kyberturvallisuusvarustautumista ja oman yrityksen kyber- ja tietoturvaa. Koska aiheesta ei ole aikaisemmin tehty Kymenlaakson tai Suomen alueella kattavaa analyysia, tulisi tutkimuksen metodologian olla kvalitatiivinen eli laadullinen tutkimus. Kvalitatiivinen tutkimusote pyrkii ongelman ymmärtämiseen ja vastaamiseen, tutkimuksella halutaan nimenomaan antaa raamit ilmiölle ja vastata kysymykseen ”Mistä tässä on kyse?” (Kananen 2019, 25.) Kuitenkin tutkimuksen pääpiirteet eivät täysin tue kvalitatiivisen tutkimusotteen luonnetta, koska tutkimuksessa pyritään yleistämään tämänhetkistä tilannetta Kymenlaaksossa (Kananen 2017, 44). Myös pääsääntöinen aineiston keruu tullaan saamaan kyselyn kautta, joka vahvistaa tutkimusotteeksi määrällisen tutkimuksen. Tosin vaikka pääsääntöiseksi tutkimusotteeksi määräytyy määrällinen tutkimus, ei se poissulje laadullisia tutkimuskeinoja työn toteutuksesta. Määrälliseen tutkimuksen pääpiirre edellyttää ilmiön tuntemista, koska siinä pyritään yleistämään. Pääkeinona määrällisen tutkimuksen tiedonkeruu mene-

telmänä on kyselyt, joiden luomiseen tarvitaan vahva ymmärrys jo tutkittavasta ilmiöstä. Tutkittavan ilmiön vahva perusluontoinen ymmärrys saadaan aikaan selittävien mallien ja teorioiden kautta (Kananen 2019, 25.) Kyselyn toteuttaa Taloustutkimus Oy, joka toteuttaa kyselyn 430 yrityksen päättäjälle ja tarjoaa kyselyaineiston aineistoanalyysia varten. Näin suuri otanta vahvistaa opinnäytetyön validiteettia ja reliabiliteettia huomattavasti. Opinnäytetyö tullaan tekemään Kyberturvan tulevaisuus Kymenlaaksossa -hankkeen toimeksiantona ja Taloustutkimuksen palvelut on hankittu hankerahoituksen avulla.

Vaikka kyselyt ovat lähtökohtaisesti pääkeino selvittää nykyistä tilannetta, eivät ne riitä luomaan vertailukohdetta, jos sitä ei ole alun perin määritelty. Kyselyjen lisäksi tarvitaan määrittää hyvä perustaso kaikille yrityksille. Tämä toteutetaan kaikkiin yrityskokoihin pätevällä kyberhygieniatasotaulukolla, joka pitää sisällään keinon määrittää minkälainen minimitaso kyberturvassa tulisi olla yrityksen koosta riippumatta. Tasotaulukkoon verrataan jokaista yritystä ja niiden antamia vastauksia, jotta voidaan päätellä myös se, että onko yrityksellä minimivaatimukset kunnossa ja missä olisi parantamisen varaa. Tämän luomiseen tarvitaan huomattava määrä kirjallisuuden tutkielmia ja lähteitä, jotta voidaan varmasti luoda yhtenäinen taulukko kaikille yrityksille. Kirjallisuutta ja tutkimuksia hyvistä kyberturvatavoista on olemassa runsaasti, tämän takia tasotaulukko ei täytä laadullisen tutkimuksen määritelmää ilmiöstä, josta ei ole aikaisempia teorioita, tietoja tai tutkimuksia (Kananen 2017, 32)

2.2 Tutkimusongelma ja tutkimuskysymykset

Johdantoluvussa mainittiin suomalaisten yritysten heikko kyberturvatilanne, kun sitä verrataan muuhun Eurooppaan. Kymenlaakso on laaja alue, jossa Taloustutkimuksen kyselyn yhteydessä antaman TOL-taulukon mukaan on noin 5 000 toiminnassa olevaa yritystä. Näistä yritysten kyber- ja tietoturvatasosta ei ole luotu kattavaa analyysia aikaisempien tietojen mukaan. Kun huomioidaan Digital Innovation Hub Kymenlaakso -hankeen (2022) selvitys yrittäjien ja yritysneuvojien huonoista digitalisaatio- sekä kyberturvataidoista, on kyber- ja tietoturva kyselyn luomisessa se vaara, että yrittäjät eivät tiedä yritystensä oikeaa tasoa. Sen takia kysely tulee luoda tämä asia huomioon ottaen. Tätä tukee myös alla oleva Mattilan ym. (2020, 23) digibarometrin tulos tietovuodon kohteeksi joutuneista yrityksistä.



Kuva 1. Tietovuodon kohteeksi joutuneet yritykset kokoluokittain (2019), % (Mattila ym. 2020, 23)

Jos otetaan huomioon Suomen yritysten heikentynyt kyberturvallisuuden taso ja mahdollinen yrittäjien tietämättömyys aiheeseen, voidaan muodostaa tutkimusongelma tutkimukselle: *tietävätkö Kymenlaakson yrittäjät oikeasti mitä kaikkea heidän yrityksensä kyberturvaan liittyy?* Jos kyberongelmat yrityksissä jatkavat kasvuaan, täytyy selvittää, mistä tämänkaltainen ilmiö johtuu ja mitkä ovat siihen johtavat tekijät.

Tutkimusongelmaa tukevat tutkimuskysymykset ovat:

1. Mitkä ovat yleisimmät kyberturvauhat suomalaisille yrityksille?
2. Kuinka määrittää yritysten oikea kyber- ja tietoturvatilanne?
3. Mikä on Kymenlaakson yritysten kyber- ja tietoturvan oikea tilanne?

Tutkimuskysymysten avulla pyritään rajaamaan yleisesti ottaen laajaa tutkimusongelmaa ja antamaan tarkemmat raamit opinnäytetyön tekemiseen ja sitä kautta tutkimusongelman vastaamiseen.

2.3 Aineistonkeruumenetelmät

Jotta tutkimusongelmaan saadaan tarvittava ratkaisu, tulee tutkimuksessa määrittää oikeat aineistonkeruumenetelmät. Tämänkaltainen tutkimus tulee siis vaatimaan primääri- sekä sekundääriaineistoa. Pelkästään yrittäjien oma mielipide yrityksen omaan turvallisuus tasoon ei riitä, vaan yrittäjiltä saatu tieto pitää pystyä vertaamaan paljon teknisempään ja ei niin vapaamuotoiseen kyselyyn.

Primääriaineisto

Primääriaineisto on jotain ilmiötä tai tutkimusta varten kerättyä tietoa, jonka kautta saatu vastaus vaatii analyysimenetelmien käyttöä (Kananen 2017, 83). Koska suurinta osaa aineistosta tullaan keräämään tutkimusongelmaa varten kyselyjen muodossa, täytyy määrittää kyselyjen taso, kenelle ne tullaan lähettämään ja kuinka anonymisoida kyselyjen vastaukset. Yrittäjille tullaan lähettämään strukturoitu kysely, joka pitää sisällään kartoitus-, mielipide- ja tarkentavat kysymykset. Kartoituskysymyksillä pyritään saamaan selville yrityskoko ja kunta, jossa yritys sijaitsee. Mielipidekysymyksillä saadaan selville yrittäjien oma suhtautuminen yrityksen kyber- ja tietoturvaan sekä mitä he ajattelevat kyseisestä aiheesta. Tarkentavat kysymykset koskevat itse yrityksessä olevia kyber- ja tietoturvakäytäntöjä. Taloustutkimus hoitaa kyselyn toteuttamisen Kymenlaakson yritysten päättäjiltä. Yrittäjiltä ja yrityksiltä ei tulla kysymään sellaisia tietoja, joiden avulla kyselyn kautta saadut vastaukset voidaan yhdistää yksittäisiin yrittäjiin, yrityksen henkilökuntaan tai yritykseen.

Kyselypohjaisessa määrällisessä tutkimuksessa on huomattava määrä käsitteitä, joita tulee selvittää tutkimuksen toistettavuuden vuoksi. Nämä käsitteet liittyvät itse kyselyn sisältöön sekä kyselyyn itsessään. Ilman oikeankokoista tutkimusaineistoa ja sen määritystä ei pystytä vastaamaan tutkimusongelmaan kattavasti (Vilkka 2021, 80). Tutkimuksessa tullaan käyttämään kaikenkokoisia Kymenlaakson yrityksiä perusjoukkona. Kyseinen perusjoukko pitää sisällään kaikki havaintoyksiköt, jotka luovat kyselylle tärkeän otantamenetelmän. Koska tutkimuksessa pyritään nimenomaan selvittämään yritysten kyber- ja tietoturvatasoa, tulee otantamenetelmänä käyttää ryväsotantaa. Ryväsotanta tukee kyselyjä, joiden pohjana ovat luonnolliset ryhmät, näihin kuuluu esimerkiksi koululuokat, yritykset, organisaatiot, kotitaloudet ja kaupunginosat (Vilkka 2021, 80). Ryväsotannassa voidaan myös käyttää muita otannan muotoja, joka tässä työssä tulee olemaan yksinkertainen satunnaisotanta. Yksinkertaisessa satunnaisotannassa kaikilla perusjoukon havaintoyksiköillä on samansuuruinen todennäköisyys tulla valituksi (Tietoarkisto s.a.) Kaikki yritykset, jotka löytyvät Taloustutkimuksen yritysluettelosta ovat osa tätä otantaa. Osaa toimialoista on kuitenkin suosittu enemmän kuin toisia, näissä suosituissa toimialoissa on suurempi tarve hyvälle kyber- ja tietoturvalle, jonka takia

ne on valittu. Alle on taulukoitu toimialat ja niiden yritysotannat, joilta kysely pääsääntöisesti kysytään.

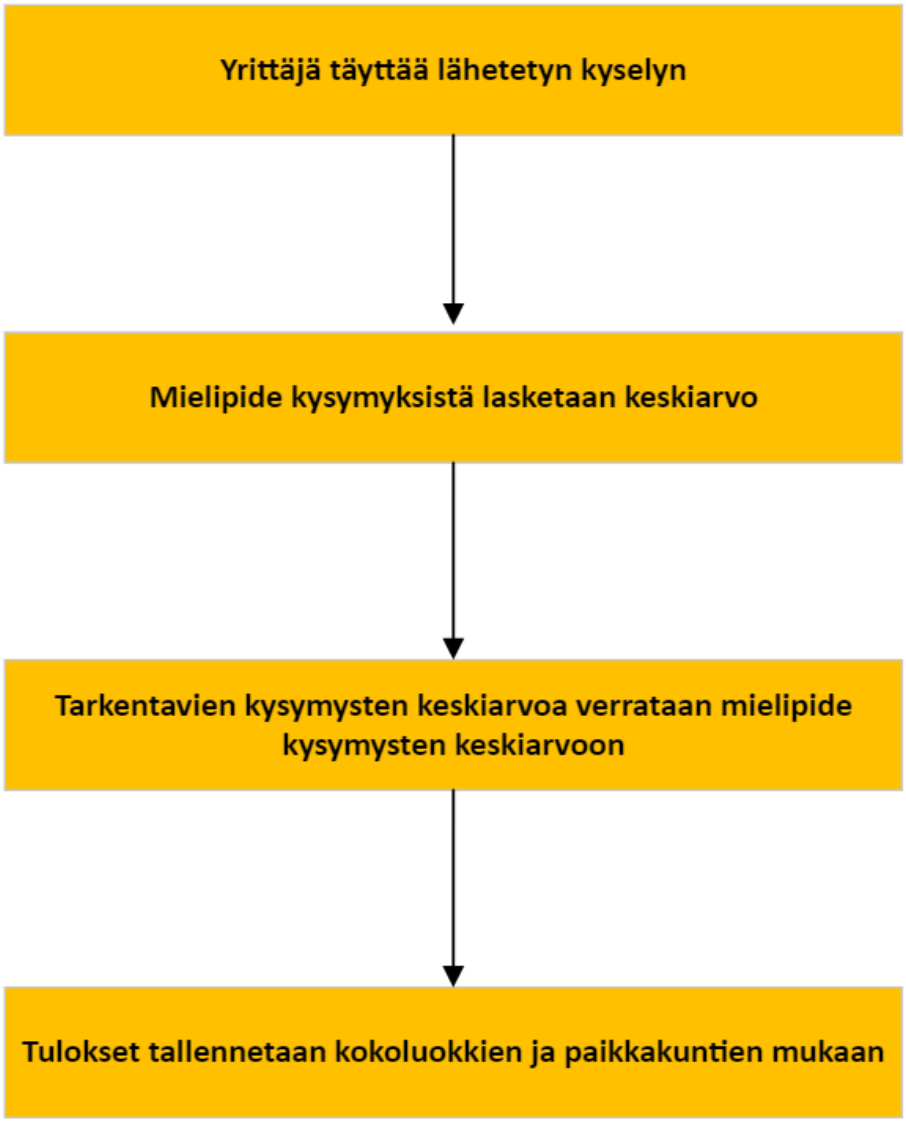
Taulukko 1. Yritysotanta TOL-luokkien mukaan

Riviotsikot	Määrä	%-osuus	Uudet kiintiöt
Kauppa	930	**12,98 %**	56
1-4 henkilöä	805	11,24 %	22
5-9 henkilöä	64	0,89 %	20
10-19 henkilöä	37	0,52 %	8
20-49 henkilöä	20	0,28 %	4
50-99 henkilöä	2	0,03 %	1
100-249 henkilöä	2	0,03 %	1
Kuljetus ja varastointi	**587**	**8,19 %**	35
1-4 henkilöä	466	6,51 %	10
5-9 henkilöä	60	0,84 %	10
10-19 henkilöä	37	0,52 %	7
20-49 henkilöä	21	0,29 %	6
50-99 henkilöä	2	0,03 %	1
100-249 henkilöä	1	0,01 %	1
MUU	4108	**57,35 %**	247
1-4 henkilöä	3841	53,62 %	161
5-9 henkilöä	143	2,00 %	45
10-19 henkilöä	66	0,92 %	25
20-49 henkilöä	32	0,45 %	8
50-99 henkilöä	19	0,27 %	6
100-249 henkilöä	7	0,10 %	2
Rakentaminen	1116	**15,58 %**	67
1-4 henkilöä	984	13,74 %	37
5-9 henkilöä	74	1,03 %	15
10-19 henkilöä	37	0,52 %	8
20-49 henkilöä	17	0,24 %	6
50-99 henkilöä	4	0,06 %	1
Teollisuus	422	**5,89 %**	25
1-4 henkilöä	339	4,73 %	9
5-9 henkilöä	29	0,40 %	6
10-19 henkilöä	24	0,34 %	4
20-49 henkilöä	19	0,27 %	3
50-99 henkilöä	7	0,10 %	2
100-249 henkilöä	4	0,06 %	1
Kaikki yhteensä	**7163**	**1**	**430**

Kyselyssä olevat kysymykset on luotu siten, että ne täyttäisivät seuraavat parametrit:

1. Vastaaja pystyy vastaamaan kysymyksiin siten, että hän ymmärtää kysymyksen ilman aikaisempaa tietoteknistä osaamista
2. Kysymysten vastauksessa on mahdollisuus vastata ”En tiedä”
3. Kysymysrakenne on rakennettu siten, että vastaaminen olisi mahdollisimman vähän vaivaa vaativaa ja helppoa

Alla on vielä kuvattu, kuinka kyselyaineiston analyysi hoidetaan käytännössä ja kuinka tutkimusongelmaan pyritään saamaan vastaus.



Kuva 2. Jatkuva aineiston analyysi opinnäytetyön ajalta

Koska kyselyn kysymykset ovat pääsääntöisesti tarkoitettu yritysten päättäjille, ei voida olla varmoja henkilöiden tietoteknisestä osaamisesta tai taidoista. Tämän takia kyselyn kysymysten luomisessa on pyritty mahdollisimman helposti ymmärrettäviin ja kansantajuisiinkysymys ja vastausvaihtoehtoihin.

Sekundääriaineisto

Sekundääriaineisto on aineistoa, joka on jo olemassa olevaa. Tätä aineistoa voidaan hyödyntää sellaisenaan (Kananen 2017, 82). Kysymys suomalaisten yritysten yleisimmistä kyberturvauhista on muodoltaan laadullinen. On kuitenkin tärkeä määrittää yrityksille yleisimmät kyberturvauhat. Uhkien pohjalta voidaan luoda relevantit kysymykset jaettavaan kyselyyn. Ilman sekundääriaineistoa ei tässä työssä voida myöskään luoda primääriaineistolle tyypillistä kyselyä, joka valmistamiseen vaaditaan reilusti tietoa yrityksiä uhkaavista kyber- ja tietoturva uhista. Kun tiedetään, mikä tällä hetkellä yrityksiä piinaa, täytyy se ottaa huomioon kyselyä luodessa. Nämä kyber- ja tietoturvauhat käydään läpi tarkemmin neljännessä luvussa, joka pohjustaa kyselyn luomista ja kyselyyn tarvittavan analysointityökalun tekemistä. Koska kysely on luotu yrittäjien kyber- ja tietoturvan tietotaidon kartoittamiseksi, tulee kyselyn tulokset analysoida siten, että siitä saadaan mahdollisimman suoraviivainen tulos, joka osoittaa mahdollisen osaamisen. Näiden tulosten määrittelyä käydään seuraavassa luvussa.

Jotta tasotaulukko voidaan luoda, täytyy kyselyn olla valmis. Tasotaulukko rakentuu nimenomaisesti kyselylomakkeen päälle ja mahdollistaa keinon vastata tutkimusongelmaan määrällisesti. Tasotaulukkoon luotu pisteytys saadaan luvussa 4 selitettyjen kyberuhkien ja niiden ehkäisemiskeinojen avulla. Tämän takia opinnäytetyössä sekundäärinen aineisto on erityisen tärkeää. Ilman kattavaa selvitystä siitä, mitä hyvät kyber- ja tietoturvakäytännöt ovat, voi yritysten pisteytys tasotaulukon avulla vääristyä.

2.4 Aineiston analyysi

Määrällisen tutkimusotteen seurauksena aineiston analysointi tulee tapahtua määrällisen analysoinnin perusteella. Määrällisessä analysoinnissa pyritään selvittämään erilaisten ilmiöiden syy- ja seuraussuhteita, ilmiöiden välisiä yhteyksiä tai ilmiöiden yleisyyttä ja esiintymistä (Koppa 2021). Määrälliseen eli kvantitatiiviseen analyysiin sisältyy myös hyvin vahvasti myös asioiden määrän selville saanti, eli käytännössä asioiden ilmaiseminen numeraalisten keinojen avulla. Kuitenkin yrittäjien kyberturvallisuuden kartoituskyselystä saatuja vastauksia ei yksinkertaisesti voi mitata määrällisesti ilman numeraalisia lukuja. Kysely pitää sisällään numerollisia vastausvaihtoehtoja kuten mielipidemittauksen numeroista yhdestä viiteen, joissa yksi heikoin ja viisi vahvin. Mutta suurin osa kyselyn vastauksista ei sisällä numeraalisia arvoja, mikä tarkoittaa, että kysymykset täytyy muuttaa laadullisesta analyysista määrälliseen. Laadullisessa analysoinnissa pyritään ymmärtämään kohteen laatua ja siihen liittyviä ominaisuuksia sekä merkityksiä. Jos kyselyn vastauksia vertailtaisiin tasotaulukkoon laadullisen analyysin menetelmin, luo vastausten määrä ja yritysten erilaisuus riskin analyysin hankaloitumiselle. Numeroiden avulla voidaan suoraviivaistaa analyysiä ja välttää mahdolliset luotettavuutta vähentävät ongelmat.

Empiirinen muoto

Kyselystä saadut tulokset täytyy pystyä laskemaan empiirisesti, jotta tasotaulukko toimii määrällisen analyysin mukaisesti. Tämänkaltaista teoreettisten käsitteiden muuttamista empiiriseen muotoon kutsutaan operationalisoinniksi ja yksinkertaisuudessaan sillä pyritään selvittämään, kuinka käsitteitä voidaan mitata (Saaranen-Kauppinen & Puusniekka 2006.) Operationalisoinnissa ei ole tarkoitus kuvailla tai spesifioida termien merkityksiä, vaan operationalisoinnilla pyritään ainoastaan osoittamaan mittaamista eikä semanttista merkitystä (Saaranen-Kauppinen & Puusniekka 2006). Opinnäytetyön kannalta tämä ei haittaa, koska koko työssä luodut selitykset yritysten yleisimmistä uhista ja parhaista kyberhygieniatavoista, selittävät kyselyssä olevat termit ja niiden semanttiset merkitykset.

