Opinnäytetyö (AMK)

Myyntityön koulutus, finanssipalvelut

2024

Otto Räsänen

Kyberturvallisuus osana pienyrityksen riskienhallintaa

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Myyntityön koulutus | Finanssipalvelut

2024 | 58 sivua

Otto Räsänen

Kyberturvallisuus osana pienyrityksen riskienhallinta

Digitaalisten palvelujen lisääntymisen sekä tekoälyn kehityksen myötä ovat myös yrityksiin kohdistuneet kyberhyökkäykset lisääntyneet valtavasti viime vuosien aikana. Erityisesti pienyrityksissä kyberhyökkäyksen aiheuttamat vahingot voivat muodostua kriittisiksi liiketoiminnan jatkuvuuden kannalta. Kyberturvallisuuden integroiminen osaksi yrityksen riskienhallintaa on nyt ajankohtaisempaa kuin koskaan.

Opinnäytetyön teoreettinen viitekehys muodostuu riskienhallinnan, tietoturvan sekä kyberturvallisuuden ympärille, jonka tarkoituksena on tukea toteutettua tutkimustyötä sekä siinä esitettyjä tuloksia ja havaintoja.

Tutkimustyön tavoitteena oli selvittää pienyritysten kyberturvallisuuden nykytilaa ja sitä, miten kyberturvallisuus on huomioitu osana yrityksen riskienhallinnan strategiaa. Työ tehtiin toimeksiantona vakuutusyhtiölle ja tutkimuksen kohteena oli toimeksiantajan alle 10 henkilö työllistävät yritysasiakkaat. Työssä toteutettiin kvantitatiivinen tutkimustyö, jossa kohderyhmälle lähetettiin kyberturvallisuuden hallintaan liittyvä kyselylomake.

Tulosten mukaan noin joka kolmas vastaajista oli kohdannut liiketoiminnassaan kyberhyökkäyksiä. Vastaajat kokivat kuitenkin kyberuhkien olevan hyvin neutraali riski yrityksen liiketoiminnan jatkuvuuden varmistamisen näkökulmasta. Kyberturvallisuusstrategian integroiminen osaksi yrityksen riskienhallintaa oli myös tulosten perusteella vielä hyvin alhaisella tasolla.

Asiasanat:

Kyberturvallisuus, Tietoturva, Riskienhallinta, Pienyritykset

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Bachelor Degree of Business Administration | Financial Services

2024 | 58 pages

Otto Räsänen

Cyber security as part of risk management in small businesses

With the growth in digital services and the development of artificial intelligence, cyber-attacks against businesses have also increased dramatically in recent years. For small businesses in particular, the damage caused by a cyber-attack can become critical to business continuity. Integrating cyber security into company´s risk management is now more relevant than ever.

The theoretical framework of the thesis is formed around risk management, information security and cyber security, which is intended to support the research work carried out and the results and findings presented in it.

The aim of the research was to investigate the current state of cyber security in small businesses and how cyber security is considered as part of the company´s risk management strategy. The study was commissioned by an insurance company and focused on its corporate clients with less than 10 employees. The study was a quantitative research project, in which a survey on cyber security management was sent to the target group.

According to the results, around one in three respondents had experienced cyber-attacks in their business. However, respondents felt that cyber threats were a very neutral risk in term of ensuring business continuity. The integration of cyber security strategy into the risk management of the company was also found to be at a very low level.

Keywords:

Cyber security, Information security, Risk management, Small businesses

Sisältö

Kuvat

Kuviot

Taulukot

Käytetyt lyhenteet tai sanasto

CIA	Tietoturvan käytäntö. Käännetty englanninkielisistä sanoista: confidentality, integrity, availability.
DDoS	Hajautettu palvelunestohyökkäys. Käännetty englanninkielisestä sanasta: Distributed Denial of Service.
DoS	Palvelunestohyökkäys. Käännetty englanninkielisestä sanasta: Denial-of-Service.
NIST	Yhdysvaltalainen standardointi- ja teknologiainstituutti.

1 Johdanto

Asiakas- ja kumppanuussuhteet perustuvat pohjimmiltaan luottamuksen varaan. Organisaatioiden tietoturva ja kyberturvallisuus muodostuvat sen hallussa olevasta datasta ja siitä, miten sitä käytetään ja suojataan. Digitaalisten palvelujen lisääntymisen myötä myös enenevissä määrin kasvaneet kyberriskit voivat kuitenkin tuhota hetkessä organisaation maineen, jos sen kyberstrategia ja prosessit eivät ole riittävän tehokkaita. Jos luottamus katoaa organisaatiota kohtaan, katoavat tältä myös nopeasti asiakkaat. Tanskalainen pienyritys Cloudnordic antaa varoittavan esimerkin siitä, jos tietoturvaa kohtaan ei ohjata riittävästi resursseja. Pilvipalveluja tuottava Cloudnordic joutui elokuussa 2023 kyberhyökkäyksen kohteeksi, jonka seurauksen kaikki yrityksen palvelinten tiedot oli onnistuttu salaamaan ja tämän seurauksena asiakastiedot oli menetetty lopullisesti. Cloudnordic ei ollut kykenevä jatkamaan enää tämän jälkeen liiketoimintaansa ja sen olemassaolo yrityksenä päättyi. (Kauppalehti 2023.)

Kyberturvallisuuden opinnäytetyö toteutetaan toimeksiantona vakuutusyhtiölle, jossa myös itse työskentelen pienyritysasiakkaiden parissa. Tutkimusongelmaksi nousi esiin toimeksiantajan pienyritysasiakkaiden kyberturvallisuuden nykytilanne ja miten se on otettu osaksi yrityksen kokonaisvaltaista riskienhallintaa. Etlan (2020, 8) muistiossa todetaan, että alle 10 henkilöä työllistävien kotimaisten yritysten kyberturvallisuudesta on heikosti tilastoja saatavilla. Muistiossa nostetaan myös esiin huolestuttava havainto, jonka mukaan kyberuhan realisoituminen voi aiheuttaa esimerkiksi uudelle kasvuyritykselle liiketoiminnan päättymisen.

Opinnäytetyön aihetta voidaan pitää ajankohtaisena organisaatioille muun muassa digitaalisten palvelujen lisääntymisen ja tekoälyn kehittymisen myötä. Myös tuoreimmat tutkimustulokset ja käsiteltävään aiheeseen liittyvät artikkelit viittaavat kyberuhkien ajankohtaisuuden puolesta. Elisan teettämän tutkimuksen mukaan 71 prosenttia suomalaisista organisaatioista on vauhdittanut varautumistaan kyberhyökkäyksiin. Keskisuurista yrityksistä jo puolet arvioivat tietomurtojen ja kiristyshaittaohjelmien määrän kasvaneen viimeisen vuoden aikana. (Kauppalehti 2023.) Kunnallisalan kehittämissäätiön (Kaks) teettämän kyselyn mukaan jopa 82 prosenttia suomalaisista pitävät kyberhyökkäyksiä ja tietomurtoja lähitulevaisuudessa erittäin tai melko vakavana uhkana. (Yle 2023.)

Tämän opinnäytetyön tavoitteena on tuoda esiin toimeksiantajan yritysasiakkaiden näkökulma kyberturvallisuudesta osana organisaation riskienhallintaa. Opinnäytetyön tutkimuskysymykseksi on nostettu: ”Miten yrityksen kyberuhkiin on varauduttu liiketoiminnan jatkuvuuden kannalta?” Opinnäytetyössä käsitellään aluksi aihepiirin liittyvä teoriaosuus, jota sovelletaan myöhemmin opinnäytetyön tutkimusosiossa. Tieto- ja kyberturvaan liittyvissä asioissa hyödynnän tieteellisiä artikkeleita, Traficom Kyberturvallisuuskeskusta, alan kirjallisuutta, sekä tuoreimpia uutisia.

Työssä kuvataan sitä, miksi kyber- ja tietoturvallisuus ovat edellytyksiä yrityksen kilpailukyvyn ja liiketoiminnan jatkuvuuden kannalta, mitkä ovat yleisimpiä kyberuhkia yritykselle sekä millä eri keinoin yritys voi turvata liiketoimintaansa kyberhyökkäyksiltä, erilaisten riskienhallintamenetelmien avulla. Tämän jälkeen syvennytään tutkimaan kyber- ja tietotuvallisuutta yritysten näkökulmasta. Opinnäytetyön tapaustutkimuksen tarkoituksena on selvittää kvantitatiivisten menetelmien avulla, ovatko lisääntyneet kyberturvallisuusriskit näkyneet yritysten liiketoiminnassa ja miten niihin on varauduttu. Tämän tutkimuksen avulla toimeksiantajan on helpompi ymmärtää asiakkaidensa tarpeita sekä mahdollisesti löytää uusia mahdollisuuksia ja uhkia.