Tasotaulukossa olevat pisteytykset tarkentaville kysymyksille on pohjustettu näistä selityksistä, jotka ovat jo käsitelleet teoreettiset termit niiden sekundääriaineiston avulla. Kysymykset pitävät sisällään yhden parhaan kyberkäytäntöä osoittavan vastausvaihtoehdon, keskivertoa kyberkäytäntöä osoittava vastausvaihtoehdon ja huonoa kyberkäytäntöä osoittavan vastausvaihtoehdon. Kyselyssä on myös kysymyksiä, joista saa vain osan pisteistä riippuen yrityskoosta. Pienemmät yritykset saavat hieman paremmat pisteet osasta kysymyksistä kuin isommat yritykset. Syy tälle on yritysten oma investointikyky panostaa kyberturvaan. Isommilla yrityksillä on paremmat mahdollisuudet parantaa ja vahvistaa omaa kyberturvallisuuttaan kuin pienemmillä yrityksillä. Tämän takia isommat yritykset ovat tarkemman tarkastelun alla. Tätä pisteytysmenetelmää verrataan lopuksi tasotaulukkoon, joka antaa yrityksen kyberturva-arvosanan. Tämänkaltaista muuttujaa kutsutaan tilastomuuttujaksi, eli mittaustulokset muutetaan muotoon, jotta niitä voidaan käsitellä tilastollisin menetelmin (Kananen 2011, 60). Pisteytykset yrityskoon mukaan:

1. Parhainta kyberkäytäntöä osoittava vastaus
    a. Suuremmat yrityskoot = täydet pisteet
    b. Pienemmät yrityskoot = täydet pisteet
2. Keskivertoa kyberkäytäntöä osoittava vastaus
    a. Suuremmat yrityskoot = 40 % pisteistä
    b. Pienemmät yrityskoot = 60 % pisteistä
3. Huonointa kyberkäytäntöä osoittava vastaus
    a. Suuremmat yrityskoot = ei pisteitä
    b. Pienemmät yrityskoot = ei pisteitä

Kysymykset siitä, kuinka määrittää yritysten oikea kyber- ja tietoturvatilanne ja mikä on Kymenlaakson yritysten kyber- ja tietoturvan oikea tilanne, ovat osittain määrällisen tutkimusotteen mukaisia. Yritysten kyberturvatilanteen määrittäminen viittaa niihin aineiston keräyskeinoihin, joilla tarvittava tieto saadaan selville. Tähän kuuluu aikaisemmin mainittu primääriaineiston kysely ja sekundääriaineiston kautta saatu tasotaulukko, joka noudattaa jatkuvaa muuttujaa. Eli yritys voi saada minkä tahansa arvon kahden arvon välillä. Tasotaulukossa nämä arvot voivat olla 1 ja 5 välillä. Kyselyn jokainen kysymys on pisteytetty, ja hyvää kyberhygieniaa vastaavat vastaukset saavat aina viisi pistettä.

Tasotaulukon pisteytys ja keskiarvo

Opinnäytetyössä luotu tasotaulukko loi yrittäjille kaksi keskiarvoa, jotka perustuivat heidän antamiinsa mielipiteisiin ja konkreettisiin toimiin yrityksissä. Näitä kahta keskiarvoa verrataan toisiinsa ja niistä pyritään saamaan selville erot mielipiteen ja yrityksen konkreettisten toimien välillä. Tätä ”vääristymää” kuvaillaan työssä sanalla ”eroavaisuus”. Termillä eroavaisuus pyritään tuomaan esille yrittäjien tietämystason eroa mielipiteiden ja konkreettisten toimien välillä. Syyt sille miksi kyselyn kaksi eri osaa saavat omat keskiarvot, johtuvat näiden kahden arvon vertailukelpoisuudesta. Jos keskiarvojen välillä on esimerkiksi 0,5 pisteen heitto, voidaan arvella yrityksen oma käsitys kyber- ja tietoturvasta olevan melko oikea. Kuitenkin jos eroavaisuus on 1,0 pisteestä ylöspäin, on mahdollista, että yritys ei välttämättä tiedä mitä kaikkea kyber- ja tietoturvaan liittyy. Alle on listattu lista eroavaisuuksista mielipidekysymysten ja tarkentavienkysymysten välillä.

- 0,0 → 0,5 = Ei mahdollista eroavaisuutta
- 0,5 → 1,0 = Mahdollinen eroavaisuus
- 1,0 → 2,0 = Eroavaisuus
- 2,0 → 5,0 = Suuri eroavaisuus

Nämä kyseiset eroavaisuudet analysoidaan kaikkien haastattelujen osalta ja sijoitetaan paikkakunnittain, jotta saadaan selville, kuinka eroavaisuudet ovat jakautuneet koko Kymenlaakson alueella. Tämän avulla pystytään vastaamaan toiseen ja kolmanteen tutkimuskysymykseen.

2.5 Luotettavuuden arviointi

Kun halutaan selvittää ilmiöitä tai tutkitaan tutkimukselle ominaisia asioita, on tärkeää varmistua tutkimuksen luotettavuudesta. Kvantitatiivisessa tutkimuksessa tämä on erityisen tärkeää, koska täten voidaan varmistua, että tutkimuksen tutkimusmenetelmät, mittarit ja otos ovat määritetty oikein. Samalla varmistetaan, että tutkimuksen validiteetti ja reliabiliteetti on huomioitu toteutuksen yhteydessä. (Kananen 2011, 118–119.)

Opinnäytetyön validiteetti (pätevyys) ja reliabiliteetti (pysyvyys) voidaan opinnäytetyössä määrittää avaamalla kummankin käsitteen roolia tutkimuksessa. Validiteetti määrittää tutkimuksessa keinot ja tavat, joilla voidaan varmistua, että tarvittavat mittarit mittaavat sitä mitä halutaan mitata. Opinnäytetyössä

mittarina toimii tasotaulukko, jolla voidaan selvittää Kymenlaaksossa sijaitsevien yritysten taso paikkakunnittain. Tämänkaltainen vertailu täyttää ulkoisen validiteetin määritelmän, jossa pyritään yleistämään saadut tulokset siten, että voidaan nähdä otoksen vastaavan populaatiota. Kun otos on kaikki Kymenlaaksolaiset yritykset, voidaan siitä johdattaa tulokset yleistämään myös muita alueita. Kuitenkin tämänkaltaisen tutkimuksen validiteettia heikentää mahdollinen alhainen vastausprosentti. Alhaisen vastausprosentin takia ei yleistettävyyttä välttämättä voida tehdä (Kananen 2011, 121–122.) Validiteettia voidaan myös arvioida sisäisen ja ulkoisen validiteetin muodostamaa kokonaisvaliditeettia. Ongelmana on kuitenkin määrällisessä tutkimuksessa sisäisen validiteetin arvioinnin mahdottomuus. Tätä voidaan tosin pienentää hyvällä dokumentaatioilla ja määrittelemällä sekä johdattelemalla käsitteet tarkasti. Tätä käydään läpi tarkemmin teoreettisessa osuudessa (Kananen 2011, 124)

Hyvällä validiteetilla voidaan myös olettaa reliabiliteetin olevan hyvä. Hyvän reliabiliteetin takaa tutkimuksen onnistunut toistettavuus. Määrällisessä tutkimuksessa tämä onnistuu tehokkaasti, kun seuraavat parametrit ovat kunnossa:

1. Tutkimuksen mittari on määritetty oikein
2. Tutkimuksen toteutus on dokumentoitu tarkasti siten, että se voidaan helposti toteuttaa uudestaan toisen tutkijan toimesta
3. Ratkaisujen täytyy olla perusteltuja, jotta voidaan varmistua prosessin aukottomuudesta alusta loppuun

Tutkimusongelmaan vastauksen saamisen puolesta olisi tärkeää varmistaa aineistosta saatujen tuloksien luotettavuus. Tämän takia mittaaminen tulisi kohdistaa yksikköön. Opinnäytetyössä on tarkoitus tutkia yrityksiä, jonka takia yksikkönä käytetään tilastoyksikköä. Tilastoyksikkö tulee määrittää tarkasti, jotta se tukee tutkimuskysymyksiin vastaamista oikealla tavalla ja kyselystä saatavien tulosten luotettavuutta. Opinnäytetyössä yrityksellä tarkoitetaan liiketoimintaa Kymenlaakson seudulla, jonka työntekijöiden määrää ja liikevaihtoa ei ole rajattu. Tutkimuskysymyksiin vastaaminen vaatii tarvittavien muuttujien määrittämisen. Varsinkin muuttujien rakenne on tärkeä tietää, jotta voidaan määrittää minkä kaltaisia arvoja ne voivat saada. (Kananen 2011, 58–62; Holopainen & Pulkkinen 2008, 15–16)

3 TEOREETTINEN VIITEKEHYS

Hyvä teoreettinen viitekehys luo suunnan tutkimukselle osoittamalla aiheeseen liittyvät termit, avainsanat ja hypoteesit. Käymällä nämä läpi voidaan todistaa, että tutkimus ei ole niin sanotusti ”tyhjästä ilmestynyt” vaan tutkimukselle on tarkoitus (Scribbr 2016). Kun opinnäytetyön tutkimusongelma on ”*tietävätkö Kymenlaakson yrittäjät oikeasti mitä kaikkea heidän yrityksensä kyberturvaan liittyy?*” tulee määrittää tutkimuksen termit ja avainsanat. Tärkeimmät termit ovat kyberturva ja kyberrikollisuus.

Kyberturvallisuudesta puhutaan nykyaikana paljon ja hyvästä syystä. Kyberturvauhat jatkavat lisääntymistään ja yritykset sekä yksityishenkilöt, joutuvat huijausten ja haittaohjelmien uhreiksi yhä etenevissä määrin. Hoitokeinona tähän ongelmaan pyritään tuomaan esille kyberturvan tärkeyttä henkilön ja yrityksen turvallisuuteen, mutta mitä kyberturvallisuus tarkoittaa. Kyberturvaa ei voi tehdä tai harjoittaa, jos ei tiedetä mitä siihen konkreettisesti kuuluu. Traficomin (2020b, 4) Kyberturvallisuus ja yrityksen hallituksen vastuu oppaassa kyberturvallisuus määritetään käytännössä viittaamaan organisaatioiden ja yhteiskunnan digitalisaation seurauksena ilmestyneisiin uusiin turvallisuushaasteisiin. Kyberturva on toimenpiteitä, joilla organisaatio, yritykset ja yhteiskunnalliset toimijat suojaavat tarvittavia järjestelmiä, ohjelmistoja, laitteita ja tietoliikenneyhteyksiä kyseisiltä turvallisuushaasteilta. America’s Cyber Defense Agency (2021) taas määrittelee kyberturvallisuuden ”taiteen tai taidon” lajiksi, jossa pyritään suojaamaan verkkoyhteydet, laitteet ja data luvattomalta pääsyltä. Pääperiaate on pitää CIA-kolmio (confidentiality, integrity ja availability) toiminnallisena ja kestävänä. Yhtenäistä kuitenkin näissä kahdessa määrittelyssä on niiden periaate pitää tietoverkot ja laitteet suojattuna, jotta jatkuva normaalielämä ja yritystoiminta voisi jatkua ilman ongelmia. Kyberturva pitää siis sisällään kaiken aina laiteteknisestä turvallisuudesta ihmisten aiheeseen kouluttamiseen.

Kun tutkitaan viranomaisten määritelmiä konerikollisuudelle ja järjestäytyneelle rikollisuudelle, voidaan huomata määritelmien vaikeaselkoisuus. Aku Limnell (2023) blogikirjoituksessaan kirjoittaa seuraavasti ” Kyberrikollisuudella tai kyberrikoksilla ei ole yhtä yleisesti hyväksyttyä määritelmää”. Kuitenkin Sisäministeriö (s.a) määrittelee julkaisussaan kyberrikollisuus ylittää rajat

tietoverkoissa kyberrikollisuuden seuraavasti: ” Kyberrikollisuus eli tietotekniikkarikollisuus tarkoittaa tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtäviä rikoksia”. Aku Limnell (2023) myös omassa kirjoitelmassaan kertoo kyberrikollisuus määritelmän olevan tietoverkkorikollisuutta, joka voidaan jakaa kahteen muotoon:

1. Tietotekniikkaa ja tietoverkkoihin kohdistuvaa rikollisuutta tai hyökkäyksiä (cyber-dependent crime)
2. Tietotekniikka ja tietoverkkoja hyväksikäyttävät rikollisuuden elementit ja hyökkäykset (cyber-enabled crime)

Yhteistä myös Sisäministeriön (s.a) ja Aku Limnellin (2023) määritelmissä on kyberrikollisuuden kansainvälisyys ja sen laaja leviäminen. Näiden perusteiden mukaan kyberrikollisuus voidaan määritellä kansainväliseksi rikolliseksi toiminnaksi verkossa, joka hyödyntää tietotekniikkaa tai tietoverkkoja vahingoittaen ihmisiä, yrityksiä, organisaatioita tai yhteisöjä

Vuonna 2022 Kymenlaaksossa oli 9 800 yritystä ja yritysten toimipaikkoja oli noin 11 500 (Kymenlaakso Ennakoi 2022). Tällä hetkellä ei ole tehty kartoitusta siitä, minkä tasoinen kyberturva näissä yrityksissä on. Jonkin asteinen kartoitus on hyvä luoda, kun otetaan huomioon, että Suomessa yrityksiin kohdistuvat tietomurrot ovat yli kolme kertaa yleisempiä Euroopan keskilukuun verrattuna (Mattila ym. 2020, 6). Tähän kyberturvan kartoittamiseen ei kuulu pelkästään hyvät kyberhygieniatavat, mutta myös tietoturvasuunnitelmat ja liiketoiminnan jatkuvuussuunnitelma. Kyberturva ABC-hanke on Euroopan Sosiaalirahaston (ESR) rahoittama hanke, jonka pääsääntöisenä tavoitteena on ” Opastaa maksutta ja käytännönläheisesti Kymenlaakson nykyisiä ja tulevia yrittäjiä nostamaan kyber- ja tietoturvallisuuttaan.” (Kaakkois-Suomen ammattikorkeakoulu 2022). Hankkeen toteutuksen aikana on käynyt kuitenkin ilmi yrittäjien pelko ilmaista oman yrityksensä kyberturvatasoa. Tämä käy erityisen selväksi sosiaali- ja terveydenhuollon yritysten kanssa, jotka pelkäävät kokevansa saman kohtalon kuin psykoterapiakeskus Vastaamo. Jos otetaan huomioon Mattilan ym. (2020, 5) huomiot vuoden 2020 digibarometrin tuloksissa, pienien ja keskisuurten yritysten tilanne Suomessa on huomattavan huono kyberturvallisuuden uhkien osalta. Kun otetaan huomioon tämänhetkinen kiristynyt maailmantilanne, ovat riskit kyberhyökkäyksistä yrityksiä kohtaan kasvaneet.

Yritysneuvojat

Suomessa ja Kymenlaaksossa toimivia yrittäjiä on jo pitkään auttaneet yritysneuvontayhtiöt ja -organisaatiot. Näiden laitoksien osaaminen ei ainakaan tutkintahetkellä pystynyt palvelemaan yrityksiä kyberturvallisuudessa. Avoimien tietolähteiden tutkintaprosessilla selvitettiin, että yksikään seuraavista yritysneuvontayhtiöstä tai -organisaatiosta ei tarjonnut minkäänlaista kyberturvaan liittyviä palveluita tai tietolähteitä:

- Kymen Yrittäjät
- Kymenlaakson naisyrittäjät
- Kotkan yrittäjät
- Haminan yrittäjät
- Pyhtään yrittäjät
- Virolahti-Miehikkälän yrittäjät
- Kouvolan yrittäjät
- Valkealan yrittäjät
- Kuusankosken yrittäjät
- Jaalan yrittäjät

Pienille ja varsinkin mikroyrityksille tämänkaltainen apu on todella arvokasta, jos huomioidaan yritysten tarve luoda esimerkiksi yrityksen tietosuojalauseke tai jatkuvuussuunnitelma. Näiden tekeminen siten, että niissä huomioidaan kyber- ja tietoturva oikealla lailla, voi olla yrittäjälle todella vaikeaa ilman oikeanlaista opastusta. Yrittäjäneuvonta olisi hyvä auttaja tämänkaltaisessa toiminnassa, mutta ikävä kyllä varsinkin Kymenlaaksosta puuttuu tämänkaltainen osaaminen. Opinnäytetyötä on myös tarkoitus jakaa yritysneuvojille, jotta voidaan aloittaa kyberturvan tietoisuuden lisääminen tarvittavissa yhtiössä ja organisaatioissa.

Vakuutusyhtiöt

Suomessa toimivat pääsääntöiset vakuutusyhtiöt tarjoavat myös yrityksille kyberturvavakuutuksia, joiden ehdot ja vakuutusmaksut vaihtelevat vakuutusyhtiöiden mukaan. Kuitenkin vakuutusyhtiöiden ehdot vakuutusmaksujen maksamisille ovat kaikilla varsin samankaltaiset ja väärin ymmärrettynä myös haitallisia. Kyberturvavakuutukset voivat pelastaa pienemmät ja mahdolliset suuretkin yritykset kyberhyökkäysten tuomalta taloudelliselta vahingolta. Kuitenkin,

jotta kyberhyökkäyksistä saatavat vakuutusmaksut voidaan maksaa, täytyy yritysten ylläpitää ja seurata varsin tiukkoja sisäiseen kyberturvaan liittyviä ehtoja. Vakuutusyhtiöt, jotka tarjoavat kyberturvavakuutuksia ovat:

- If
- OP
- LähiTapiola
- Fennia

Suurille yrityksille ehtojen noudattaminen ei välttämättä aiheuta suuria haasteita, mutta mikro- ja pk-yrityksille tämä voi olla melko vaikeaa. Myös joissakin tapauksissa yrittäjä ei välttämättä tiedä mitä vaatimuksiin sisältyy, voi vakuutus tuoda valheellisen turvallisuuden tunteen ja aiheuttaa kyberturvallisuuden laiminlyönnin.

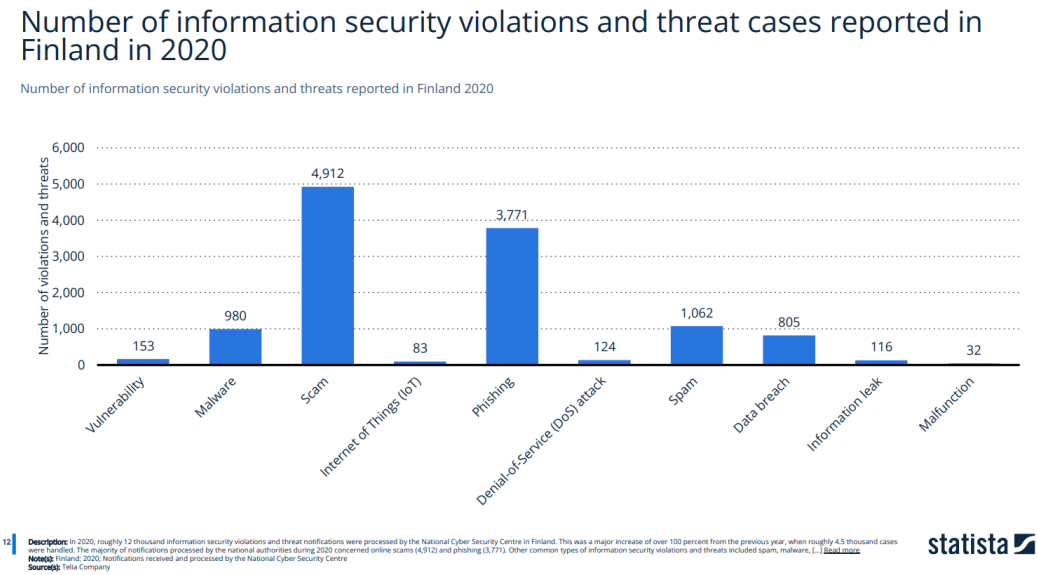
4 YLEISET KYBERUHAT YRITYKSIÄ KOHTAAN

Kuten aiemmin tutkimusotteen käsittelyssä mainittiin, Suomessa pienet, keskisuuret ja suuret yritykset kärsivät kyberturvavaikeuksista Euroopan muita yrityksiä todennäköisemmin. Vaikka tieto on saatu Digibarometrin 2020 -tutkimuksesta, ovat hyökkäykset ja kyberturvatapahtumat lisääntyneet Traficomin (2022a) raportin mukaan huomattavasti. Nämä hyökkäykset ja kyberturvatapahtumat koostuvat pääsääntöisesti haittaohjelmista yritysverkoissa ja laitteissa, palvelunestohyökkäyksistä ja huijauksista sekä kalasteluviesteistä. Näistä kaikista huijaukset ja kalasteluviestit olivat ylivoimaisesti yleisempiä kyberhaittoja, joita yrittäjät kohtasivat. Tässä luvussa tullaan käymään läpi ne uhat, jotka kaikista todennäköisemmin voivat aiheuttaa kyber- ja tietoturvauhkia kaikenkokoisille yrityksille.