2 Riskienhallinta

Riskit ovat yritysmaailmassa aina väistämätön asia, mutta laadukkaan riskienhallinnan avulla niitä voidaan kuitenkin hallita tehokkaasti. Riskienhallinnan avulla yritykset pyrkivät varautumaan riskeihin niin, että se on taloudellisesti kannattavaa. Riskienhallinnan kappaleessa käyn läpi mitä eri lähestymistapoja riskeihin varautumisessa on yleisesti käytetty, mihin riskianalyysi perustuu sekä miten riskien vakavuutta voidaan arvioida osana yrityksen riskienhallintaa.

2.1 Riskien käsittely

Yritykset kohtaavat liiketoiminnassaan merkittävän määrän erilaisia riskejä ja mahdollisuuksia. Riskien käsittelyn voi Shimpi (2001, 16) ja Juvonen ym. (2023, 33) mukaan jakaa pääsääntöisesti neljään eri vaihtoehtoon, jonka avulla yritykset voivat hakea tasapainon riskien ja mahdollisuuksien väliltä. Alla olevassa kuviossa 1 havainnollistetaan riskeihin varautumisen nelikenttää.

Kuvio 1. Riskeihin varautumisen nelikenttä mukaillen (Shimpi 2001, 16; Juvonen ym. 2023, 33).

Kuviosta 1 käy ilmi, että riskin välttäminen ja riskin vähentäminen linkittyvät riskin kontrollointiin, jossa riskin vaikutus pyritään minimoimaan. Riskin rahoittamiseen linkittyvät riskin siirto sekä riskin säilyttäminen. Riskin rahoittamisella pyritään kattamaan tappiota, jotka jäävät riskienhallinnan keinojen hyödyntämisen jälkeen. (Shimpi 2001, 16; Juvonen ym. 2023, 33.)

Riskin välttäminen

Shimpi (2001, 16–17) ja Juvonen ym. (2023, 33) toteaa, että yritykset voivat tietoisesti astua sivuun hankkeista, jotka ylittävät yrityksen riskinsietokyvyn, mutta liiallinen riskien välttäminen voi myös johtaa kilpailukyvyn heikkenemiseen ja etumatkan antamiseen kilpailijoille, joka itsessään myös asettaa omat riskinsä liiketoiminnan kannattavuuden ja jatkuvuuden ylläpitämiselle. Yrityksillä on useasti liiketoiminnassaan riskejä, joita se ei pysty kokonaan välttämään, vaan yrityksen tulee ymmärtää ja vähentää niitä parhaansa mukaan. Jotta yritys pystyisi kokonaan eliminoimaan riskin, tulisi riskin aiheuttajan syy pystyä poistamaan kokonaan.

Riskin vähentäminen

Shimpi (2001, 17–18) ja Juvonen ym. (2023, 33) mukaan yritykset pystyvät vähentämään riskiä kolmella eri tavalla, johon kuuluvat riskin ehkäiseminen, riskin hallitseminen sekä hajauttaminen. Riskien ehkäisemisellä pyritään vähentämään tunnistetun vahingon sattumisen todennäköisyyttä. Riskin hallitsemisen tarkoituksena on taas minimoida realisoituneen riskin haitallisuus. Hajauttamisen avulla pyritään varmistamaan toiminnan jatkuvuus, riskin realisoitumisen jälkeen. Riskiä pyritään vähentämään silloin, kun sen siirtäminen tai välttäminen ei ole mahdollista.

Riskin siirtäminen

Shimpi (2001, 18) ja Juvonen ym. (2023, 33) toteaa, että riskin siirtäminen toiselle osapuolelle voi olla yritykselle kannattava vaihtoehto, jos riskin realisoituminen aiheuttaisi yritykselle sietämättömän tilanteen. Yksi yleisesti käytössä oleva tapa riskin siirtämiselle on siirtää riski vakuutusyhtiölle, jossa yritys turvaa omaa liiketoimintaansa uhkaavia riskejä, vakuutusmaksuja vastaan. Tämä toimintatapa helpottaa riskienhallinnan budjetointia, koska vakuutusmaksu ja sen omavastuuosuus ovat ennalta määriteltyjä. Toinen yleisesti käytössä oleva riskien siirtämisen keino on siirtää vastuuta esimerkiksi asiakkaille ja toimittajille, jossa itse yritys ei kanna liian suurta vastuuta riskeistä.

Riskin säilyttäminen

Shimpi (2001, 19) ja Juvonen ym. (2023, 33) toteaa, että yritykset voivat tehdä päätöksen tiettyjen riskien säilyttämiselle, koska jossain tapauksissa se voi olla kustannustehokkain ratkaisu. Näiden riskien realisoitumisen todennäköisyys voi olla hyvin matala tai sen vaikutus ei aiheuta merkittävää haittaa. On myös yleistä, että yritykset kantavat tiedostamattaan tiettyjä riskejä. Yritykset voivat rahoittaa säilyttämiään riskejä esimerkiksi suoraan käyttöbudjetista tai erilaisten korvausrahastojen avulla.

2.2 Riskianalyysi

Riskianalyysin luomisen tarkoituksena on luokitella tunnistetut riskit niiden merkityksellisyyden mukaan ja arvioida sen perusteella, miten niihin tulisi reagoida. On syytä ottaa kuitenkin huomioon, että riskin merkityksellisyyttä arvioidessa, tulee se suhteuttaa yrityksen taloudellisen aseman kanssa. Heikon maksuvalmiuden omaava yritys ei todennäköisesti pysty juurikaan ottamaan vastaan merkittäviä uhkia, liiketoiminnan jatkuvuuden kannalta. Riskianalyysi toimii myös pohjana luvussa 2.1 läpikäydyn riskien käsittelyn määrittelyssä. (Wolke 2017, 15; Juvonen ym. 2023, 30.)

Jokaisen yrityksen kohtaamat riskit eroavat jossain määrin toisistaan, jonka puolesta riskien tunnistaminen ja arviointi tapahtuvat aina yrityskohtaisesti. Yrityksen tulee myös määrittää oma riskinsietokykynsä, ennen oman riskianalyysinsä suunnittelua. Riskianalyysiä ei voi myöskään tämän seurauksena yleistää, koska jokaisella yrityksellä on persoonallinen riskinottohalukkuutensa. (Wolke 2017, 74; Juvonen ym. 2023, 28.)

Riskianalyysin tavoiteltavana lopputuloksena voidaan pitää kehystä, jossa on kuvattu yrityksen tavoittelemat mahdollisuudet ja reagointia vaativat uhat. Riskienhallinnan keskiössä on hyödyntää riskianalyysiä niin, että mahdollisuuksien ja riskien välistä vaakakuppia pyritään kallistamaan enenemissä määrin mahdollisuuksien puolelle. (Merna & Al-Thani 2008, 51.)

Merma & Al-Thani (2008, 51) toteaa kirjassaan, että kaksi yleisintä tapaa analysoida riskejä ovat määrällinen- ja laadullinen analyysi. Laadullisessa riskianalyysissä ei hyödynnetä ollenkaan numeraalisia arvoja, vaan analyysin tarkoituksen on ymmärtää riskejä ja niiden seurausten vaikutusta. Määrällisessä riskianalyysissä luodaan analyysi tilastotietojen kautta saadun datan avulla.

2.3 Riskien vakavuuden arviointi

Yritykset voivat arvioida riskiensä vakavuutta hyödyntämällä riskimatriisia, jossa luokitellaan ja pisteytetään tunnistettuja riskejä, niiden kriittisyyden mukaan. Kriittisiä riskejä voi olla yritykselle esimerkiksi riskit, jotka liittyvät sen ydinliiketoimintaan, tietosuojan mukaisiin henkilötietoihin tai viranomaisvaatimuksiin. Yrityksen tulee myös kiinnittää erityistä huomiot riskeihin, jotka eivät ole välttämättä erityisen kriittisiä mutta niiden realisoitumisen todennäköisyys on verrattain korkea. (Pinto & Magpili 2015, 23.)

Yleisesti käytössä oleva tapa riskimatriisin pisteyttämiselle on kertoa riskin todennäköisyys sen vakavuudella. Alla olevassa kuvassa 1 havainnollistetaan riskimatriisin rakennetta.

		Consequence				
Likelihood of occurrence		**Negligible**	**Minor**	**Major**	**Significant**	**Catastrophic**
	Very likely					
	Likely					High
	Moderately possible	Low	Low medium	Medium	Medium high	
	Unlikely					
	Very unlikely					

Kuva 1. Riskimatriisi (Pinto & Magpili 2015, 24).