4.1 Tietojenkalastelu ja huijaukset

Traficomin pääjohtaja Kirsi Karlamaan mukaan tietojenkalastelu ja huijausviestit ovat muuttaneet muotoaan kuluneiden vuosien aikana. Traficomin suorittaman analyysiin mukaan suomalaisiin organisaatioihin on kohdistettu entistä räätälöidympiä hyökkäyksiä, aikaisemman ”määrä voittaa laadun” -taktiikan sijaan (Traficom 2022a). Vaikka organisaatioilla Traficomin artikkelissa tarkoitetaan suurimmaksi osaksi hallinnollisia ja julkispalveluja, olisi naiivia kui-

tenkin ajatella, että nämä taktiikat eivät vaikuttaisi myös jokapäiväisiin suomalaisiin yrityksiin. Tämänkaltaiset kohdennetut tietojenkalastelut ja tiedonkeruukeinot ovat usein ensimmäinen askel yritykseen kohdistuvassa hyökkäyksessä. Yritykset, jotka tämänkaltaiseen hyökkäykseen ovat kaikista alttiimpia, ovat alihankintaketjun alkupäässä olevat mikro- ja pienyritykset, joiden kautta hyökkääjän on helpompi edetä suuremman yrityksen tai organisaation verkkoon. Alla on kuva, joka osoittaa huijausten olevan yleisin kyberturvauhka Suomessa.



Kuva 3. Tapausmäärät tapaustyypeittäin vuonna 2020 (Traficom 2021, 17)

Tietojenkalastelu (phishing) on toimintaa, jossa uhri koitetaan manipuloida luovuttamaan senkaltaisia tietoja, joiden luovuttaminen on hänen tai ympäristönsä kannalta haitallista. Usein tietojenkalastelusta puhutaan mediassa erilaisten sähköpostihuijausten muodossa ja lähes riesaksi muodostuneiden huijauspuheluiden muodossa. Tietojenkalastelu pitää sisällään useita eri muotoja:

1. Kohdennettu tietojenkalastelu (Spear phishing)
2. Tekstiviestihuijaukset (Smishing)
3. Huijauspuhelut (Vishing)

Kohdennettu tietojenkalastelu on satunnaisen tietojenkalastelun vastakkainen keino, jossa henkilön manipuloiminen tapahtuu kohdennetusti. Uhriksi valitaan usein yritysten tai organisaatioiden työntekijöitä tai niiden johtohenkilöitä. Näitä henkilöitä manipuloidaan siten, että he antavat keinolla tai toisella pääsyn yrityksen tai organisaation sisälle. Työntekijä voi esimerkiksi antaa oman

työsähköpostin käyttäjätunnuksen ja salasanan kyberrikolliselle, joka on naamioitunut sisäiseksi IT-osaston työntekijäksi (Traficom 2020a).

Tekstiviestihuijaukset ovat käyneet varmasti monelle kansalaiselle tutuksi niiden suuren määrän vuoksi. Yleisimmät Suomessa nähtävät tekstiviestihuijaukset ovat usein pankin, paketti- sekä postipalveluiden tai valtiollisten laitosten nimissä lähetyt tekstiviestit. Näiden tekstiviestin sisältö hoputtaa viestinsaajaa ratkaisemaan tekstiviestissä olevan pulman usein antamalla linkin haitalliselle mutta virallisen näköiselle palvelusivulle. Omien tietojensa syöttäminen näille kyseisille palvelusivuille ovat yksi yleisimmistä käyttäjätunnusten varkaus keinoista. Pelkästään vuonna 2022 keskusrikospoliisi ilmoitti suomalaisten menettäneen yhteensä 10 miljoonaa euroa valeviranomais- ja tekstiviestihuijauksissa (Poliisi 2023.) Sähköpostin kautta tulevat huijausviestit ovat tekstiviestihuijauksia yleisempiä ja huomattavasti vanhempi keino saada ihmiset toimimaan itselleen epäsuotuisasti. Vaikkakin sähköpostin kautta tulevat massasähköpostit (spam-viestit) ja kohdennetut huijaussähköpostit käyttävät eri alustaa kuin tekstiviestipohjaisissa huijauksissa, ei niiden olemus ole ollenkaan erilainen. Samat sosiaalisen manipuloinnin keinot ovat läsnä myös tässä huijauskeinossa.

Huijauspuhelut ovat jo pitkän aikaa olleet myös tuttuja valtaväestölle. Huijauspuhelujen motiivi on sama kuin tekstiviestihuijauksissa, mutta tekotapa muuttuu tekstipohjaisesta puhepohjaiseen. Suomessa tällaiset puhelimitse tapahtuvat huijausyritykset torjutaan usein suomalaisten skeptisyyden vuoksi, joka kohdistuu vieraisiin kieliin ja voimakkaaseen aksenttiin, tästä huolimatta suomalaiset menettivät Traficomin (2023) mukaan vuosina 2020 ja 2021 miljoonia euroja huijauspuheluja tehtaileville rikollisille. Traficomin aloittama uusi määräys teleoperaattoreille pakottaa operaattorit varmistamaan numeroiden oikeellisuus, vaikka numerot tulisivat Suomen ulkopuolelta. Tämän määräyksen takia rikolliset eivät pysty väärentämään ulkomaalaisia numeroita näyttämään suomalaisilta (Traficom 2023). Tämä uudistus ei kuitenkaan suojele yrityksiä kohdennetulta tietojenkalastelusta. Myös uudet innovaatiot koneoppimisessa ovat tuoneet esille ihmispuheen väärentämisen tekoälymallien avulla, joka voi olla todella hankala erottaa oikeasta ihmisestä.

4.2 Haittaohjelmat

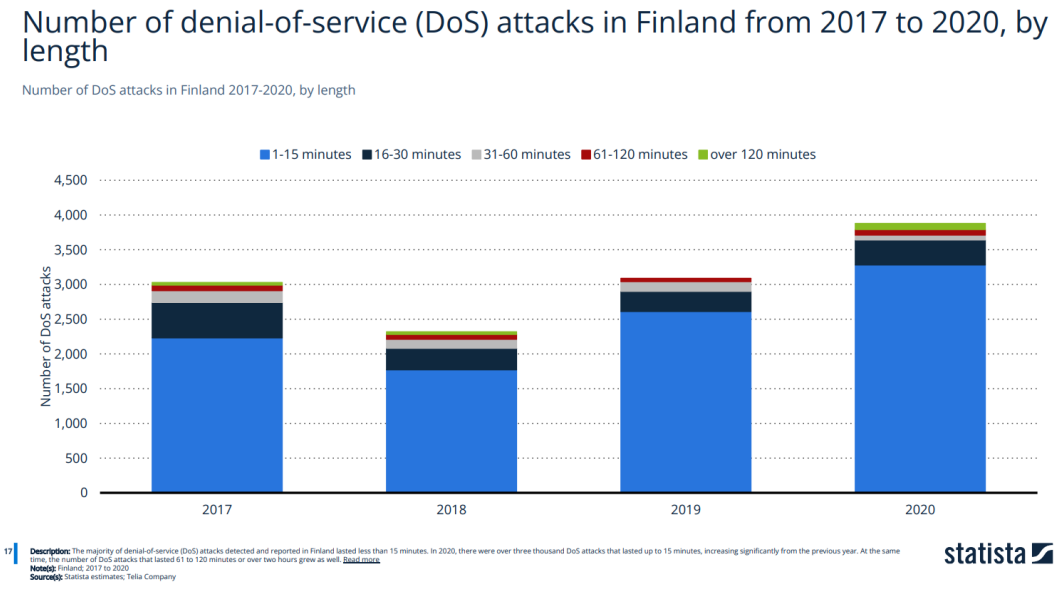
Haittaohjelmat voivat olla yrityksen tuhoavia uhkia, jotka päätyvät laitteisiin usein sosiaalisen manipuloinnin ja aikaisemmin mainittujen huijaustekstiviestien ja sähköpostien kautta. Haittaohjelmia on jalostettu eri kohteita varten, esimerkiksi yksityishenkilöt voivat kärsiä pankkitroijalaisista tai etähallintatroijalaisista, kun taas yrityksiin voi kohdistua yhä enemmän kiristyshaittaohjelmahyökkäyksiä. Kuitenkin yksityishenkilöiden kyberturva tulisi ottaa myös huomioon yritysten lisääntyneen etätyön takia. Työntekijän laitteiden saastuminen voi tämän takia lisätä haittaohjelmien pääsyä yritysverkkoihin. Tässä luvussa tullaan keskittymään pääsääntöisesti yksityishenkilöiden/työntekijöiden laitteita saastuttaviin haittaohjelmiin, joihin kuuluu RAT (Remote Access Troijan) sekä muut vakoiluhaittaohjelmat, joiden tehtävänä on kerätä informaatiota uhrista rahallisen hyödyn toivossa (CIS & CTI 2023). Yrityksiä kohtaan tehdyt haittaohjelmakyberhyökkäykset ovat usein koostuneet kiristyshaittaohjelmista ja remote access -troijalaisista. RAT ja kiristyshaittaohjelmat ovat erityisen vaarallisia myös seuraavista syistä:

1. Yritysten tärkeiden asiakirjojen menettäminen ja tuhoutuminen
2. Henkilötietojen mahdollinen vuotaminen/tuhoutuminen
3. Yritystoiminnan estyminen
4. Haittaohjelmien kehittyminen Ransomware as a Service (RaaS) ja Malware as a Service (MaaS) -palveluiksi, jotka madaltavat rikollisten kynnystä aloittaa kyberhyökkäyksiä
5. Etätöiden yleistyminen yrityksissä ja organisaatioissa lisää saastumisten riskiä

Blackfog (2023) kyberturvallisuusyrityksen mukaan vuoden 2023 toukokuu oli ennätyksiä rikkova kuukausi raportoitujen kiristyshaittaohjelmatapausten saralta. Raportti selvensi, että vuonna 2023 kiristyshaittaohjelmien raportointi nousi 154 % vuoteen 2022 verrattuna. Lukemat vahvistavat kiristyshaittaohjelmien yleistymisen kyberrikollisten keskuudessa, ja tulevaisuutta ajatellen lukemat eivät todennäköisesti lähde laskemaan tulevien kuukausien ja vuosien aikana. Tämä voi luoda varsin suuren riskin kymenlaaksolaisille ja suomalaisille mikro- ja PK-yrityksille, jotka eivät ole välttämättä aivan ajan tasalla kyber- ja tietoturvavarustautumisessaan. Kiristyshaittaohjelmat myös leviävät usein sähköpostien liitetiedostoissa aiheuttaen saastumisen sille laitteelle, jolla liitetiedosto on avattu. Laitteen ollessa yhteydessä yrityksen sisäiseen verkkoon, voi tuho olla yrityksen kaatava. Blackfogin (2023) raportin mukaan 89 % kiristyshaittaohjelmahyökkäyksistä ei pelkästään salaa tietoja, vaan myös kerää niitä ja käyttää vuotamista painostuskeinona hyökättyä yritystä vastaan.

4.3 Palvelunestohyökkäykset

Traficomin (2022b) mukaan Suomessa tapahtuu noin 10 000 palvelunestohyökkäystä vuosittain eri yrityksiä ja organisaatioita vastaan. Palvelunestohyökkäyksellä kyberrikolliset, valtiolliset toimijat ja yksityishenkilöt ohjaavat mahdollisimman paljon liikennettä kohteen verkkosivuja tai palveluja vastaan aiheuttaen katkoksia. Nämä katkokset aiheuttavat rahallista vahinkoa yrityksille ja organisaatioille ja häiritsevät ihmisten kykyä käyttää tarvittavia palveluita. Palvelunestohyökkäyksen tapahtuminen kymenlaaksolaiselle yritykselle on riski, johon varsinkin pienempien yritysten on vaikea varautua. Palveluestohyökkäysten tekeminen käy kyberrikollisille entistä helpommaksi, johtuen suurempien rikollisorganisaatioiden palveluista luoda tämänkaltaisia hyökkäyksiä maksua vastaan (Traficom 2022c, 2). Alle on kuvattu palvelunestohyökkäysten määrät ja pituudet. Jo pieni palvelunestohyökkäys voi aiheuttaa yrityksessä tuntuvia taloudellisia vahinkoja, jos sen ajoittaa yritystoiminnalle kriittiseen aikaan.



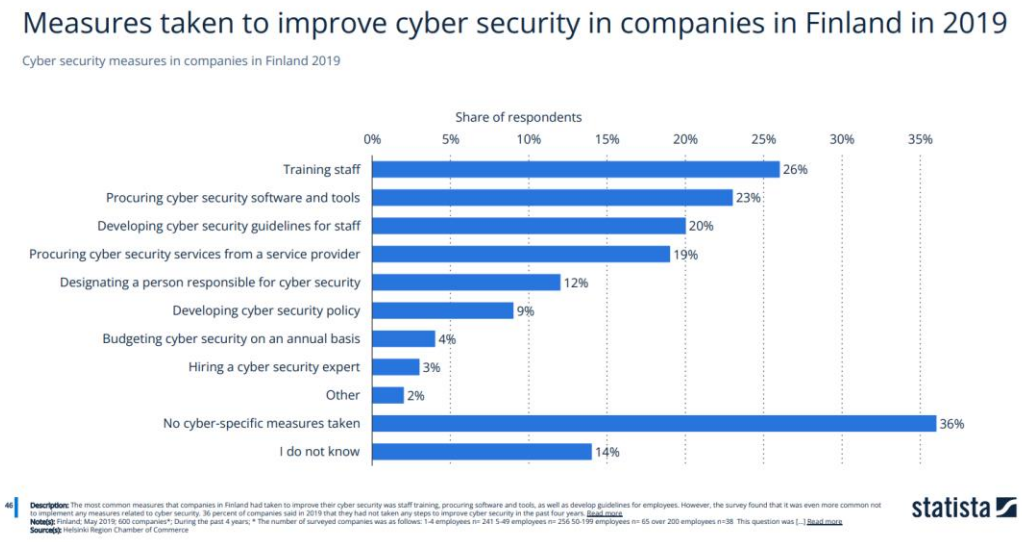
Kuva 4. Palvelunestohyökkäysten määrä Suomessa pituuden mukaan (Statista 2021)

Palvelunestohyökkäyksiin varautuminen vaatii yrityksiltä tehokasta suunnitelmallisuutta, joka tulisi toteuttaa hyvissä ajoin. Traficomin palvelunestohyökkäyksen toimintaohjeen mukaan (2022c, 3–4) tärkeimmät näistä suunnitelmista ovat poikkeamahallintasuunnitelma ja palveluntarjoajan palvelutasosopi-

musta. Hyvänä tapana kaikille yrityksille olisi laatia yrityksen jatkuvuussuunnitelma tai suunnitelma poikkeamatilanteissa, mutta Traficomin yleispätevät ohjeet palvelunestohyökkäyksiä vastaan ei ole pätevä yksin mikro- ja PK-yrittäjille. Palveluntarjoajan palvelutasosopimukseen eivät pienemmät yrittäjät suurella todennäköisyydellä pysty sitoutumaan ja tekniset toimet vaativat jo suuryrityksen tasoisia resursseja. Tämän takia kyselyyn ei voida liittää osaa varautumistoimenpiteistä niiden taloudellisen laajuuden takia. Kuitenkin jatkuvuussuunnitelmaan voidaan liittää toimenpiteet palvelunestohyökkäysten varalta. Vaikkakin pienemillä yrittäjillä ei olisi suoranaisia keinoja estää tai korjata palvelunestohyökkäyksiä sekä niistä aiheutuvia vahinkoja, tulisi varautumistoimet silti kirjoittaa ylös.

5 KÄYTÄNNÖT YRITYKSILLE

Tässä luvussa käydään läpi perustelut sille, mitkä ovat hyvät kyber- ja tietoturvakäytännöt yrityksille. Hyvien käytäntöjen pohjalta voidaan luoda kyselyn kysymykset ja tasotaulukkoon vaadittava pisteytys. Ajallisesti ei ole mahdollista tehdä kaikille yrityskokoluokille yksityiskohtaista kyberturvan käytäntöohjeistusta. Tämän kaltaisen käytäntöohjeistuksen tekeminen vaatisi huomattavasti aikaa ja vaivaa, mikä haittaisi tämän kyseisen tutkimuksen valmistumista ajallaan. Sen takia luodaan yleispätevä hyvien kyberturvakäytäntöjen ohjeistus kaikille yrityksille, joissa otetaan huomioon yritysten suurimmat kyberturvauhat ja käytännöt näiden estämiseksi yrityksen koosta riippumatta. Käytäntöjen tueksi alle on listattu suomalaisissa yrityksissä käyttöön otetut kyber- ja tietoturvatoimet ja niiden prosentuaaliset osuudet yrityksissä.



Kuva 5. Kyberturvaa parantavat keinot yrityksissä (Helsinki Region Chamber of Commerce 2019, 9)

Tasotaulukon luominen ja toteutus on suoraan riippuvainen tämänkaltaisesta hyvien kyberhygienian tapojen kartoituksesta pisteytyksen osalta. Useat eri yrityskoot ja niiden kaikkien hyvien kyber- ja tietoturvakäytäntöjen selvittäminen toisi useita eri haasteita työn tulosten operationalisoinniksi, jonka takia perusarvona pidetään niitä toimia, jotka yksin- ja mikroyritykset voivat toteuttaa.

Ympäristö

Hyvät tietoturvakäytännöt alkavat perusteista. Kyber- ja tietoturvan perusta kaikille yrityksille on tieto siitä, mitä laitteita ja ohjelmistoja yritykseen on hankittu. Laitteille ja ohjelmistoille olisi hyvä laatia inventaario, jotta niiden yksityiskohdat olisivat helposti saatavilla. Tämä varmistaa vastatoimien tehokkaan aloittamisen sekä kartoittamisen heti kun kyberhyökkäys havaitaan. Pääsääntöisesti yrityksen johdon ja mahdollisen IT-tiimin tehtävä on tunnistaa yrityksen sisäiset laitteistot ja ohjelmat sekä ottaa ensiaskel kyberturvauhkien lieventämisessä. Viimeiset vaiheet liittyvät kyberturvauhan jälkeisellä palvelujen palauttamisella ja verkon sekä laitteiden putsauksella. Tarvittavat perusohjelmistojen hankinta yritysten laitteisiin on myös hyvien käytäntöjen mukaista ja tullaan ottamaan huomioon kyselyssä. Ohjelmistoihin kuuluvat haittaohjelmien tunnistusohjelmat ja epäilyttävän toiminnan havaitseminen henkilöstön tileillä.

Kun etätyö on lisääntyessä, ovat yritykset ovat avanneet mahdollisia prosesseja ja palveluita julkiseen verkkoon työntekijöiden etäyhteyksien mahdollistamiseksi. Traficomin kansallisessa kyberturvakatsauksen (2021, 6–7) ohjeistuksessa kehotettiin huomioimaan kaikki ulkoverkkoon näkyvät palvelut ja tarkistamaan yhdistämismahdollisuudet ulkoverkosta yrityksen sisäverkkoon. Kaikki palvelut, joita ei tarvita tulisi ottaa pois käytöstä ja kaikkea yrityksen näkyvää verkkotoimintaa tulisi rajoittaa siten, että yrityksen ulkopuoliset uhkatekijät eivät voi yhdistää yritysverkkoon.

Riskit

Yritysten tulisi myös tunnistaa riskit, joita liittyy verkkolaitteisiin, päätelaitteisiin, tarvittaviin ohjelmistoihin ja ihmisiin. Esimerkkeinä tähän liittyen on yrityksen sisäisten tietokoneiden etäyhteys työntekijöiden omalta laitteelta tai riski sille, että työntekijä painaa haitallista linkkiä työsähköpostiinsa tulleesta kalastelu-viestistä. Tämänkaltaiset riskit tulisi käydä läpi, jotta niihin voidaan varautua oikeaoppisesti. Kyselyssä myös tiedustellaan tämänkaltaisten riskien tiedostamista kysymällä perusluontoisten kyberturvaan liittyvien toimintaperiaatteiden käyttöönotoista. Jokainen yrittäjä tavalla tai toisella osaa havaita riskit, joilla on mahdollisuus vahingoittaa yritystä. Perinteisesti nämä saattavat jakautua fyysisiin asioihin kuten tulipaloihin tai laiterikkoontumisiin. Tällaisissa tilanteissa riskin vastuu siirretään usein vakuutusyhtiöille, jotka maksavat korvauksen.