Riskimatriisi antaa suuntaviivat siihen, miten yrityksen tulisi priorisoida riskejä. Riskimatriisia hyödyntämällä yritys voi panostaa tarpeeksi resursseja sekä aikaa liiketoiminnan jatkuvuuden kannalta uhkaavimpien riskien hallitsemisen varalle. (Pinto & Magpili 2015, 24.)

Juvonen (2023, 31) tuo esiin riskienhallintaa käsittelevässä kirjassaan, miten riskin vakavuutta ja sen aiheuttamia mahdollisia jatkotoimenpiteitä voidaan luokitella. Alla olevassa taulukossa 1 havainnollistetaan riskin eri vakavuusasteet sekä mahdolliset jatkotoimenpiteet.

Taulukko 1. Riskin vakavuus ja tarvittavat jatkotoimenpiteet mukaillen (Juvonen ym. 2023, 31).

Riskin vakavuus	Jatkotoimenpiteet
Merkityksetön riski	Riskin realisoituminen ei aiheuta jatkotoimenpiteitä
Vähäinen riski	Ei aiheuta välittömiä toimenpiteitä, mutta riskin kehityskaarta tulee seurata
Kohtalainen riski	Toimenpiteet riskin vähentämiseksi tulee aloittaa, kuitenkin kannattavuus huomioiden
Merkittävä riski	Toimenpiteet riskin vähentämiseksi tulee aloittaa nopeasti, jonka aikana toiminta tulee minimoida ennen kuin riskiä on pystytty vähentämään
Sietämätön riski	Toimenpiteet riskin poistamiseen tai vähentämiseen tulee aloittaa välittömästi, jonka aikana riskialtis toiminta pitää keskeyttää

Taulukosta 1 voimme havaita, että vaikka kaikki riskit eivät välttämättä johdakaan aina jatkotoimenpiteisiin, niin silti mitä vakavampaan riskiin päin siirrytään, niin sitä epävarmemmaksi liiketoiminnan jatkuvuus muodostuu.

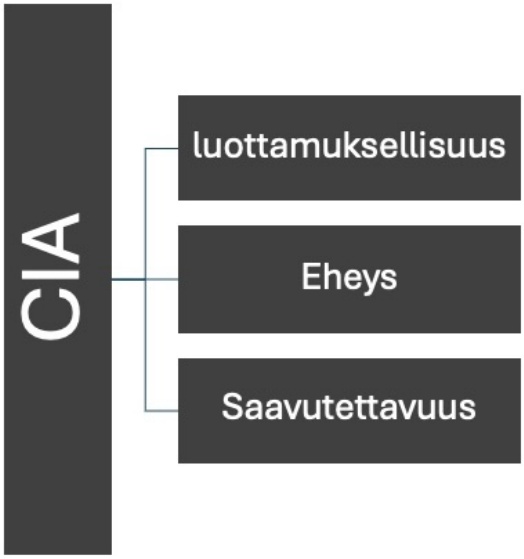
3 Tietoturva

Tietoturvan tarkoituksena on yrityksen toiminnan turvaaminen yrityksen omien tietojen oikeaoppisella suojaamisella. Toisin kuin tietosuojassa, yritykset saavat tietoturvan suhteen itse päättää miten he käsitellevät tietojaan. Yrityksen ylläpitämä data on arvokas resurssi yrityksen kilpailukyvyn ylläpitämisen suhteen, jonka takia yrityksissä on alettu yhä enemmän panostamaan arvokkaan tiedon suojaamiseen. Tietoturva kappaleessa käyn läpi sisäisen tietoturvan parhaiden käytäntöjen toteuttamista sekä henkilötietojen käsittelyyn liittyvää tietosuojaa.

3.1 CIA-malli

Yrityksen tietoturvan suojaamisessa voidaan hyödyntää kolmea keskeistä periaatetta, johon kuuluvat tiedon luottamuksellisuus, eheys ja saavutettavuus. Kyseistä toimintamallia, joka tunnetaan maailmalla lyhenteestä CIA (Eng. confidentiality, integrity, availability) on hyödynnetty laajasti eri ISO-standardeissa, kansallisissa standardeissa sekä lainsäännöksissä. (Järvinen 2022, 13, 25.; Wen-Lung ym. 2023, 2.)

Alla olevassa kuviossa 2 on esitetty CIA-mallin koostumus. Kuvion jälkeen avataan vielä erikseen jokaisen kohdan sisältöä.