Riskiarvioinnin voi tehdä vasta silloin kun ympäristö, jossa työskennellään, on hyvin kartoitettu. Kuitenkin monille PK-yrittäjille voi tulla ongelmia tarvittavien verkko- ja älylaitteiden riskien mitgoinissa. Näitä voi olla esimerkiksi haittaohjelmat, jotka saastuttavat yrityksen laitteiston ja tätä kautta yritys joutuu tietomurron kohteeksi. National Institute of Standards and Technology (NIST) on luonut tietoturvakehikon, jonka tarkoituksena on auttaa organisaatioita paremmin hallitsemaan kyber- ja tietoturvaansa. NIST:in määritelmä suojelemiselle on: ”yritysten ja organisaatioiden tulisi kehittää ja laittaa käytäntöön suojatoimet, jotka takaavat asianmukaisen turvan kriittisille palveluille” (NIST 2018, 14). Riskien kartoitus on jatkuva ja ennen kaikkea muuttuva prosessi. Jos yrittäjä arvioi yrityksen riskiksi mahdolliset haittaohjelman aiheuttamat vahingot, voi mitigointi tämänkaltaiseen tilanteeseen olla haastava ilman oikeanlaista

tietotaitoa. Koska kaikkia riskejä ei voida erikseen kysyä kyselyssä, rajataan ne yleisiin luokkiin, joita luvussa 4 on käyty läpi.

Koulutus

National institute of standards and technology (NIST) on luonut organisaatiolle tietoturvakehikon parempaan kyberturvallisuuteen. NIST:in luomassa kehikossa tietoturva jaetaan viiteen luokkaan, jotka ovat:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Näiden avulla organisaatiot voivat parantaa omaa kyberturvallisuuttaan. Kuitenkin Chris Moschovitis (2018, 24–26) ilmaisee vielä kuudennen keinon: Deter (estää). Kyberturvallisuutta on monesti ilmaistu puolustajilla ja hyökkääjillä. Puolustajat puolustavat kriittisiä ja tärkeitä verkkoja sekä laitteita, kun taas hyökkääjät pyrkivät pääsemään käsiksi näihin verkkoihin ja laitteisiin. Puolustettavien tietoverkkojen skaalan ja monimutkaisuuden takia puolustamista luonnehditaan myös paljon vaikeammaksi kuin hyökkäämistä. Hyökkääjät tarvitsevat vain yhden heikon kohdan päästäkseen sisään, kun taas puolustajien täytyy turvata koko tietoverkko. Tämän skaalan takia estäminen nähdään haastavana. Chris Moschovitic (2018, 24–26) ilmaisee kirjassaan koulutuksen olevan yksi parhaimpia kyberuhkia vastaan ennaltaehkäisevä toimenpide organisaatiolle. Timothy M.McKenzie (2017, 1–2) tuo esille estämisen passiivisena toimena. Tämä käytännössä tarkoittaa senkaltaisen ympäristön luomista, jonka hyökkääjä näkee liian vaikeana tai vaivalloisena hyökätä. Jos yrityksellä on työntekijöitä, jotka tarvitsevat työssään tietokoneita tai mobiililaitteita, olisi tärkeää opastaa ja kouluttaa näitä työntekijöitä kyberturvaan ja kuinka esimerkiksi tunnistaa kalasteluviesti. Tämän kaltaisella toiminnalla voidaan pienentää riskiä joutua onnistuneen kalastelukampanjan kohteeksi.

Riskejä pystytään myös pienentämään teknisin keinoin, joista tehokkaimmat ovat kaksivaiheiset tunnistautumiset, vahvat salasanat ja käyttäjänhallinta. Nämä kyseiset keinot ovat myös mikro- ja pienyrityksille melko helppoja tehdä, eivätkä vaadi suurta tietoteknistä osaamista. Tämän takia nämä otetaan huomioon myös kyselyssä. Tämän takia hyväksi käytännöksi ei voida

suoraan laittaa kyberuhkien havaitsemiseen tarvittavien laitteiden hankintaa tai ulkoisten samanlaisten palveluiden hankintaa. Kyselyssä otetaan huomioon vain työntekijöiden oikeanlainen koulutus kyberturvauhkien havaitsemiseksi. Tämä pitää sisällään komentoketjun järjestämisen, jossa kaikki tietävät kenelle ilmoitus kyberturvauhasta tulisi tehdä. Tämän komentoketjun skaala voi kasvaa yrityksen kokoluokan mukaan. Se mitä kaikille yritysluokille kuitenkin yhteistä havaitsemissa on henkilöstön koulutus kyberturvauhista ja raportointi jos sellainen havaitaan. Täten havaitsemista voidaan jo luoda riskit osion henkilökunnan koulutuksessa.

6 KYSELYN JA TASOTAULUKON LUOMINEN SEKÄ NIIDEN ANALYYSI

Opinnäytetyön toteutuksen onnistumiseksi on tärkeää, että aikaisemmin mainittu kysely, käytännöt ja tasotaulukko luodaan mahdollisimman toisiaan tukevasti. Tämä vahvistaa tutkimuksen reliabiliteettia ja validiteettia sekä varmistaa sen, että kaikista osa-alueista saadaan mahdollisimman paljon irti opinnäytetyön kannalta. Alaotsikot on jaettu kronologisesti prosessin etenemisen mukaan. Ensimmäiseksi täytyy luoda vertailupohja, jonka jälkeen voidaan lähteä luomaan kyselyä. Kysely on opinnäytetyön tärkein aineistokeruutapa ja siihen tarvittavat vertailukohteet ovat tärkeässä asemassa. Niiden avulla varmistetaan kyselyn oikeellisuus ja tarkkuus. Lopuksi kyselystä saatu aineisto täytyy analysoida ja siihen käytetään käytäntöjä sekä kyselyä vertailupohjana.

6.1 Kysely

Koko opinnäytetyö perustuu määrälliseen tutkimukseen ja kyselyyn, jolla pyritään saamaan vastaus tutkimusongelmaan. Koska lähes kaikki kerätty tieto saadaan yrittäjille jaettavan kyselyn kautta, on tärkeää varmistaa, että kysely on oikein muodostettu ja määrällistä tutkimusotetta myötäilevä. Kysely kuitenkin eroaa normaalista mallista siten, että kyselystä saadut tulokset ja aineisto eivät sellaisenaan kykene antamaan vastausta tutkimuskysymyksiin ja sitä kautta tutkimusongelmaan. Kyselyn tavoite on tuoda esille yrittäjien ja yritysten aito kyberturvatilanne, joka savutetaan teemoittamalla kysely siten, että toisen osion vastauksia vertaillaan kolmannen osion vastauksiin. Tällä vertailulla pyritään välttämään tilanne, jossa esimerkiksi yrittäjä ei tiedä, mitä oike-

asti kyberturvaan liittyy tai yliarvioi kyberturvan tason yrityksessä. Tässä luvussa käydään läpi kysely ja selitetään kaikki kolme kyselyn teemaa. Tämän avulla voidaan varmistaa tutkimuksen reliabiliteettia.

Kartoitustiedot ja paikallistaminen

Kysely alkaa taustatietojen kartoittamisella, mikä auttaa tarkentamaan kymenlaakson eri alueiden, yritysten kokojen, toimialojen ja verkkopalveluiden tilannetta. Nämä kysymykset sijoitetaan tarkoituksella kyselyn alkuun niiden selkeän vastausmuodon vuoksi. Näiden tietojen kerääminen on olennaista, jotta vastaukset voidaan arvioida asianmukaisesti.

Kyselyn taustatieto- osuus muodostuu viidestä kysymyksestä. Kysely alkaa kysymyksellä yrityksen työntekijämäärästä. Vastausvaihtoehtoina ovat:

a. 5–9
b. 10–19
c. 20–49
d. 50–249
e. 250 →
f. 1–4

Kyselyssä on tärkeä saada selville yrityksen koko. Tämä vaikuttaa suoraan tasotaulukon tulokseen, koska täytyy pystyä ottamaan huomioon pienempien ja suurempien yritysten erot kyberturvan toteutuksessa. Pienemmällä yrityksellä ei välttämättä ole samanlaisia resursseja ylläpitää omaa kyberturvallisuuttaan ja tietoverkkoaan kuin isommalla yrityksellä, jolla on pääomaa investoida turvallisuuteen. Aineistoanalyysissa isommat yritykset sijoittuvat tarkemman aineistoanalyysin piiriin tasotaulukossa.

Kyselyn toinen kysymys koskee yrityksen toimialaa. Yritys vastaa itse, mutta jos varmuutta omasta toimialasta ei ole, käytetään Taloustutkimuksen omaa TOL-listaa. Tilanteessa missä Taloustutkimuksen toimialalistaus on väärä yrityksen toimialasta, merkitään tietoihin yrittäjän oma vastaus. Kun saadaan selville yritysten toimialaluokat, voidaan luoda nosto yritysten tilanteesta toimialaluokkien mukaan.

Kyselyn kolmas kysymys tiedustelee yrityksen mahdollisesta verkkokaupasta tai muusta verkkopalvelusta. Näitä ovat esimerkiksi internetsivut ja asiakasportaalit. Vastausvaihtoehtoina ovat:

a. Kyllä
b. Ei
c. En tiedä

Alussa kysymällä yrityksen julkisesti saatavilla olevista verkkopalveluista, voidaan luoda ristiintaulukointi kysymys 17:n kanssa. Tämä myöhemmässä aineiston tarkastelussa tuo selville tiettyjen GDPR:ään ja tietosuojaselosteeseen liittyviä käytäntöjä, joita on hyvä tarkastella koko kymenlaakson tasolla.

Kyselyn neljäs kysymys kysyy yrityksen kyberturvavakuutuksesta. Vastausvaihtoehtona ovat:

a. Kyllä
b. Ei
c. En tiedä

Kun kysytään yritykseltä sen vakuutuksistaan, pitää se sisällään tietyt ehdot, jotka vakuutusyhtiö on sopimuksessaan asettanut vakuutuksen maksun saamiseksi. Varsinkin kybervakuutuksen kohdalla nämä ehdot ovat tarkkoja ja pitävät sisällään hyvät kyberhygienian tavoitteet, joita myös käydään läpi myöhemmissä luvuissa. Kysymys kysytään, jotta saadaan kerättyä tietoa kybervakuutuksien yleisyydestä Kymenlaaksossa.

Kyselyn viides kysymys ottaa selvää yrityksen työntekijöiden työskentelytiloista ja mahdollisuuksista. Vastausvaihtoehdot ovat:

a. Toimistossa
b. Etänä
c. Hybridi (sekä toimipaikassa että etänä)
d. Yrityksessä ei juurikaan työskennellä toimitiloissa/tietokoneiden kautta (esim. rakennusurakoitsijat)
e. En tiedä

Kysymyksen avulla voidaan luoda vertailukohde henkilökunnan kyber- ja tietoturvan tiedottamiseen tasoon ja etätyön turvallisuuskoulutukseen.

Mielipide

Kysymällä yrittäjän tai työntekijän omaa mielipidettä yrityksensä kyberturvasta, voidaan tuoda esille kaikkia niitä osa alueita, jotka kuuluvat hyviin kyberhygienia tapoihin. Näitä seikkoja tuodaan esille paremmin tarkentavissa kysymyksissä, jotka tulevat mielipideteemaisten kysymysten jälkeen. Vain tässä teemassa on kysymyksiä, jotka on tehty skaaloihin perustuvaan kysymystyyppiin perustuen. Skaala on jaettu 1 ja 5 välillä, jossa 1 tarkoittaa huonointa lukemaa ja 5 parasta lukemaa (Hirsjärvi ym. 2009, 200–201.) Näistä kysymyksistä lasketaan keskiarvo, jota verrataan tarkentavien kysymysten kesiarvoon. Suuri ero keskiarvojen välillä tuo esille sen, että yrittäjä/työntekijä ei välttämättä tiedä mitä kaikkea kyber- ja tietoturvaan sisältyy ja on täten arvioinut väärin oman tasonsa.

Yrittäjän tai vastaavan IT-päällikön mielipidettä mittaava kysymysosuus alkaa kysymyksellä 6: Millaiseksi arvioit kyberturvallisuuden tason yrityksessä, jossa olet yrittäjänä/työntekijänä? Anna arviosi viisiportaisella asteikolla, jossa 1 = heikko ja 5 = erinomainen.

a. 1 = Heikko
b. 2 = Välttävä
c. 3 = Kohtalainen
d. 4 = Hyvä
e. 5 = Erinomainen

Mielipidettä kysyvän kysymyksen kysyminen kyselyn alussa on tärkeä osa opinnäytetyötä. Kysymällä mielipidettä voidaan arvioida yrityksen kyberturvataso toimitusjohtajan/vastaavan IT-päällikön näkökulmasta ja itse tekninen varmuus saadaan kyselyn lopussa olevien tarkentavien kysymysten avulla. Näin voidaan näyttää ristiriita mielipiteiden ja konkreettisten turvatoimien välillä.

Yrittäjän tai vastaavan IT-päällikön mielipidettä mittaava kysymysosuuden 7 kysymys: Kuinka hyvin uskot yrityksen selviytyvän kyberhyökkäyksestä? Anna arviosi viisiportaisella asteikolla, jossa 1 = heikko ja 5 = erinomainen.

a. 1 = Heikosti
b. 2 = Välttävästi

c. 3 = Kohtalaisesti
d. 4 = Hyvin
e. 5 = Erinomaisesti

Kun kysytään yrittäjältä hänen mielipidettään yrityksen selviytymiseen, voidaan luoda vertailu kohde kysymykselle 13. Samalla saadaan selville yrittäjän asenne yrityksen jatkuvuuteen.

Yrittäjän tai vastaavan IT-päällikön mielipidettä mittaava kysymysosuuden 8 kysymys: Kuinka tärkeänä näet kyberturvan merkityksen yritystoiminnassa? Anna arviosi viisiportaisella asteikolla, jossa 1 = heikko ja 5 = erinomainen.

a. 1 = Ei lainkaan tärkeänä
b. 2 = Vähemmän tärkeänä
c. 3 = Kohtalaisen tärkeänä
d. 4 = Melko tärkeänä
e. 5 = Erittäin tärkeänä

Kysymyksessä periaate on sama kuin aikaisemmassa ja tarkoituksena on varmistaa yrittäjän asenne ja mahdolliset erot yrityksen kyberturvan suhteen.

Tarkentavat kysymykset

Tarkentavilla kysymyksillä pyritään saamaan vahvistus aikaisempiin mielipidekysymyksiin. Kysymyksillä halutaan varmistaa, että vastaaja tietää mitä oikeasti liittyy niin sanottuun hyvään kyberturvaan, jota kysyttiin aiemmin. Tämänkaltaisen toiminnan tarkoituksena on löytää mahdolliset virheelliset arviot oman yrityksensä tai työpaikkansa kyberturvallisuudesta. Tällaisessa arviossa saatetaan esimerkiksi aliarvioida kalasteluviestien vakavuutta ja niihin liittyviä toimenpiteitä yritystoiminnassa. Tarkentavat kysymykset liittyvät juuri niihin aloitustason teknisiin toimiin, joilla voidaan määrittää hyvä kyberhygieniataso. Nämä toimet voivat pitää sisällään verkkoturvallisuutta, jatkuvuussuunnitelmia ja mahdolliset tietosuojaselosteet verkkoasiakkaille. Lisäksi näihin sisältyy salasanahygienia yrityksen laitteille, työntekijöiden pääsynhallintaa sekä mahdolliset tietotekniset toteutukset laitteiston turvaamiseen liittyen.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuus alkaa kysymyksellä 9: Pidetäänkö yrityksessä kyberturvallisuuteen liittyviä koulutuksia työntekijöille?

a. Parin kuukauden välein
b. Parin vuoden välein
c. En ole varma onko koskaan järjestetty
d. Ei ole koskaan järjestetty
e. En tiedä

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä kymmenen kysytään yrityksen kyberturvatapojen ylläpidosta. Tapoihin kuuluu esimerkiksi tietokoneen lukitseminen, kun sitä ei käytetä tai vahvat salasanakäytännöt. Yrittäjän tai vastaavan IT-päällikön tuli valita vaihtoehdoista yritystään parhaiten kuvaavin.

a. Henkilöstöä on ohjeistettu yrityksen kyberturvakäytännöistä ja sitä valvotaan aktiivisesti
b. Henkilöstöä on ohjeistettu, mutta valvonta ei ole aktiivista tai sitä ei ole ollenkaan
c. Henkilöstöä ei ole ohjeistettu yrityksen kyberturvakäytännöistä
d. En tiedä

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä yksitoista kysytään yrityksen tietoteknisestä inventaariosta eli listaus kaikista käytössä olevista tietoteknisistä laitteista ja ohjelmistoista. Vastausvaihtoehdot ovat:

a. Kyllä
b. Ei ole
c. En osaa sanoa

Luotu antamaan vastapainoa varsinkin mielipide kysymykselle 7.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä kaksitoista kysytään yrityksen toimia liittyen monivaiheinen tunnistautuminen. Näitä ovat esimerkiksi tekstiviestivahvistukset tai mobiilisovellus.

a. Kyllä, kaikissa sovelluksissa ja palveluissa
b. Joissakin sovelluksissa ja palveluissa
c. Ei, yrityksessä ei käytetä monivaiheista tunnistautumista
d. En tiedä käytetäänkö

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä kolmetoista kysytään yrityksen jatkuvuussuunnitelmasta. Jatkuvuussuunnitelma takaa yritystoiminnan jatkumisen kyberhyökkäyksen tai muun yritystoimintaa uhkaavan tilanteen sattuessa. Vastausvaihtoehdot ovat seuraavat:

a. Yrityksessä on luotu jatkuvuussuunnitelma ja sen sisältö on jaettu yrityksen työntekijöiden kanssa sekä sitä on harjoiteltu
b. Jatkuvuussuunnitelma on tehty, sen sisältö on jaettu yrityksen työntekijöiden kanssa sekä sitä on harjoiteltu, mutta sitä ei ole päivitetty pitkiin aikoihin
c. Yrityksessä on luotu jatkuvuussuunnitelma, mutta sitä ei ole jaettu muille työntekijöille eikä harjoiteltu
d. Jatkuvuussuunnitelmaa ei ole tehty
e. En tiedä mikä on jatkuvuussuunnitelma

Luotu antamaan vastapainoa varsinkin mielipide kysymykselle 7.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä neljätoista kysytään yrityksen toimista laitteiden suojausohjelmistojen suhteen. Näitä ohjelmistoja ovat esimerkiksi virustorjuntaohjelmat. Vastausvaihtoehdot ovat seuraavat:

a. Kaikissa tietokoneissa ja älylaitteissa on suojausohjelmistoja
b. Vain tietyissä tietokoneissa tai älylaitteissa on suojausohjelmistoja
c. Missään tietokoneissa tai älylaitteissa ei ole suojausohjelmistoja
d. En tiedä käytetäänkö laitteissa suojausohjelmia / en osaa sanoa

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä viisitoista tiedustellaan yrityksen pääsynhallinnasta. Kyselyssä halutaan erityisesti tietää, kuinka yrityksessä on määritetty pääsynhallinta. Esimerkiksi henkilöt, joilla ei ole oikeuksia, eivät pääse käsittelemään heille kuulumattomia tiedostoja tai pääse toimitiloissa sellaisiin paikkoihin, jonne heillä ei ole asiaa. Vastausvaihtoehdot ovat seuraavat:

a. Jokaisella yrityksen työntekijällä on keino todentaa oma henkilöllisyytensä siten, että voidaan varmistua pääsynhallinnan toimivan
b. Pääsynhallinta on käytössä vain yrityksen kriittisissä paikoissa ja todella salassa pidettävissä tiedostoissa
c. Yrityksessä ei ole pääsynhallintaa
d. En tiedä käytetäänkö yrityksessä pääsynhallintaa

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä kuusitoista kysytään henkilökunnan ohjeistuksesta etätyön kyberturvan suhteen. Vastausvaihtoehdot ovat seuraavat:

a. Kyllä
b. Ei ole
c. Yrityksessä ei ole työntekijöitä / Yrityksessä ei tehdä etätyötä
d. En tiedä

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8.

Yrityksen konkreettisia kyber- ja tietoturva toimia mittaava kysymysosuuden kysymyksessä seitsemäntoista kysytään yrityksen toimintaa asiakastietojen suhteen. Asiakastietoihin kuuluu esimerkiksi henkilökohtaiset tiedot kuten nimet, puhelinnumerot, sähköpostit jne. Vastausvaihtoehdot ovat seuraavat:

a. Yritys kerää tarvittavat asiakastiedot, jotka ovat määritelty yrityksen tietosuojaselosteessa
b. Yritys kerää asiakkaista tietoja, joita voidaan mahdollisesti tarvita tulevaisuudessa tietosuojaselosteen mukaisesti
c. Yritys kerää asiakastietoja ilman tietosuojaselosteen määrittelyä
d. Yritys ei kerää ollenkaan asiakastietoja
e. En tiedä kerääkö yritys asiakastietoja

Luotu antamaan vastapainoa varsinkin mielipide kysymyksille 6 ja 8 ja kartoitus kysymykselle 3.

6.2 Kyselyn teemat ja muotoilu

Kyselyn rakenne on muotoiltu kahta pääperiaatetta seuraten. Ensimmäinen on kyselyn muotoilu siten, että vastaajat jaksavat vastata kaikkiin kysymyksiin ajatuksella. Tämä pyritään saavuttamaan laittamalla kyselyn alkuun lyhyempiä kysymyksiä, joihin on helppo vastata. Tämän avulla voidaan luoda vastaajalle kuvitelma, että kysely ei ole niin työläs tehdä kuin on alun perin kuviteltu. Kyselyn tulee myös olla sen verran lyhyt, että vastaajat jaksavat vastata myös viimeisiin kysymyksiin (Hirsjärvi ym. 2009, 202–203.) Toinen periaate on yhdistää kyselyssä kysymyksiä, jotka tukevat toisiaan siten, että niiden avulla voidaan selvittää yrityksen oikea kyberturvataso, kun sitä verrataan tasotaulukkoon. Esimerkki tällaisesta yhdistämisestä on kysyä yrityksen kyberturvatasoa vastaajan omien mielipiteiden perusteella. Kuitenkin muut kysymykset tarjoavat mahdollisuuden todentaa tämä kysymys kysymällä esimerkiksi tarkemmin yrityksen tietoturvatasosta tai hyvien salasanasuositusten noudattamisesta. Kysymykset myös jaetaan teemoihin niin, että mielipiteitä koskevat kysymykset ja tarkentavat kysymykset voidaan erottaa toisistaan.

Hyviä kyselylomakkeen esimerkkejä myötäillen kyselyssä pyritään myös varmistamaan kaikkien kysymysten ymmärrettävyys välttämällä vaikeaa tekniikan sanastoa. Tarjoamalla myös useampia vaihtoehtoja kysymysten vastaamiseen ja välttämällä ”samaa mieltä / eri mieltä” -väitteitä (Hirsjärvi ym. 2009, 202–203.) Vaikka määrällisen tutkimuksen kyselyissä pyritään välttämään kyllä ja ei -vastausvaihtoehtoja sen suoraviivaisen ja kapean luonteen vuoksi, joudutaan osaan vastausvaihtoehdoista kuitenkin muotoilemaan ”kyllä/ei/en osaa sanoa” -vastausmuotoon. Näin siksi että tarkoitus on saada kartoitettua tietoa yrityksen sisäisistä hankinnoista ja kerättyä tärkeää tietoa ilman, että kyselystä tulisi liian pitkä.

6.3 Tasotaulukko

Tasotaulukon tarkoitus on luoda keino pisteyttää yrityksiä siten, että tulokset pysyvät samana riippumatta yrityksen koosta ja toimialasta. Luomalla pohja kyselyaineistonanalyysille voidaan samalla myös parantaa reliabiliteettia. Tasotaulukko helpottaa myös aineistoanalyysia siten, että vaikka kyselyyn vastaisi huomattava määrä yrityksiä, ei yritysten vastausten analysointi missään kohtaa periaatteessa voi vääristyä. Jokainen yritys käy läpi saman analysointivaiheen yrityskoon mukaan, mikä pienentää mahdollisuutta virheiden syntymiseen.

Tasotaulukon muuttuva pisteytys yrityksen henkilömäärän mukaan on suoraan verrannollinen yrityksen kokoon. Suurilla yrityksillä on enemmän tietotaitoa ja resursseja parantaa omaa kyber- ja tietoturvallisuuden valmistautumistaan. Jos tasotaulukon pisteytys luodaan olettaen, että jokaisen yrityksen tulisi hoitaa oma kyber- ja tietoturvallisuutensa suuren yrityksen tavoin, on riskinä tulosten vääristyminen. Pienimmillä yrityksillä ei ole samankaltaista osaamista sekä resurssia hoitaa oma kyber- ja tietoturvaansa samalla lailla kuntoon kuin isoilla yrityksillä, jonka vuoksi pisteytys pitää luoda tämä huomioon ottaen. Yrityskokojen pisteytykset on perusteltu henkilöstökoon ja liikevaihdon mukaan. Lukemat näille saadaan alla olevasta taulukosta.

Taulukko 2. Keskimääräinen liikevaihto yrityskokojen mukaan (Tilastokeskus 2022)

Yritykset henkilöstön suuruusluokan mukaan 2022

Henkilöstön suuruusluokka	Yritykset		Henkilöstö, henkilötyö-vuotta		Liikevaihto	
	Lukumäärä	%	Tuhatta	%	Milj. €	%
Yhteensä	**571 742**	**100**	**1 498**	**100**	**555 953**	**100**
0–4	533 811	93,4	219	14,6	68 271	12,3
5–9	17 728	3,1	115	7,7	30 092	5,4
10–19	10 021	1,8	134	9,0	35 904	6,5
20–49	6 380	1,1	191	12,8	55 893	10,1
50–99	2 106	0,4	146	9,8	53 748	9,7
100–249	1 027	0,2	156	10,4	58 783	10,6
250–499	369	0,1	126	8,4	46 679	8,4
500–999	176	0,0	124	8,3	47 950	8,6
1 000–	124	0,0	286	19,1	158 633	28,5

Kun käyttää apuna Tilastokeskuksen Yritysten rakenne- ja tilinpäätöstilastosta (2022) saatua henkilöstön suuruusluokkaa, voidaan laskea keskimäärin yhden yrityksen liikevaihto. Liikevaihdon mittaaminen on näin suuren kyselyn tapauksessa paras keino mitata yritystoiminnan laajuutta.

- 0–4 = 127 894 €
- 5–9 = 1 697 428 €
- 10–19 = 3 582 876 €
- 20–49 = 8 760 658 €
- 50–99 = 25 521 367 €
- 100–249 = 57 237 585 €

Guim (2021) laski artikkelissaan pienen, keskisuuren ja suuren yrityksen keskimääräisen vuosittaisen budjetin kyberturvallisuusinvestoineille:

- Suuryritys: 2 ja 5 miljoonan dollarin välillä
- Keskisuuri: 500 000 ja 2 miljoonan dollarin välillä
- Pieni yritys: Alle 500 000 dollaria

Vaikka nämä ovat tiedot pohjustavatkin Yhdysvaltojen yrityksiin, luo se silti tarvittavan vertailupohjan Suomen alueen yrityksiin, kun otetaan huomioon suomalaisen ja eurooppalaisen dokumentaation vähyys asiaan liittyen. Ison ja pienen yrityksen ero saadaan Tilastokeskuksen (s.a) pienen yrityksen käsitteen määrittelystä. Pieni yritys määritellään yritykseksi, jonka:

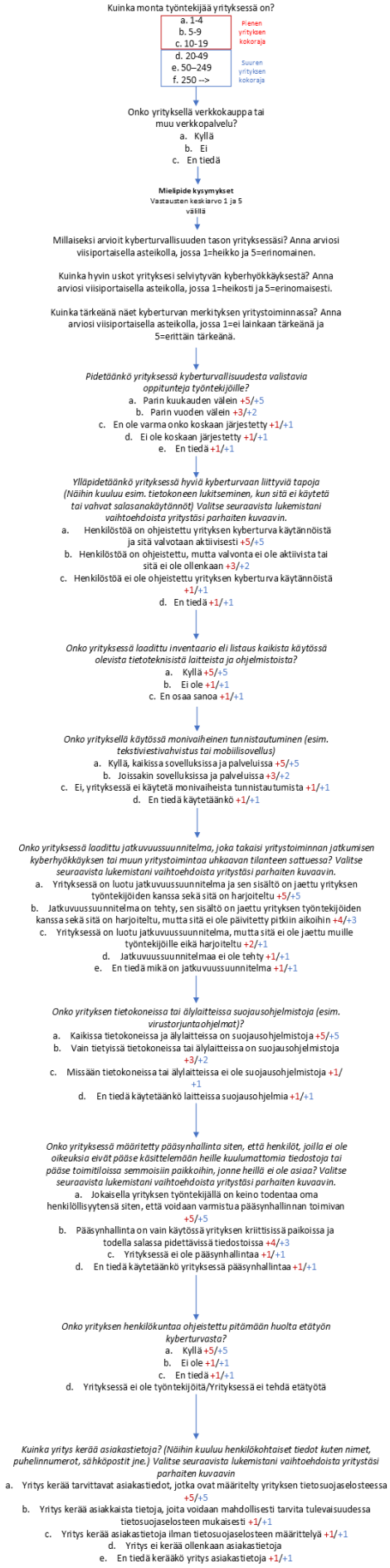
1. palveluksessa on vähemmän kuin 50 työntekijää
2. vuosiliikevaihto on enintään 10 miljoonaa euroa
3. tai taseen loppusumma on enintään 10 miljoonaa euroa

Määrityksen mukaan siis kaikki yritykset, joissa on yli 50 työntekijää ovat silloin joko keskisuuria tai suuria yrityksiä. Kuitenkin pieni yritys, jolla on esimerkiksi 30 työntekijää, on kuitenkin osaamis- ja resurssitasoltaan varsin korkeassa asemassa, kun otetaan huomioon mahdollinen liikevaihto sen kokoiselle yritykselle. Tasotaulukon tilanteessa kevennystä pistemääriin saavat kaikki yritykset, joissa on alle 19 työntekijää. Tämänkokoisilla yrityksillä liikevaihto osoittaa yrityksen puutteet kokonaisvaltaiseen kyber- ja tietoturvan kattamiseen. Jos lasketaan keskimääräinen osuus kyber- ja tietoturvan investoinneista pienelle yritykselle, alle 10–19 henkilöä työllistävien yrityksien puolen miljoonan investointi olisi noin 14 % vuosittaisesta liikevaihdosta. Kun lisäksi otetaan huomioon mahdolliset haasteet oikeanlaisen osaamisen hankkimisessa, niin ei voida olettaa tämänkokoisten yritysten pystyvän samoihin tuloksiin kuin suuremmat yritykset.

Tasotaulukon ulkoasu

Alle on luotu tasotaulukon visuaalinen ulkoasu, jota vasten jokainen kyselyanalyysi tehdään. Tämänkaltainen visuaalinen versio tasotaulukosta parantaa opinnäytetyön reliabiliteettia ja varmistaa tutkimuksen jatkokehitysideat, tuomalla esille tarkasti kuinka analysointi on konkreettisesti tehty. Visualisoimalla tasotaulukko saadaan pisteytys yksinkertaisemmin myös ilmi jokaisen kysymyksen ja yrityskoon osalta.

Taulukko 3. Tasotaulukon pistelasku reliabiliteetin varmistamiseksi

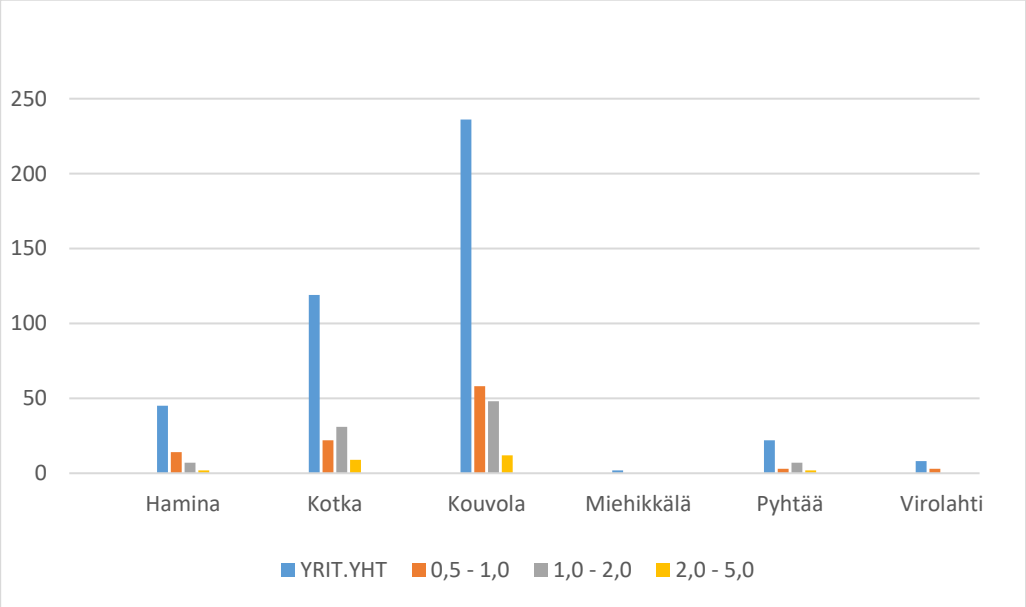


Tasotaulukko pyrkii myös tuomaan esille erot yrittäjän olettamuksen ja teknisten toimien välillä. Kuitenkin osa yrittäjistä on mielipideosiossa antanut vastauksen ”en tiedä”. Tämän kaltaisen vastauksen esiintyessä käytetään hyödyksi tarkentavia kysymyksiä, joista luodaan mielipiteelle arvo. Esimerkiksi, jos yrittäjä vastaa kuudenteen kysymykseen vastauksella ”en tiedä”, lasketaan kyseisen mielipiteen arvo kysymyksistä 9, 10, 12, 14, 15, 16, 17. Jos kaikkiin mielipidekysymyksiin on vastattu vastauksella ”en tiedä”, niin haastattelu ohitetaan. Kun mielipiteille on laskettu uusi arvo tarkentavien kysymysten avulla, käydään analyysi sen jälkeen normaalilla tavalla läpi.

7 TULOKSET

Taloustutkimus teki kyselyn strukturoituna (ja yhtenä avoimena kysymyksenä) 432 Kymenlaakson alueen yritykselle. Kysely suoritettiin puhelinkyselynä, jossa yksittäisen haastattelun keskimääräinen pituus oli noin 10 minuuttia. Jokainen haastattelu käytiin tasotaulukon avulla läpi, jotta jokainen kyselyyn vastannut yritys saataisiin arvioitua. Tässä luvussa käydään läpi haastatteluiden kautta saadut tulokset. Alla olevaan taulukkoon on listattu eroavaisuudet, jotta niistä käy selväksi jokaisen kaupungin osuus eroavaisuuksista.

Taulukko 4. Vääristymien osuus yritysmääristä kaupungeissa



Kun ottaa koko Kymenlaakson huomioon, niin eroavaisuudet 432 yritykselle olivat seuraavat:

- 0,5–1,0 = 100
- 1,0–2,0 = 93
- 2,0–5,0 = 25

Yhteensä tämä on 218 eli noin 50,45 prosenttia kaikista Kymenlaakson yrityksistä. Yksittäisten vääristymien osuus koko Kymenlaakson tilanteesta on seuraavanlainen:

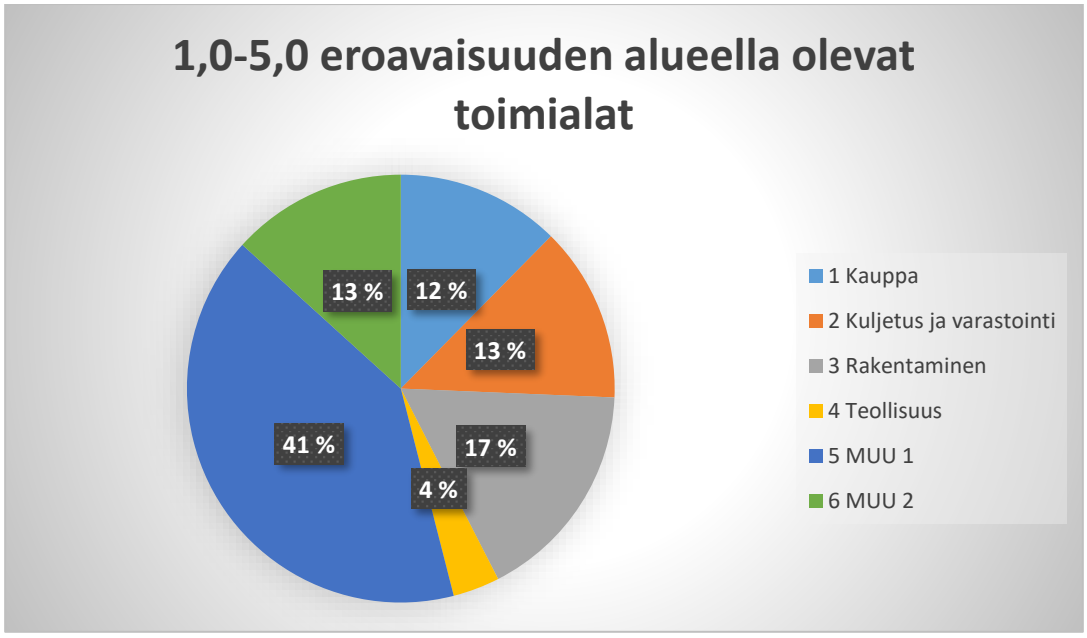
- 0,5–1,0 = 23,15 %
- 1,0–2,0 = 21,53 %
- 2,0–5,0 = 5,79 %

Alla tämä on vielä ilmaistu graafisesti.

Taulukko 5. Tarkat lukemat vääristymistä kaupunkien mukaan

	Hamina	Kotka	Kouvola	Miehikkälä	Pyhtää	Virolahti
YRIT.YHT	45	119	236	2	22	8
0,5 - 1,0	14	22	58	0	3	3
1,0 - 2,0	7	31	48	0	7	0
2,0 - 5,0	2	9	12	0	2	0

0,5:n–1,0:n eroavaisuus on lievin eroavaisuuden taso, kun otetaan huomioon tasotaulukon pisteytys. Koska yritysotannasta suuri enemmistö sisälsi mikro- ja yksinyrittäjiä, ei voida tuloksia suoraan vertailla yrityskokojen mukaan.



Kuva 6. Vääristymien osuus yritysmääristä kaupungeissa

Yllä oleva ympyräkaavio selittää kuinka toimialat sijoittuvat tasotaulukon vääristymiin. Kaaviossa näkyvät MUU 1 ja MUU 2 ovat Taloustutkimuksen räätä-

löimiä toimialapaketteja ja toimivat usein niin sanottujen toimialojen keräilyerinä eli ovat sellaisia toimialoja, joita ei saada mukavasti niputettua yhden otsikon alle (esimerkiksi teollisuus, rakentaminen ja niin edelleen). Alle on annettu esimerkkitaulukko, joka kuvaa, kuinka toimialat on listattu tiedostoon.

Taulukko 6. Muu ryhmien sisällöt Excel taulukossa

(08111) Koriste- ja rakennuskiven louhinta
(08120) Soran, hiekan, saven ja kaoliinin otto
(08920) Turpeen nosto
(09900) Muuta kaivostoimintaa ja louhintaa palveleva toiminta
(33110) Metallituotteiden korjaus ja huolto
(33121) Yleiskäyttöön tarkoitettujen koneiden korjaus ja huolto
(33122) Maa- ja metsätalouskoneiden korjaus ja huolto
(33123) Metallintyöstökoneiden ja muiden konetyökalujen korjaus ja huolto
(33129) Muiden erikoiskoneiden korjaus ja huolto
(33130) Elektronisten ja optisten laitteiden korjaus ja huolto
(33140) Sähkölaitteiden korjaus ja huolto
(33150) Laivojen ja veneiden korjaus ja huolto
(33170) Muiden kulkuneuvojen korjaus ja huolto
(33190) Muiden laitteiden korjaus ja huolto
(33200) Teollisuuden koneiden ja laitteiden ym. asennus
(35111) Sähkön tuotanto vesi- ja tuulivoimalla
(35113) Sähkön ja kaukolämmön yhteistuotanto
(35115) Teollisuutta palveleva sähkön ja lämmön tuotanto
(35120) Sähkön siirto
(35130) Sähkön jakelu
(35140) Sähkön kauppa
(35210) Kaasun tuotanto
(35220) Kaasumaisten polttoaineiden jakelu putkiverkossa
(35301) Kaukolämmön ja -kylmän erillistuotanto ja jakelu

MUU-ryhmä luotiin alun perin sisältämään toimialat, jotka eivät syystä tai toisesta sopineet suurten toimialakäsitteiden alle. Lisäksi MUU-ryhmään haluttiin sisällyttää toimialoja, joiden kyber- ja tietoturvatasosta haluttiin ottaa erityisesti selvää. Koska MUU-ryhmä pitää sisällään todella paljon toimialoja, ei niitä kaikkia ole pystytty liittämään tutkimukseen esille. Tämän takia toimialat voi tarkastaa täältä omasta Excel tiedostostaan: Muu ryhmien sisältö.xlsx.