Kuvio 2. CIA-malli Wen-Lung (2023, 2) mukaillen.

Luottamuksellisuus (C)

Tiedon tulee olla suojattua niin, että ulkopuoliset tahot eivät pääse käsiksi esimerkiksi yrityksen liikesalaisuuksiin tai palkanmaksutietoihin. Tiedon luottamuksellisuuden ylläpitämiseen linkittyy vahvasti henkilöstön vaitiolovelvollisuus sekä laitteiden oikeaoppinen suojaaminen. (Järvinen 2022, 13.)

Eheys (I)

Tiedon eheydellä viitataan siihen, että tietoon ei ole tehty siihen kuulumattomia muutoksia, jonka lisäksi tiedon tulee muodostaa looginen kokonaisuus. Tiedon eheyttä voi uhata esimerkiksi henkilöstön pääsy heille kuulumattomiin arkaluontoisiin tiedostoihin, yrityksen verkkosivujen hakkerointi tai ohjelmointivirheet yrityksen järjestelmissä. (Järvinen 2022, 13.)

Saavutettavuus (A)

Tiedon saavutettavuudella viitataan aiemmista kohdista poiketen puhtaasti teknisiin ongelmiin. Saavutettavuuden varmistamiseksi yrityksillä on lukuisia eri vaihtoehtoja varautua häiriötilanteiden varalle mutta täydellisen saatavuuden tavoittaminen voi koitua useasti liian kalliiksi. (Järvinen 2022, 13.)

3.2 Tietosuoja

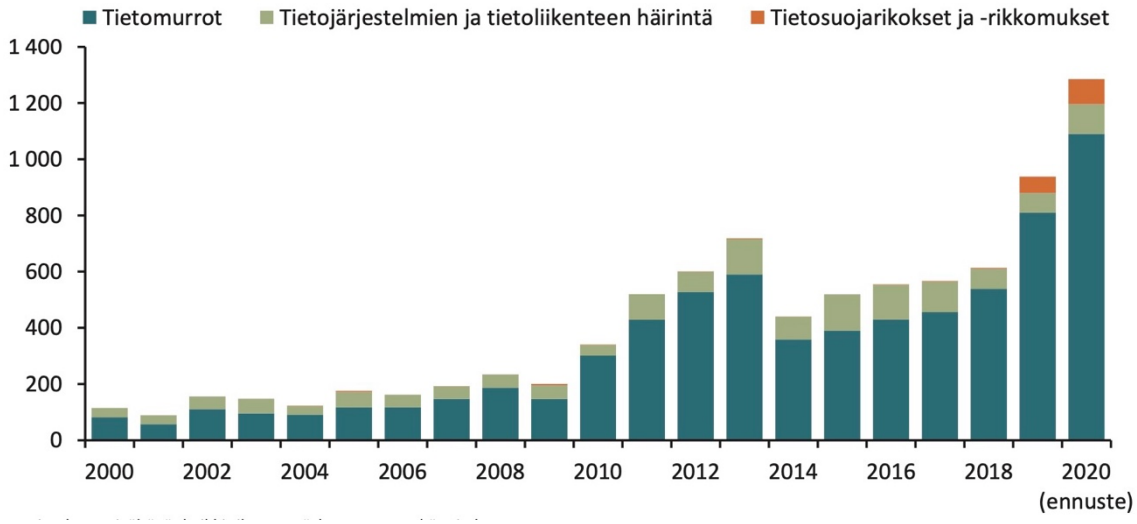
Tietosuoja termiä käytetään silloin, kun yrityksessä käsitellään esimerkiksi asiakkaiden henkilötietoja. Henkilötiedot kuuluvat yksityisyyden mukaiseen perusoikeuteen, eikä niitä saa tämän puolesta käsitellä tai kerätä ilman perusteltuja syitä. Asiakassuhteiden hallinnointi edellyttää kuitenkin usein asiakkaan henkilötietojen keräämistä mutta tietojen tulee silloinkin olla olennaisia ja välttämättömiä kyseisen toiminnan kannalta. Asiakkailla on tämän lisäksi aina oikeus tarkistaa ja pyytää yritystä poistamaan tietonsa, jos kokee tämän tarpeelliseksi. (Järvinen 2022, 25.)

Vuodesta 2018 alkaen EU-maissa tietosuojaa on suoraan sovellettu oikeudessa tietosuoja-asetuksen (GDPR) avulla. Tietosuojaa koskevia velvoitteita valvotaan aktiivisesti ja yritykset voivat kohdata merkittäviä rangaistusmaksuja, jos he eivät täytä tietosuoja-asetuksen mukaisia velvoitteitaan. Tietosuojasta aiheutuvat mainehaitat voivat olla myös hyvin haitallisia ja pitkäkestoisia yrityksen imagolle. Tietosuojaa käsiteltävissä asioissa voidaan GDPR-asetuksen lisäksi myös hyödyntää kansallisia tietosuojalakeja sekä muita toimialakohtaisia lakeja. Yrityksen tietosuojaa koskevista velvoitteista vastaa aina yrityksen hallitus sekä toimiva johto. (Järvinen 2022, 25–26.)

4 Tapaus

”Olen vakuuttunut siitä, että on olemassa vain kahdenlaisia yrityksiä: niitä, jotka on hakkeroitu, ja niitä, jotka tullaan hakkeroimaan. Ja jopa ne ovat siirtymässä yhteen luokkaan: yritykset, jotka on hakkeroitu ja jotka tullaan hakkeroimaan uudelleen”. (The FBI 2012.) Entinen FBI:n johtaja Robert S. Mueller lausui edellä mainitut legendaariset sanat jo vuonna 2012 pidetyssä kyberturvallisuuden konferenssissa. Vaikka kyberriskit ovat olleet jo verrattain pitkään keskuudessamme, herää silti kysymys, ovatko yritykset varautuneet riittävästi mahdollisia uhkia kohtaan mitä kyseessä oleva aihepiiri sisältää.

Allianzin teettämän riski barometrin mukaan kyberriskit, joihin kuuluvat muun muassa kiristysohjelmat, tietomurrot ja palvelunestohyökkäykset ovat nyt organisaatioille ensimmäistä kertaa globaalisti selkeästi suurin riski, organisaation koosta riippumatta (Allianz 2024). Myös kotimaassa kyberrikokset ovat kasvaneet voimakkaasti viime vuosien aikana. Alla olevassa kuvassa 1 kuvataan poliisin tietoon tulleiden kyberrikosten määrää Suomessa vuosina 2000–2020.



Kuva 2. Poliisin tietoon tullut kyberrikollisuuden määrä Suomessa vuosina 2000–2020, kpl (Mattila ym. 2020, 3).

Kyberturvallisuudella pyritään määrittämään toimenpiteet, joiden avulla pystytään proaktiivisesti hallitsemaan ja määrittämään erilaisia kyberuhkia ja niiden seurauksia. Yritysten kyberturvallisuudella tarkoitetaan organisaation digitaalisten palveluiden turvallisuutta ja niiden merkitystä kyseisiin toimintoihin. Tietoturva on myös kriittinen osa kokonaisvaltaista kyberturvallisuutta, koska useasti kybertoimintaympäristön häiriön taustalla on juuri tietoturvauhka. Tietoturvalla tarkoitetaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta. (Kyberturvallisuuden sanasto, Turvallisuuskomitea 2018).

Samalla kun kyberuhat lisääntyvät voimakkaasti, tulevat yritykset entistä riippuvaisemiksi digitaalisista järjestelmistä ja palveluista. Kyberuhilla tarkoitetaan yrityksen ohjelmistoihin, tietoliikenneyhteyksiin, laitteisiin ja järjestelmiin kohdistuvia vahingollisia tapahtumia, jotka voivat vaikuttaa negatiivisesti yrityksen ylläpitämään tietoon ja taloudelliseen asemaan sekä pahimmassa tapauksessa aiheuttaa liiketoiminnan keskeytymisen. Kyberturvallisuutta määritellessä täytyy kuitenkin ottaa huomion myös uhan kääntöpuoli eli mahdollisuus. Kybermaailma tarjoaa valtavasti uusia mahdollisuuksia organisaatioille tehostaa liiketoimintaansa, kehittää uusia palveluja, vähentää kustannuksia ja vallata uusia markkinoita. Organisaatioiden tulee pyrkiä juuri löytämään tämä sopiva tasapaino toimialakohtaisten uhkien ja mahdollisuuksien välillä. (Traficom, 2020; Limnéll ym. 2015, 15).

4.1 Kyberuhat

Yrityksen kyberuhat voivat muodostua ulkoisista, sisäisistä, tahallisista tai tahattomista tapahtumaketjuista. Usein kyberuhat mielletään ulkopuolisiksi hyökkäyksiksi yrityksen järjestelmiin eikä täten oteta huomioon, että pelkästään henkilöstön huolimattomuus voi muodostaa vakavan kyberuhan.