Koska 0,5:n–1,0:n eroavaisuus voidaan olettaa rehelliseksi tietämättömyydeksi omasta kyber- ja tietoturvatasostaan, samaa ei voida sanoa 1,0:n–2,0:n ja 2,0:n–5,0:n välisistä eroavaisuuksista. Yritykset, jotka osuivat näille väleille ovat arvioineet oman yrityksensä tason vahvasti väärin. Näille väleille osui yhteensä 193 yritystä, joista vain 6 oli suurempia kuin 10–19 henkilöstöluokassa

ja arvioitiin suuremman yrityksen pisteytyksen mukaan. Vahva enemmistö yrityksistä kuului 1–4 henkilön kokoluokkaan. Tulos ei koko Suomen kontekstissa ole yllättävä, Tilastokeskuksen (2022) Yritysten rakenne- ja tilinpäätöstilastoa taulukko näyttää liikevaihdon lisäksi myös Suomessa toimivien yritysten lukumäärät. Taulukosta voidaan nähdä, että 0–4 henkilöä työllistävien yritysten osuus Suomen kaikista yrityksistä on 93 prosenttia. Pelkästään näin suuren luvun takia voidaan olettaa, että suurin osa yrityksistä, jotka osuvat 1,0:n–5,0:n väliselle eroavaisuusrajalle olisi yksin- ja mikroyrityksiä. Kuitenkin yrityksiä, joiden arviointi ei tuonut esille eroavaisuuksia yrittäjän oman mielipiteen ja konkreettisten toteutuksien välillä oli yhteensä 214, näistä 133 oli 1–4 henkilöä työllistäviä yrityksiä eli noin 62 prosenttia. Vuoden 2020 digibarometrin tilannekuvassa mainittiin suomalaisten yksin- ja mikroyritysten kyberturvatilanteesta olevan tällä hetkellä varsin niukasti tietoa olemassa (Mattila, Ali-Yrkkö ym. 2020, 23). Tämänkaltaista dataa ei ole koskaan aikaisemmin saatu kerättyä Kymenlaakson alueella ja varsinkaan yksin- ja mikroyrityksistä.

8 NOSTOT

Kysely piti sisällään myös paljon kysymyksiä, jotka toivat esille mielenkiintoisia nostoja yleisesti yritysten kyberhygieniaan liittyvistä toimista, kuten etätyön kyber- ja tietoturvasta, asiakastiedoista ja jatkuvuussuunnitelmasta. Tulokset näihin liittyvistä kysymyksistä olivat mielenkiintoisia jo pelkästään sen takia, että ne osoittavat tiettyjen kyber- ja tietoturvaan liittyvien aiheiden tilanteen Kymenlaaksossa. Alla on tilastoja ja kuvia yksittäisien kysymyksien vastauksista ja ristiintaulukointia kahden kysymyksen välillä. Ristiintaulukoinnit toimitti Taloustutkimus Oy osana haastattelutarjousta.

Kuva 7. Vastanneiden prosenttiosuudet kolmanteen haastattelukysymykseen

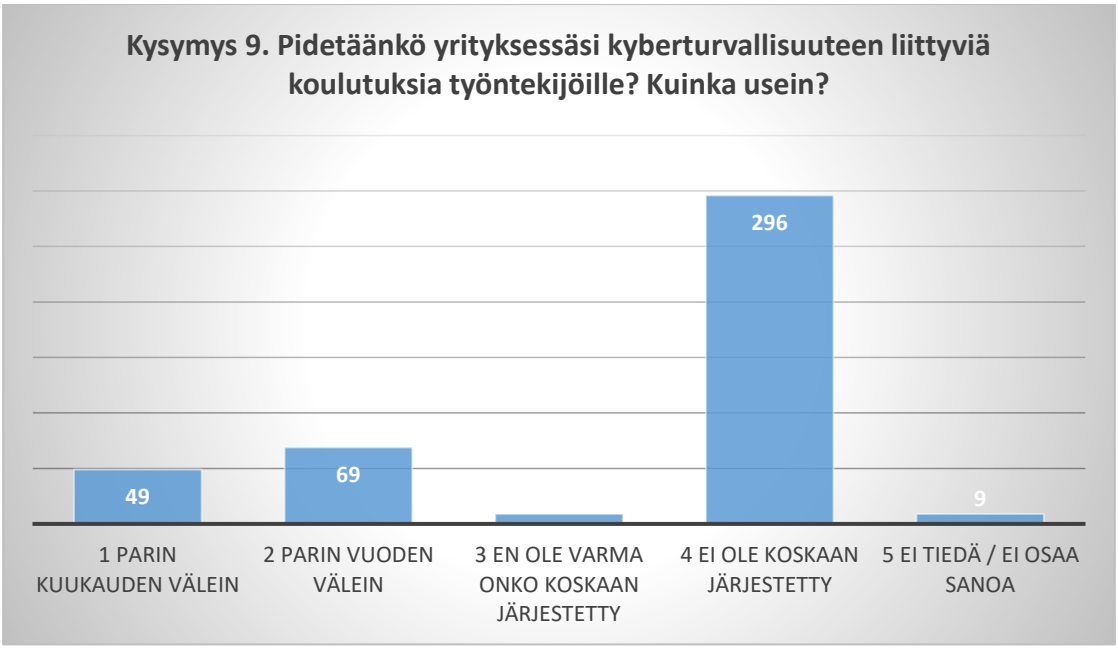
Kysymys kolme toi esille yritykset, joilla on käytössä erilaisia verkkopalveluja, kuten verkkokauppa, asiakasportaali tai internetsivut. 432 yrityksestä 262:lla (61 %) oli käytössään jonkinlainen verkkopalvelu käytössään. Yrityksien suurella enemmistöllä on jonkinasteista näkyvyyttä julkiseen verkkoon. Vaikka nykyään verkkosivujen ja verkkokauppojen ylläpitäminen on tehty helpoksi kolmannen osapuolten palveluiden avulla (esim. WordPress, Squarespace), ei se poista riskiä joutua kyberuhan kohteeksi. Vaikka tekniset hyökkäykset kolmannen osapuolen ylläpitämiin yritysverkkosivuihin ovat harvinaisia, eivät ne poissulje sosiaalisen manipuloinnin hyökkäyksiä, joissa pyritään saamaan verkkosivut hallintaan käyttäjätunnusten kautta.

Kuva 8. Vastanneiden prosenttiosuudet haastattelukysymykseen kymmenen

Kysymys kymmenen tuo hyvää jatkoa aikaisempaan kuvaan, koska se tuo esille yritysten mahdolliset yleispäteviin kyberturvakäytäntöihin liittyvät vaaranpaikat. 432 yrityksestä 209 (48 %) oli ohjeistanut henkilöstöä kyberturvakäytännöistä ja niitä valvottiin aktiivisesti. Kyselyssä ei kuitenkaan erikseen varmistettu, olivatko käytännöt alun pitäen hyvät, joten tämä kysymys oli yrityksen oman tulkinnan varassa. 223 (52 %) yritystä oli kuitenkin vastannut käytäntöjen tekemisen tai niiden valvomisen olleen puutteellista.

Kuva 9. Vastanneiden prosenttiosuudet haastattelukysymykseen kaksitoista

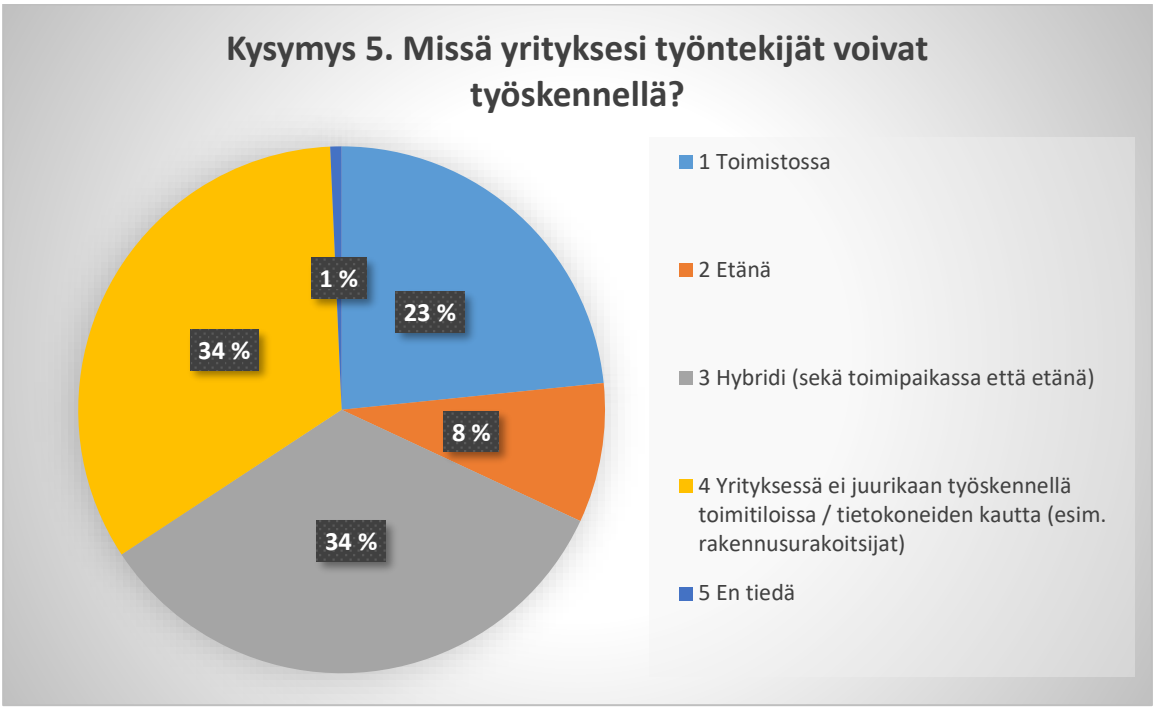
Kysymys kaksitoista luo lisää jatkumoa kysymyksille kolme ja kymmenen. 432 yrityksestä 224 (52 %) käytti jossain määrin sovelluksissaan ja palveluissaan kaksivaiheista tunnistautumista. 104 yrityksessä (24 %) oli kaikissa palveluissa ja ohjelmissa käytössään kaksivaiheinen tunnistautuminen. Tämän pohjalta voidaan positiivisesti todeta, että Kymenlaakson alueella yritykset ovat olleet aktiivisia ottaessaan käyttöönsä multi-factor authentication (MFA) tekniikkaa. Jos näiden tulosten pohjalta oletetaan, että kaksivaiheista tunnistautumista käytetään myös verkkosivujen hallintapuolella, luo se vahvaa lisäsuojaa, jos käyttäjätunnukset anastetaan tai murretaan. Tässä tietenkin olettaen, että työntekijä tai yrittäjä ei lankea hyökkääjän sosiaalisen manipuloinnin keinoihin. Tätä varten tarvitaan koulutusta yrityksissä, jotta työntekijät tai itse yrittäjä voivat huomata mahdolliset manipuloinnin keinot.



Kuva 10. Vastanneiden lukumäärät haastattelukysymykseen yhdeksän

432 yrityksestä 296 (68,5 %) ei ole koskaan järjestänyt työntekijöille minkäänlaista kyberturvallisuuskoulutusta. Vaikka luku on suuri, täytyy tässäkin ottaa huomioon yksin- ja mikroyritysten osuus kokonaisotannasta. Näiden yritysten resurssit ja henkilökuntamäärät ovat usein aivan liian pieniä. Tämän takia yrittäjä voi ajatella koulutusten olevan hyödyttömiä ja pelkkä kuluerä. Yrittäjät voivat myös luulla heidän yrityksensä olevan aivan liian pieni kyberhyökkäyksille. Tätä tukee Insurance Bureau of Canadan (2023) tekemä kyberturvallisuuskysely, josta paljastui, että yli 60 % pienistä yrityksistä uskoo heidän yrityksensä

olevan aivan liian pieni joutuakseen verkkorikollisten kohteeksi. Tässä tosin pitää myös ottaa huomioon Kanadan suuret yrityskoot jopa pienyrityskategoriassa. Tämän takia kuitenkin voidaan olettaa, että yksin-, mikro- ja jopa pienyrittäjät eivät näe tarpeellisena kouluttaa itseään ja henkilökuntaansa siinä toivossa, että heidän yrityksensä ei tule koskaan kokemaan kyberhyökkäystä.

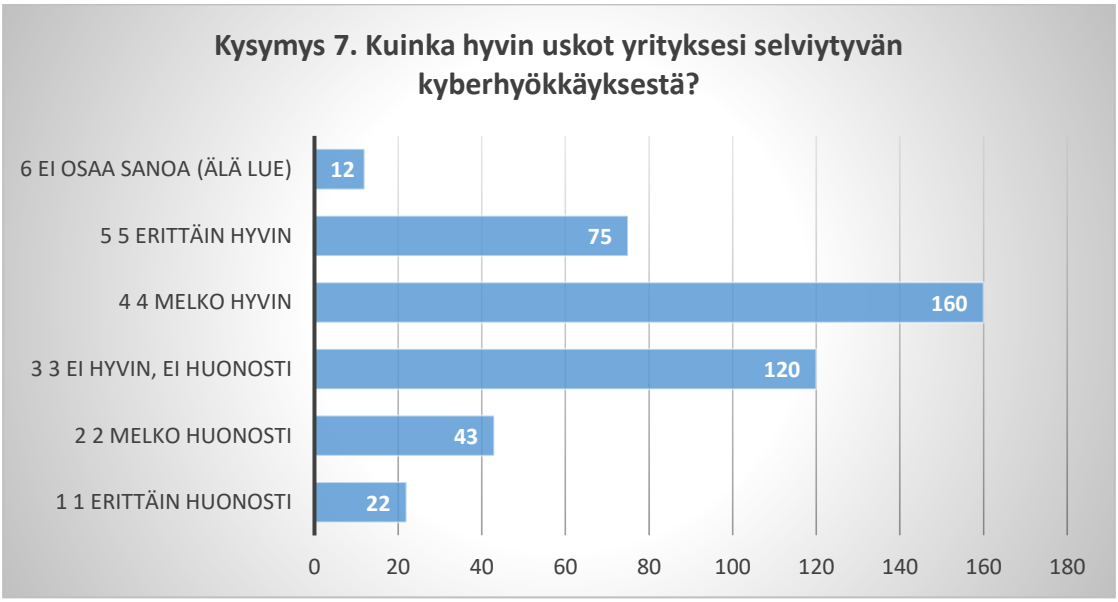


Kuva 11. Vastanneiden prosenttiosuudet viidenteen haastattelukysymykseen

Kysymys viisi tuo esille, että Kymenlaakson yritykset ovat ottaneet aktiivisesti myös etätyön käyttöön omassa yritystoiminnassa. 432 yrityksestä 183 (42 %) on soveltanut omaan yritystoimintaansa etätyötä. Yhteensä yrityksiä, joissa ei ole etätöitä/työskennellä aktiivisesti tietokoneiden kautta, oli 246 (57 %).

Kuva 12. Vastanneiden lukumäärät haastattelukysymykseen kuusitoista

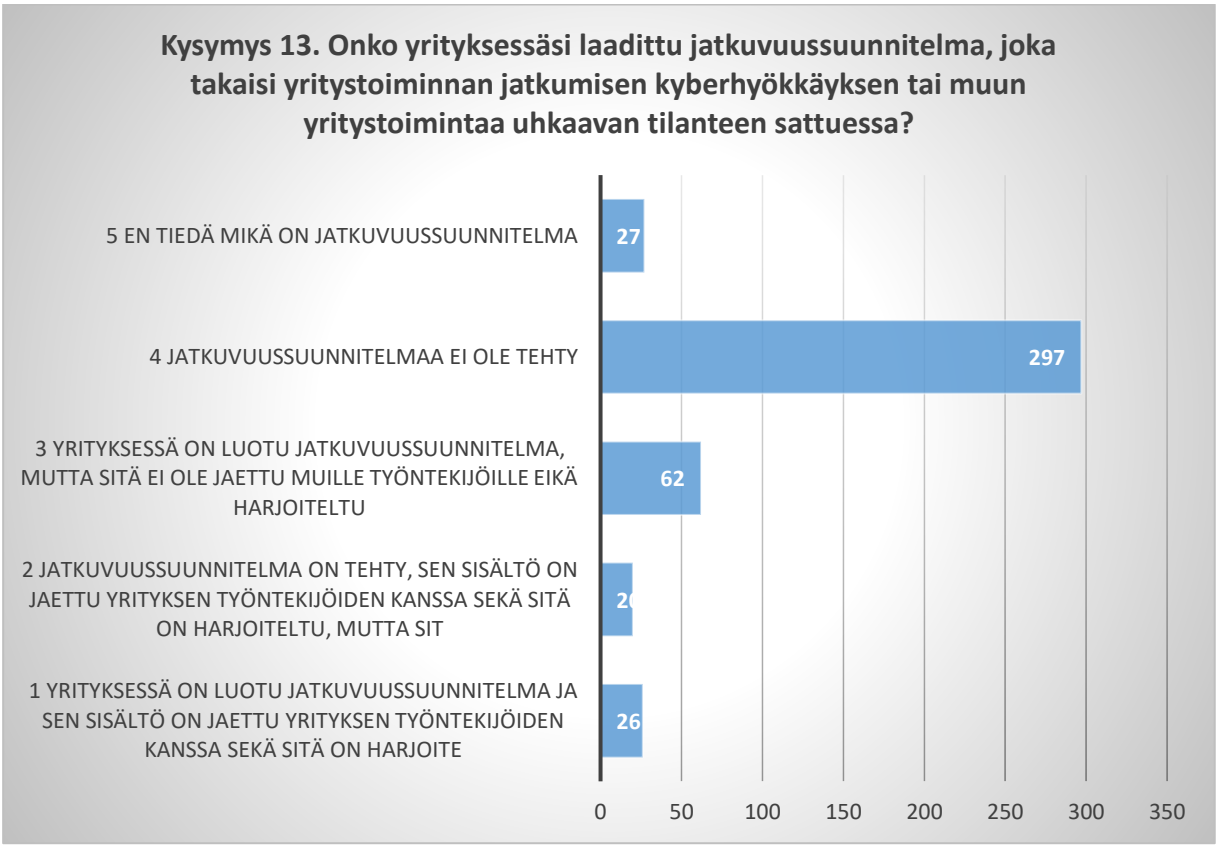
Kysymys kuusitoista tuo suoraa jatkoa kysymykseen viisi, jossa kysyttiin henkilökunnan etätyön kyberturvan ohjeistuksesta. Yhteensä 432 yrityksestä 189 (44 %) oli ohjeistanut henkilökuntaansa pitämään huolta etätyön kyberturvasta ja vain 49 (11 %) yritystä ei ollut ohjeistanut henkilökuntaansa. Tulos on positiivinen siinä mielessä, että tulos on 103,28 prosenttia korkeampi kuin yritykset, jotka olivat ottaneet käyttöön etätyön. Tätä voidaan myös selittää rehellisellä erehdyksellä yrittäjän puolelta, mutta myös yrityskoulutuksena, jossa oli käyty etätyön kyberturvaa läpi, vaikka yrityksessä ei pääsääntöisesti tehtäisikään etätöitä.



Kuva 13. Vastanneiden lukumäärät haastattelukysymykseen seitsemän

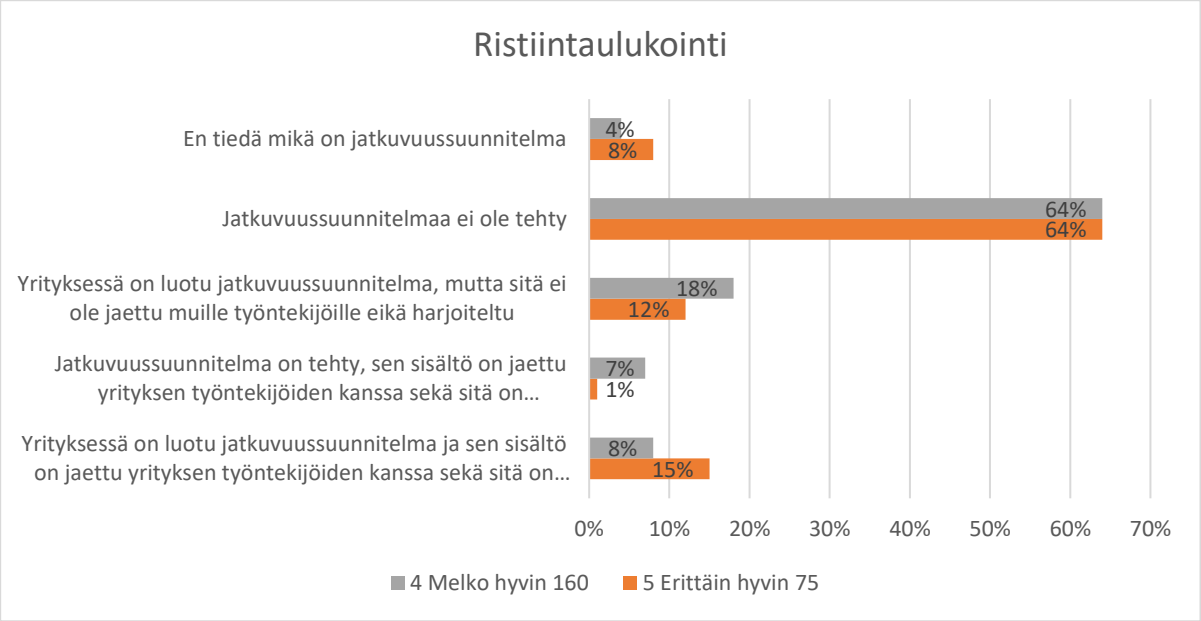
Kyselyssä pyrittiin myös selvittämään yritysten kriisinhallintaan ja varsinkin jatkuvuussuunnitelmaa. Mielipidekysymyksessä seitsemän tiedusteltiin yrittäjän

mielipidettä yrityksen selviytymiseen, jos siihen kohdistuu kyberhyökkäys. 432 yrityksestä 235 (54 %) yrittäjää uskoi yrityksensä selviytyvän kyberhyökkäyksestä joko melko hyvin tai erittäin hyvin. Jos tähän luetaan myös mukaan kolmas vastausvaihtoehto, on yritysten kriisinkestävyys todella vahvalla tasolla Kymenlaakson yrittäjien mielipiteen mukaan.



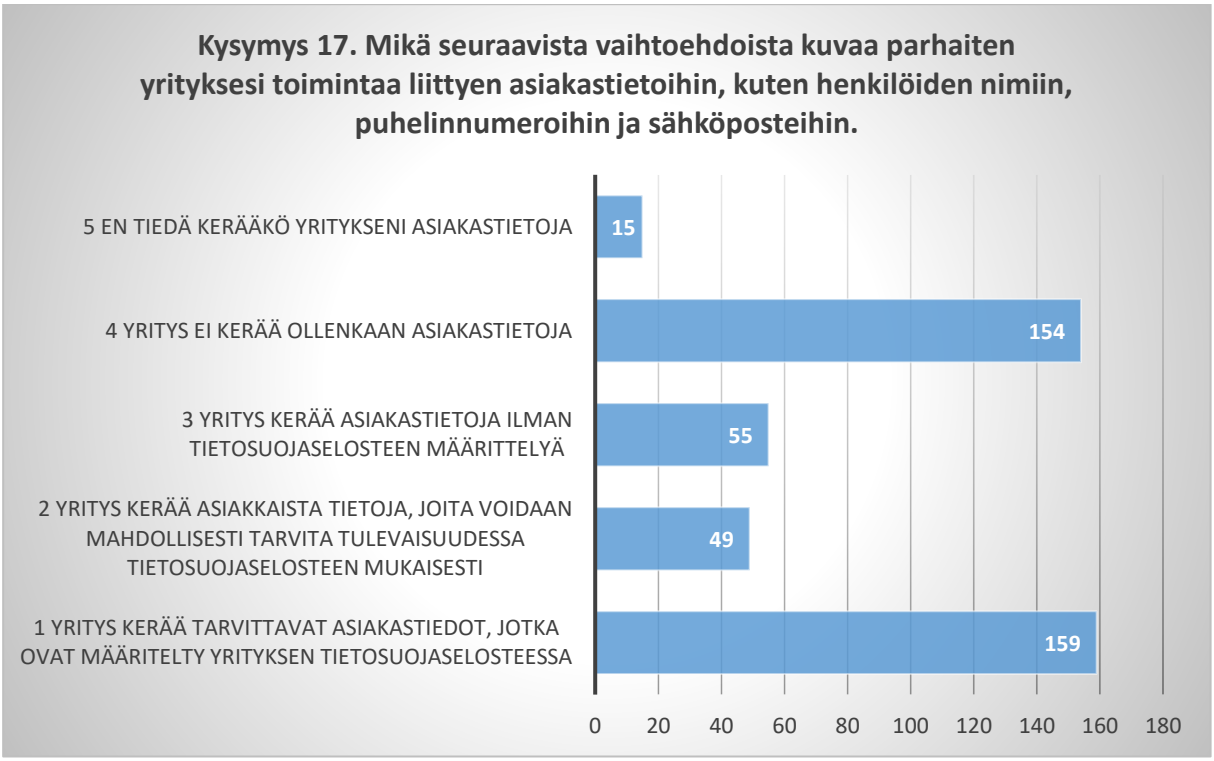
Kuva 14. Vastanneiden lukumäärät haastattelukysymykseen kolmetoista

Kysymys kolmeatoista voidaan suoraan vertailla kysymykseen seitsemän. Yrittäjiltä kysyttiin, onko yrityksessä konkreettisesti laadittu jatkuvuussuunnitelmaa, joka takaisi yritystoiminnan jatkumisen, vaikka kyseinen toiminta olisi uhattuna. 432 yrityksestä 297 (69 %) ei ollut luonut jatkuvuussuunnitelmaa ollenkaan. 82 (19 %) yritystä on luonut jatkuvuussuunnitelman, mutta sen ajankohtaisuus tai henkilökunnan tiedottaminen on ollut puutteellista. Vain 26 (6 %) yritystä oli luonut ajankohtaisen jatkuvuussuunnitelman ja tiedottanut siitä muuta henkilökuntaa. Jos kysymyksen kolmetoista neljättä vastausvaihtoehtoa vertaillaan kysymyksen seitsemän erittäin hyvin ja melko hyvin vastausvaihtoehtoihin saadaan seuraavat tulokset:



Kuva 15. Ristiintaulukointi kysymys seitsemässä olevan neljännen ja viidennen vastausvaihtoehdon sekä kysymyksen kolmetoista välillä

64 % yrityksistä, jotka vastasivat yrityksensä selviävän kyberhyökkäyksestä, joko erittäin hyvin tai melko hyvin, eivät ole luoneet yritykselleen jatkuvuussuunnitelmaa lainkaan. Erittäin hyvin vastausvaihtoehdon tapauksessa tämä tarkoittaa 48 yritystä ja melko hyvin vastausvaihtoehdon kohdalla sama lukema on 102 yritystä. Tuloksia voidaan selittää yrittäjien väärinkäsityksellä yrityksen varautumistoimiin. Jatkuvuussuunnitelma ei pidä sisällä pelkästään tietoteknisiä toimia, vaan se on koko yrityksen kokonaisvaltainen suunnitelma, joka takaa yrityksen toiminnan jatkuvuuden tilanteessa kuin tilanteessa. Tähän siis sisältyy myös esimerkiksi luonnonkatastrofit tai raaka-ainepulat. Jatkuvuussuunnitelman sisällyttäminen pelkästään kyber- ja tietoturvan aiheen alle on voinut luoda valheellisen kuvan jatkuvuussuunnitelman roolista yrityksessä. Tämän takia se voi olla helppo jättää huomiotta. Myös pienissä yrityksissä yrittäjä voi ajatella, että pienen kokonaisuuden hallitseminen ei tarvitse erillistä suunnitelmaa.



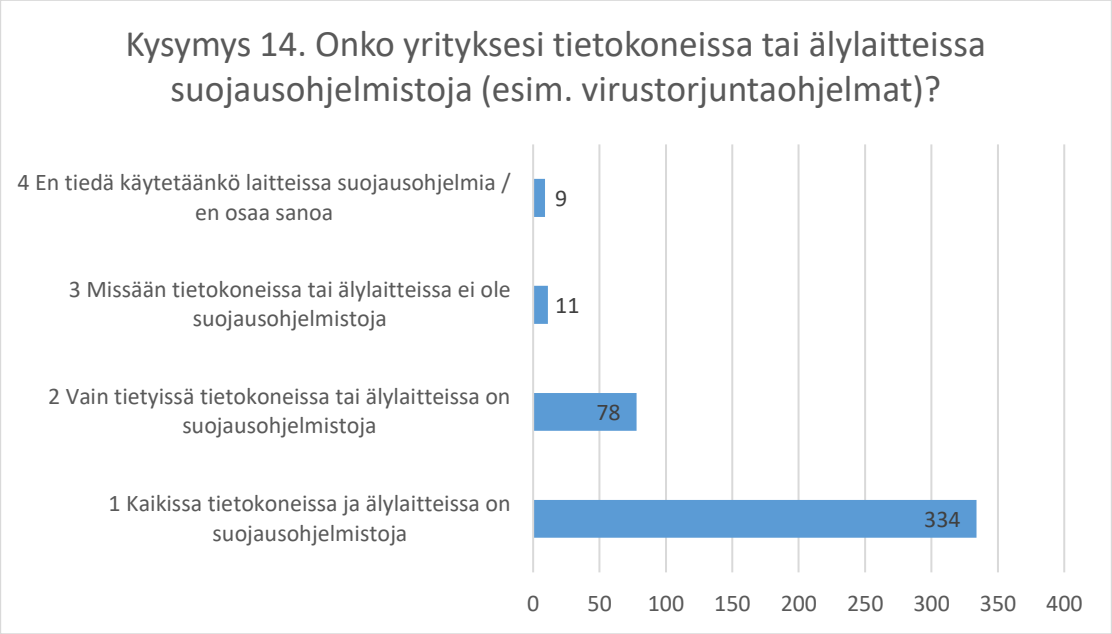
Kuva 16. Vastanneiden lukumäärät haastattelukysymykseen seitsemäntoista

Kyselyn viimeinen kysymys tiedusteli yrittäjiltä, kuinka heidän yrityksessään kerätään asiakastietoja. Tätä kysymystä voidaan ristiintaulukoida suoraan kysymyksen kolme kanssa. 432 yrityksestä 154 (36 %) ei kerää ollenkaan asiakastietoja. Vaikka on teoriassa mahdollista, että yritys pystyisi toimimaan ilman minkäänlaista kirjaa omista asiakkaistaan, on se teoriassa lähes mahdotonta, kun otetaan huomioon, mitä kaikkia tietoja yleinen tietosuoja-asetus määrittelee. Yleisen tietosuoja-asetuksen mukaan ”rekisterillä” tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu (tietosuoja-asetuksen 4 artikla). Vaikkakin artikla on vaikeasti selitettävä, Penttilä (2018) blogissaan avaa tähän rekisteriin kuuluvan seuraavat yrityksen henkilötietorekisterit:

- Yhteystiedot puhelimessa
- Asiakas- ja tilausrekisteri
- Excel-taulukko asiakkaiden yhteystiedoista
- Sähköpostiarkisto
- Lasku- ja kuittipinot
- Vieraskirja

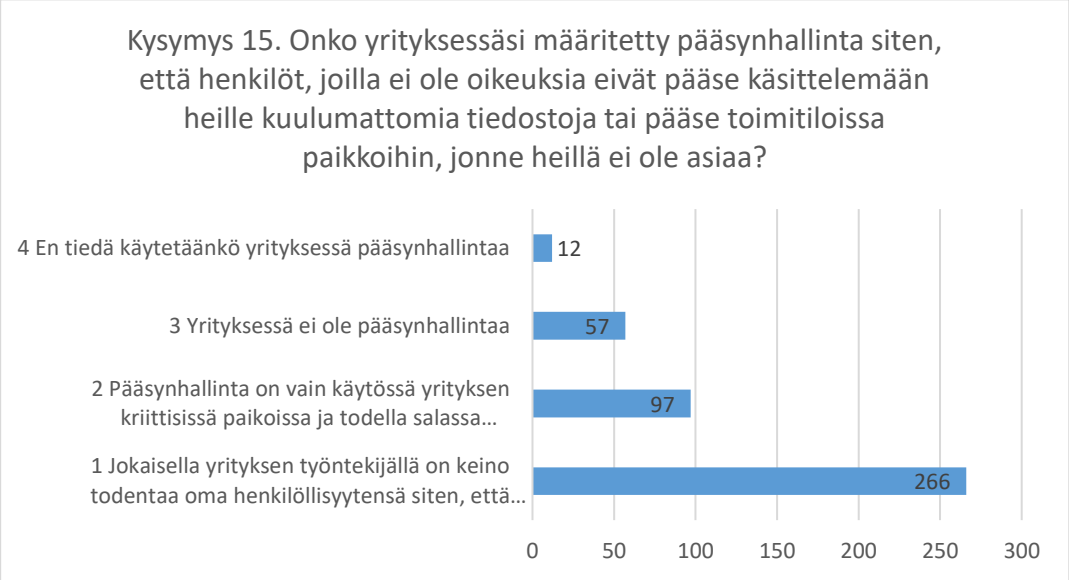
On vaikea kuvitella, että 36 % otannan yrityksistä ei keräisi mitään näistä edellä mainituista tiedoista tai tallentaisi niitä minnekään. 104 (24 %) yritystä

myös keräsi asiakastietoja, joko ilman tietosuojaselosteen määrittelyä tai keräsi senkaltaisia tietoja, joita ne uskovat tarvitsevansa tulevaisuudessa. Nämä rikkovat pääsääntöisesti yleisen tietosuoja-asetuksen artiklaa 5 (1) b) c) ja artiklaa 6 (1) a). Jos näiden artiklan rikkomisesta saatuja sakkoja tarkastellaan GDPR Enforcement Trackerin (s.a) avulla, voidaan huomata, että Suomessa pienin annettu sakko on 5 000 euroa ja suurin oli 608 000 euroa Psykoterapiakeskus Vastaamolle. Kysymykset kolme ja seitsemäntoista pystytään hyvin ristiintaulukoimaan niiden saman aihepiirin vuoksi ja samalla tuomaan esille yhteys verkkopalvelujen ja asiakastietojen käsittelyn osalta. 262 yrityksestä, joilla on jonkinlainen verkkopalvelu, 125 (48 %) yritystä kyselyn mukaan hoitaa asiakastietojen keräämisen tietosuoja-asetuksen mukaisesti. Kuitenkin 137 (51 %) verkkopalvelun omaavista yrityksistä käsittelee puutteellisesti asiakastietoja omassa yritystoiminnassaan. 169 yritystä ilmoitti, että heillä ei ole käytössään verkkopalveluja. Näistä yrityksistä 95 (56 %) ei kerää ollenkaan asiakastietoja ja vain 32 (19 %) yritystä hoiti asiakastietojen keräämisen tietosuoja-asetuksen mukaisesti.



Kuva 17. Vastanneiden lukumäärät haastattelukysymykseen neljätoista

Positiivinen huomio Kymenlaakson yrityksistä on aktiivinen suojausohjelmistojen käyttö. 432 yrityksestä 334 (77 %) yritystä on ottanut kaikissa älylaitteissa käyttöön suojausohjelmiston. Yrityksissä on hyvä ymmärrys laitteiden suojauksen tärkeydestä ja todella moni yritys on implementoinut niiden käyttöä laitteistoonsa.



Kuva 18. Vastanneiden lukumäärät haastattelukysymykseen viisitoista

Myös kysymys viisitoista osoittaa yrittäjien ymmärtävän tietojen ja tilojen hallinnan tärkeyden. 432 yrityksestä 266 (62 %) yritystä on luonut henkilökunnalle keinot todentaa oma henkilöllisyytensä ja sitä kautta päästä vain heille tarkoitettuihin tietoihin tai tiloihin käsiksi. 97 (23 %) yritystä on implementoinut sen vain yrityksen kriittisiin tietoihin tai tiloihin. Tiedostojen ja tilojen pääsynhallinta on hyvä keino ehkäistä ulkoisia hyökkäyksiä ja minimoida mahdollisten hyökkäysten vahingot.

9 JOHTOPÄÄTÖKSET

Kun tutkimuksen teoreettinen ja aineistoanalyyttinen osuus on saatu suoritettua, voidaan tuloksia tarkastella kriittisesti ja vetää siitä tarvittavat johtopäätökset. Luku muotoutuu kronologisesti tutkimuskysymysten mukaan, jotta saadaan tutkimuksen tutkimusongelmalle vastaus. Tutkimuksen tutkimusongelman oli, *tietävätkö Kymenlaakson yrittäjät oikeasti mitä kaikkea heidän yrityksensä kyberturvaan liittyy?* Tavoitteena on siis saada selko yrittäjien ymmärryksestä nimenomaisesti kyberturvaan liittyvistä osa-alueista ja kuinka se näkyy heidän yritystoiminnassaan.

Ihminen uhan alla

Osana opinnäytetyötä kartoitettiin mahdollisia kyberturvauhkia yrityksiä kohtaan. Nämä uhat otettiin huomioon myös kyselyn luomisessa ja tasotaulukon pisteytyksessä. Vaikka kyberturvan saralla usein puhutaan usein teknisistä soveltuvuuksista, ovat ne marginaalisesti varsin pieni uhka, kun niitä verrataan huijauksiin, kalasteluihin ja yleisesti ottaen sosiaalisen manipulointiin. Yrittäjien suurimat uhat liittyvät nimenomaisesti ihmisen luontaisiin heikkouksiin sosiaalisen manipulointiin liittyen. Tämän pohjalta myös luotiin opinnäytetyössä tehty kysely, jossa yrityksiltä tiedusteltiin niitä peruskeinoja, joilla sosiaalisen manipuloinnin voi huomata ja torjua.

Pienempien yritysten suuriksi uhiksi nousi huijausten, kalastelujen ja sosiaalisen manipuloinnin lisäksi myös yrityksiä kaatavat haittaohjelmat, joista yleisin on kiristyshaittaohjelmat. Kiristyshaittaohjelmat kylvävät tuhoa varsinkin huonosti valmistautuneisiin yrityksiin. Ilman oikeanlaisia suunnitelmia ja koulutuksia, voi yhden laitteen saastuminen nopeasti levitä koko yritysverkkoon ja tuhota yritystoiminnan päiviksi, viikoiksi ellei jopa kuukausiksi. Kalastelut ja sosiaalisen manipuloinnin keinot ovat rikollisten käyttämä pääsääntöinen keino saada yritys saastutettua, johtuen usein sen helppoudesta. Tämän takia huijaukset, kalastelut ja sosiaalinen manipulointi on yrityksille suurin kyber- ja tietoturvauhka marginaalisesti.

Tilanteen kartoittamiseksi tarvitaan luovia keinoja

Suomessa luodaan paljon kyselyitä, joihin ihmiset vastaavat parhaalla näkemällään tavalla. Tämä ei ollut opinnäytetyön tutkimusongelman kannalta optimaalista, kun halutaan kartoittaa yrittäjien tietoutta oman yrityksensä kyber- ja tietoturvasta. Kysymällä vain yksinkertaisesti yrittäjiltä heidän yrityksensä kyber- ja tietoturvan tilannetta saadaan suurella todennäköisyydellä se vastaus, jonka yrittäjä mieltää kyber- ja tietoturvaksi. Ongelmaa ei olisi, jos kaikki yrittäjät tietäisivät tasan tarkkaan, mitä näihin termeihin sisältyy ja kuinka ne voidaan toteuttaa. Kuitenkin kuten opinnäytetyössä saatiin selville, tämä ei ikävä kyllä ole tilanne.

Tutkimusongelmaan vastauksen saaminen vaati luovia keinoja, joilla pyrittiin tarkistamaan mahdollinen yrittäjien epätietoisuus kyber- ja tietoturvaan suhteen. Koska kyselystä saatiin vertailumuotoinen kahden eri osion välillä, loi tämä hyvän mahdollisuuden vertailulle yrittäjien kyber- ja tietoturvatietoisuuden sekä konkreettisten turvatoimien välillä.

Eroavaisuus mielipiteen ja konkretian välillä

Kyselystä saadun datan perusteella voidaan todeta, että Kymenlaakson yritysten kyber- ja tietoturvan sisältöä ei ole tiedotettu tarpeeksi yrittäjille. Vakavimmillaan ero mielipiteiden ja konkreettisten toimien välillä nähdään joka kolmannessa otannan yrityksessä. Tähän kun ottaa huomioon vielä lievimmän eroavaisuuden muodon (0,5–1,0), kattavat ne yhteensä yli puolet otannan yrityksistä. Tutkimustulosten avulla voidaan tuoda esille kyber- ja tietoturvan koulutuksen tärkeyttä ja tietoisuuden lisäämisen painoarvoa. Parantamalla yksittäisten yritysten ja toivottavasti samalla myös yksilöiden digitaalista turvallisuutta, voidaan myös parantaa maakunnan valmiutta mahdollisiin uhkiin.

Tulokset myös tuovat esille Kymenlaakson alueella toimivien digitaalista turvallisuutta parantavien hankkeiden tärkeyttä ja siihen tarvittavaa rahoitusta. Vaikkakin valtio tuottaa kyber- ja tietoturvapalveluita yrityksille ja yksilöille, jäävät pienemmät yritykset valitettavan usein ilman huomiota. Hanketoiminta on usein ainoa keino, millä tietoisuutta voidaan lisätä yksin-, mikro- ja pienyrittäjille Kymenlaakson kaltaisissa maakunnissa.

Vaikkakin kyselyn pääsääntöinen tarkoitus on osoittaa eroavaisuudet mielipiteen ja konkreettisten tekojen välillä, saatiin kyselystä irti myös paljon hyviä nostoja Kymenlaakson yrityksistä. Suuriksi kipupisteiksi muodostui suunnitelmien ja selosteiden puuttuminen, varsinkin asiakastietoihin liittyvät seikat tuottivat useille yrityksille haasteita. GDPR:ään liittyvät sakot yleistyvät hälyttävää tahtia Euroopassa, jonka takia aiheeseen liittyvää koulutusta pitää lisätä Kymenlaakson alueella. Myös jatkuvuussuunnitelmien puuttuminen yrityksissä kasvattaa riskiä pitkäaikaisiin katkoksiin yritystoiminnassa. Kuitenkin yrityslaitteiden yleinen koventaminen oli hyvällä tasolla yrityskoosta riippumatta.

Tilanne

Kun koko tutkimusta tarkastellaan kokonaisuudessa ja tutkimuskysymyksiin on saatu vastaus, voidaan tutkimusongelmaan vastata tyhjentävästi. Kyber- ja tietoturvatilanne Kymenlaakson yrittäjien keskuudessa on osittain huolestuttava ja isoille parannuksille on tarvetta. Kuitenkin yrittäjät ovat osoittaneet myös kiinnostuksensa ja halun parantaa yritystensä turvallisuutta. Tämä käy ilmi aktiivisella pääsynhallinnan valvomisella, laitesuojaamisella ja yleisesti ottaen henkilökunnan tiedottamisella. Kuitenkin otannasta saadut eroavaisuudet yrittäjien mielipiteen ja konkreettisten toimien välillä luo huolestuttavan uhkakuvan maakunnan mahdollisesta tilanteesta. Esimerkkinä on tietosuojan ja asiakastietojen tuomat vaikeudet yrittäjille. Myös yritysten riskin kartoitus ja sitä kautta saatava jatkuvuussuunnitelma vaatii tiedottamista ja mahdollisia koulutuksia, jotta niiden käyttöönottoa voidaan lisätä yrityksissä.

Mahdolliset syyt tuloksista saaduille eroavaisuuksille on hankala määrittää ja tämän tutkimuksen tutkimusaiheen ulkopuolella. Kuitenkin mahdollisten syiden miettiminen on kannattavaa, jos ongelmaan halutaan miettiä ratkaisua. Alle on listattu mahdollisia syitä eroavaisuuksille.

1. Yrittäjät eivät ole nähneet hyödyllisenä perehtyä kyberturvaan, koska eivät usko yrityksensä joutuvan kyberhyökkäyksen kohteeksi.
2. Yrittäjiä ei ole perehdytetty kyber- ja tietoturvan terminologiaan.
3. Ongelmien tiedostaminen voi luoda edellytykset niiden korjaamiselle. Yrityksen kyber- ja tietoturva puutteiden korjaaminen voidaan nähdä uhkaavana ja kalliina kulueränä, joka on vain useimmiten helpompi ohittaa.

Lisäämällä kyber- ja tietoturvan terminologiaa yleisessä puheessa sekä ottamalla aihe kunta- sekä koulutustasolla paremmin esille, voidaan parantaa aiheen ymmärrettävyyttä. Myös aiheen kansantajuistamisella on suuri rooli ongelmien ratkaisemisessa.

Otannasta saadut tulokset tuovat esille useita eri epäkohtia yritysten kyber- ja tietoturvatoimissa, joiden korjaamatta jättäminen voi tuoda haasteita lakitasolla ja yleisessä maakunnan vikasietoisuudessa. Tuomalla nämä epäkohdat esille voidaan ongelmaan heijastaa valoa ja sitä kautta pyrkiä korjaustoimenpiteisiin. Digiturvaan liittyvän tietoisuuden lisääminen maakunnassa on pitkä ja työläs prosessi, joka vaatii aikaa ja resursseja. Kuitenkin näkökulmasta riippuen voidaan väittää, että yrittäjien kyberturvan tietoisuus Kymenlaaksossa ei

ole läheskään niin huono kuin voidaan olettaa. Puolet otannan yrityksistä eivät rikkoneet raportoitavan eroavaisuuden rajaa. Vaikka rajaa ei rikottu, ei se kuitenkaan tarkoita, että tilanne olisi yrityksessä ollut hyvä. Se kuitenkin tuo esille aiheen ymmärtämisen ja sen tiedostamisen.

10 POHDINTA

Tässä luvussa käydään läpi opinnäytetyön pohdinta. Luvussa käsitellään tutkimuksen toteutusta, tarkastellaan haasteita ja ongelmia, joita opinnäytetyössä ilmeni. Lisäksi tarkastellaan mahdollisia jatkotutkimusaiheita, joita tutkimuksen pohjalta voidaan luoda tai jalostaa.

Toteutus ja haasteet

Tutkimuksen eteneminen oli aikataulullisesti vaihtelevaa. Kun tarkastellaan opinnäytetyön suorittamista sen aiheen valinnan ja valmistumisen välillä, ylittää työn valmistuminen vuoden aikajanan aika merkittävästi. Tähän on useita eri syitä:

1. Työn tutkimusotteen vaihtuminen
2. Tutkimussuunnitelman muutokset
3. Työn siirtyminen uuden kyberturvahankkeen piiriin
4. Puhelinhaastatteluiden tekijän kilpailutus ja haastatteluiden valmistuminen

Syyt aikataulumuutoksiin selittyvät opinnäytetyön tekijän ensikertalaisuuden takia varsinkin määrällisen tutkimuksen suhteen. Myös ensikertalaisuus kyselyn luonti ja hankeympäristössä toimiminen toivat aikataulullisia haasteita opinnäytetyön kulkuun. Aineiston keruuseen ja analyysiin merkityt toimet pysyivät koko opinnäytetyön ajan samana ja niihin pystyttiin palaamaan aina kun työ eteni. Opinnäytetyötä kirjoitettiin järjestyksellisesti aloittaen uhista ja luomalla hyvät käytännöt yrityksille, joilla näitä uhkia pääsääntöisesti torjutaan. Ilman näitä esitetietoja ei olisi aineiston keruulle ja analyysille tärkeiden kyselyn ja tasotaulukon tekeminen ollut mahdollista. Koska työ tehtiin pääsääntöisesti hankkeelle, tuli reliabiliteettia sekä validiteettia myös noudattaa tarkasti, jotta saatiin ylläpidettyä mahdolliset jatkotutkimusaiheet.

Koko opinnäytetyön pääpaino oli kyselyn suunnittelussa ja toteuttamisessa, ja sen avulla saatiin otannallisesti merkittävä määrä eri yritysten vastauksia niiden kyber- ja tietoturvaansa liittyen. Koko kyselyn ulkoasu ja rakenne on myös yksityiskohtaisesti selitetty ja näytetty, jotta reliabiliteetti varmistuu. Haasteiksi

ja ongelmaksi muodostui kyselyn pitäminen mahdollisimman tiiviinä sekä otannan mahdollisimman suuri koko, jotta tulokset olisivat vertailtavissa koko Kymenlaaksoon. Nämä ongelmat saatiin ratkaistua, vaikkakin kyselyn tiiviyden takia kaikkia haluttuja aiheita ei saatu kysyttyä. Jotta kysely saatiin pidettyä mahdollisimman tiiviinä, täytyi osaa kysymyksistä karsia, jonka takia kysymyspatteristo jäi tiettyjen alueiden osalta suppeaksi. Tarkempi tiedustelu henkilökunnan koulutuksista ja yrityksen mahdollisista aikaisemmista kyberturva- ja tietoturvahäiriöstä sekä tiedustelu yritysten riskienhallinnasta olisi tuonut koko tutkimukseen enemmän syvyyttä ja antanut paremman kuvan Kymenlaakson sen hetkisestä tilanteesta.

Jatkotutkimus

Jatkotutkimusaiheita on useita ja opinnäytetyö on luotu nimenomaisesti tukemaan hankkeiden luomia selvityksiä. Ideat ovat syntyneet hanketoimijoiden ja muiden oppilaitosten tapaamisista. Mahdollisia aiheita:

1. **Suomen yritysten kyberturvatilanne:** samankaltainen tutkimuskaava, mutta huomattavasti suuremmalla otannalla, joka kattaisi koko Suomen yrityskannan
2. **Henkilökunnan käsitys yritysten kyber- ja tietoturvaan:** henkilökuntaan kohdistuva kysely, jolla tiedustellaan heidän mielipidettään yrityksen kyber- ja tietoturvaan
3. **Tarkempi kysely yksin- ja mikroyrityksille:** Tarkempi otanta, joka keskittyy nimenomaisesti yksin- ja mikroyritysten kyber- ja tietoturvatilanteeseen.

Työn aikana on luotu mahdollisuus luoda kysely uudestaan joka toinen vuosi. Kyselyssä olevien kysymysten avulla voidaan kartoittaa Kymenlaakson yritysten vastauksia kyber- ja tietoturvaan ja sitä kautta saada selville vuosien aikainen kehitys. Tämä vaatisi aktiivisen hanketoimijan, joka pystyisi rahoituksen avulla luomaan samankaltaisen otannan kyselylle. Tämäntyyppisen kyselyn uudelleen luominen kuitenkin tuottaa useita haasteita, kun otetaan huomioon hankerahoitukset ja niiden mahdolliset määräajat. Kymenlaakson alueella on harvinaista, jos hanke saa toimia yli kaksi vuotta pidempään, minkä takia kyselyn ylläpitäminen vaatisi useita hankkeita toimiakseen.

LÄHTEET

America's Cyber Defense Agency. 2021. What is Cybersecurity?. WWW-dokumentti. Saatavissa: What is Cybersecurity? | CISA [viitattu 25.1.2024].

Blackfog. 2023. The State of Ransomware in 2023. WWW-dokumentti. Saatavissa: https://www.blackfog.com/the-state-of-ransomware-in-2023/ [viitattu 14.7.2023].

CIS & CTI. 2023. Top 10 Malware Q1 2023. Center for Internet Security (CIS). WWW-dokumentti. Saatavissa: https://www.cisecurity.org/insights/blog/top-10-malware-q1-2023 [viitattu 1.12.2023].

Digital Innovation Hub DIH Kymenlaakso -hanke. 2022. Kymenlaakson pk-yritysten digitalisaatiotarpeet. PDF-dokumentti. Saatavissa: Kymenlaakson pk-yrityksien digitalisaatiotarpeet (2).pdf [viitattu 11.10.2023].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.

GDPR Enforcement Tracker. s.a. Fines Database. WWW-dokumentti. Saatavissa: https://www.enforcementtracker.com/ [viitattu 27.3.2024].

Guim, T. 2021. Cost of Cyber Attacks vs. Cost of Cyber Security in 2021. pchtechnologies. WWW-dokumentti Saatavissa: https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/ [viitattu 11.3.2024].

Holopainen, M. & Pulkkinen, P. 2008. Tilastolliset menetelmät. 5.–6. painos. Helsinki: WSOY. [viitattu 5.8.2023].

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. painos. Helsinki: Tammi.

Helsinki Region Chamber of Commerce. 2019. Yrityksiin kohdistuvat kyberuhat 2019. PDF-dokumentti. Saatavissa: https://helsinki.chamber.fi/wp-content/uploads/sites/2/2020/01/yrityksiin-kohdistuvat-kyberuhat-2019.pdf [viitattu 20.10.2023].

Insurance Bureau of Canada. 2023. Small businesses are underestimating their cyber risk despite increased threats. WWW-dokumentti. Saatavissa: https://www.ibc.ca/news-insights/news/small-businesses-are-underestimating-their-cyber-risk-despite-increased-threats [viitattu 27.3.2024].

Jyväskylän yliopisto. 2022. Kyberhyökkäysten määrä kasvaa vuosittain – yritysten osaamisessa ja varautumisessa suurta vaihtelua. Jyväskylän yliopisto. Verkkolehti. Saatavissa: https://www.jyu.fi/fi/uutinen/kyberhyokkaysten-maara-kasvaa-vuosittain-yritysten-osaamisessa-ja-varautumisessa-suurta-vaihtelua [viitattu 19.3.2023].

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä. Jyväskylän ammattikorkeakoulu. [viitattu 23.5.2023].

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä. Jyväskylän ammattikorkeakoulu. [viitattu 27.4.2023].

Kananen, J. 2019. Opinnäytetyön ja pro gradun pikaopas: Avain opinnäytetyön ja pro gradun kirjoittamiseen. Jyväskylä. Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.225239 [viitattu 4.3.2023].

Kaakkois-Suomen Ammattikorkeakoulu. 2022. Kyberturvan ABC yrittäjille. Saatavissa: https://www.xamk.fi/tutkimus-ja-kehitys/kyberturvallisuuden-abc-yrittajille/ [viitattu 18.5.2023].

Koppa. 2021. Määrällinen analyysi. Jyväskylän yliopisto. WWW-dokumentti. Päivitetty 28.10.2021. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/maarallinen-analyysi [Viitattu 19.5.2023].

Kymenlaakso Ennakoi. 2022. Aluetalous ja yritykset. Kymenlaakso Ennakoi. Verkkoartikkeli. Saatavissa: https://ennakointi.kymenlaakso.fi/tilastot-ja-ennusteet/aluetalous [viitattu 29.03.2023].

Limnell, A. 2023. Ajankohtainen katsaus kyberrikollisuuteen. KRP Kyberrikostorjuntakeskus. WWW-dokumentti. Saatavissa: https://poliisi.fi/blogi/-/blogs/ajankohtainen-katsaus-kyberrikollisuuteen- [viitattu 25.1.2024].

Rajamäki M, 2022. Kyberturvallisuustilanne – miten yritysten tulee varautua. Elinkeinoelämän Keskusliitto. PDF-dokumentti. Julkaistu 27.04.2022. Saatavissa: https://kymenlaaksonkauppakamari.fi/assets/Uploads/Kyberturvallisuustilanne-Rajamaki-27042022.pdf [viitattu 18.5.2023].

McKenzie, T. 2017. Is Cyber Deterrence Possible? Air Force Research Institute. PDF-dokumentti. Saatavissa: https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF [viitattu 7.9.2023].

Moschovitis, C. 2018. Cybersecurity Program Development for Business : The Essential Planning Guide. New Jersey. John Wiley & Sons. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.4100000001115675?sid=3030372265 [viitattu 5.8.2023].

Mattila, J., Ali-Yrkkö, J & Seppälä, T. 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?. ETLA Muistio No 93. Artikkeli. Saatavissa: https://www.etla.fi/wp-content/uploads/ETLA-Muistio-Brief-93.pdf [viitattu 1.4.2023].

Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J & Tervo, E. 2020. Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Etlatieto Oy. PDF-dokumentti. Saatavissa: https://www.etla.fi/wp-content/uploads/digibarometri_2020.pdf [viitattu 4.6.2023].

NIST. 2018. The National Institute of Standards and Technology. U.S. Department of Commerce. Cybersecurity framework. PDF-dokumentti. Saatavissa:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [viitattu 8.4.2024].

Penttilä, E. 2018. Tietosuoja-asetus selkokielellä. Verkkokauppablogi.fi. Blogi. Päivitetty 7.4.2018. Saatavissa: https://www.verkkokauppablogi.fi/tietosuoja-asetus-selkokielella/ [viitattu 27.3.2024].

Poliisi. 2023. Varo, varmista, varoita: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla. WWW-dokumentti. Saatavissa: https://poliisi.fi/-/varo-varmista-varoita-digihuijausten-maara-kasvoi-selvasti-vuoden-2022-jalki-puoliskolla [viitattu 14.6.2023].

Saaranen-Kauppinen, A & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto: Operationalisointi. Tampere: Yhteiskuntatieteellinen tietoarkisto. WWW-dokumentti Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_3_2_2.html [viitattu 12.2.2024].

Scribbr. 2016. Opinnäytetyön rakenne: Miten Kirjoittaa Opinnäytetyön Teoreettinen Viitekehys? WWW-dokumentti. Saatavissa: https://www.scribbr.fi/opinnaytetyon-rakenne/opinnaytetyon-teoreettinen-viitekehys-mita-ja-miksi/ [viitattu 26.1.2024].

Statista. (2021). Number of denial-of-service (DoS) attacks in Finland from 2017 to 2020, by length. Statista. Statista Inc.. Saatavissa: https://www.statista.com/statistics/1224617/number-of-dos-attacks-by-length-finland/ [viitattu 20.10.2023].

Sisäministeriö. s.a. Kyberrikollisuus ylittää rajat tietoverkoissa. WWW-dokumentti. Saatavissa: https://intermin.fi/poliisiasiat/kyberrikollisuus [viitattu 31.1.2024].

Tietoarkisto. s.a. Otos ja otantamenetelmät. WWW-dokumetti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/otos/otantamenetelmat/ [viitattu 17.5.2023].

Tilastokeskus. s.a. Pienet ja keskisuuret yritykset. WWW-dokumentti. Saatavissa: https://www.stat.fi/meta/kas/pienet_ja_keski.html [viitattu 11.3.2024].

Tilastokeskus. 2022. Yritykset henkilöstön suuruusluokan mukaan 2022. WWW-dokumentti. Päivitetty 19.12.2023. Saatavissa: https://www.tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html [viitattu 11.3.2024].

Traficom. 2020a. Pienyritysten kyberturvallisuusopas. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf [viitattu 5.8.2023].

Traficom. 2020b. Kyberturvallisuus ja yrityksen hallituksen vastuu. PDF-dokumentti. Saatavissa: T_KyberHV_digiAUK_220120.pdf (kyberturvallisuuskeskus.fi) [viitattu 25.1.2024].

Traficom. 2021. Tietoturvan vuosi 2020: Kyberturvallisuuskeskuksen vuosikatsaus. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2020_210212_FIN.pdf

[viitattu 1.12.2023].

Traficom. 2022a. Kyberympäristön uhkataso on noussut - aktiviteetti Suomeakin kohtaan on lisääntynyt. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt [viitattu 9.6.2023].

Traficom. 2022b. Palvelunestohyökkäykset ovat arkipäivää Suomessa. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa [viitattu 14.7.2023].

Traficom. 2022c. Toimintaohje – Palvelunestohyökkäys. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf [viitattu 1.12.2023].

Traficom. 2023. Traficom ja teleoperaattorit yhteisrintamassa kansainvälisiä huijaussoittoja vastaan. WWW-dokumentti. Saatavissa: https://uutiskirje.traficom.fi/etusivu/luottamus-ja-toimintavarmuus/traficom-ja-teleoperaattorit-yhteisrintamassa-kansainvalisia-huijaussoittoja-vastaan.html [viitattu 14.6.2023].

Vilkka, H. 2021. Tutki ja kehitä. Jyväskylä: PS-kustannus. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.227023?sid=2959521564 [viitattu 17.5.2023].

KUVALUETTELO

TAULUKKOLUETTELO

Taulukko 6. Muu ryhmien sisällöt Excel taulukossa