Kasbersky Labs (2019) teettämään artikkelin pohjalta on laadittu taulukko 2, jonka avulla pyritään havainnollistamaan mitä eri aihealueita organisaation tulisi ottaa huomioon kyberturvallisuuden ylläpitämiseksi.

Taulukko 2. Kybertuvallisuuden viitekehys mukaillen (Kasbersky 2019).

Turvattava kohde	Selite
Verkkoturvallisuus	Käytäntö, jolla suojataan tietokoneverkkoa ulkopuolisilta tunkeutujilta.
Sovellusten turvallisuus	Käytäntö, jonka tavoitteena on pitää ohjelmistot ja laitteet suojattuina erilaisilta uhilta. Vaarantunut sovellus voi mahdollistaa hyökkääjän pääsyn tietoihin, joita se on tarkoitettu suojelemaan.
Tietoturvallisuus	Tiedon varastoinnissa ja siirrossa varmistettava tiedon yksityisyys, eheys ja saavutettavuus.
Operatiivinen turvallisuus	Operatiivisessa turvallisuudessa pyritään määrittämään prosessit, joiden avulla turvataan ja käsitellään tietovaroja.
Vahingosta palautuminen ja liiketoiminnan jatkuvuus	Vahingosta palautumiselle pyritään määrittämään toimintaperiaatteet, joiden avulla organisaatio pystyy palaamaan samaan toimintakykyyn kuin ennen vahingon sattumista. Toiminnan jatkuvuuden turvaamiseksi organisaation tulee määrittää toimenpiteet siitä, miten liiketoiminta voi jatkua ilman tiettyjä resursseja.
Loppukäyttäjien koulutus	Loppukäyttäjät eli inhimillisesti toimivat ihmiset muodostavat organisaatiolle arvaamattoman riskin, jos heidän kyberturvataitonsa eivät ole vaaditulla tasolla.

Taulukon 2 perusteella voimme todeta, että kyberturvallisuuden ylläpitämisessä korostuu erityisesti strategisen suunnittelun tärkeys. Taulukossa esitettyjen eri aihealueiden sisältämiä kyberhyökkäyksiä on kuvattu tarkemmin kyberuhkien kappaleen alaluvuissa.

4.1.1 Palvelunestohyökkäys

Palvelunestohyökkäyksessä (DoS attack) kyberhyökkääjä pyrkii lamauttamaan organisaation toiminnan estämällä sen pääsyn verkossa oleviin palveluihin. Kyberhyökkääjä pyrkii ruuhkauttamaan kohdistetulla liikenteellä uhrin verkkopalvelimen resurssit niin, että kriittiset palvelut eivät pysty enää vastamaan tai ne kaatuvat hyökkäyksen seurauksena. Hyökkäyksen takia käytöstä poissa olevat resurssit estävät laillisten käyttäjien pääsyn niihin, mikä aiheuttaa hyökkäyksen kohteena olevalle organisaatiolle taloudellista vahinkoa sekä vaihtoehtokustannuksen menetetystä ajasta. (CISA, 2021.)

Organisaatio voi joutua myös hajautetun palvelunestohyökkäyksen kohteeksi (DDoS attack), kun vaarallisista laitteista koostuva bottiverkko muodostaa eksponentiaalisen määrän pyyntöjä keskitettyyn kohteeseen. Hajautetussa palvelunestohyökkäyksessä tekijän jäljitettävyys hankaloituu myös hajautuksen seurauksena merkittävästi. (CISA, 2021.)

4.1.2 Tietojenkalastelu

Tietojenkalastelu on osa sosiaalisen manipuloinnin yläkäsitettä, jossa hyökkääjä pyrkii hyödyntämään petollisesti käyttäjien inhimillisyyttä, vedoten esimerkiksi kiireeseen tai tunteisiin. Tietojenkalastelijoita kiinnostavat usein käyttäjien luottokorttitiedot ja salasanat, joita he pyrkivät keräämään tyypillisesti sähköpostin, sosiaalisen median tai tekstiviestien avulla. Vilpillisten viestien tarkoituksena on ohjata hyväuskoinen käyttäjä hyökkääjän verkkosivustoille, jossa hänen luottamukselliset tietonsa pyritään kavaltamaan. (Jakobsson & Myers 2007, 1.)

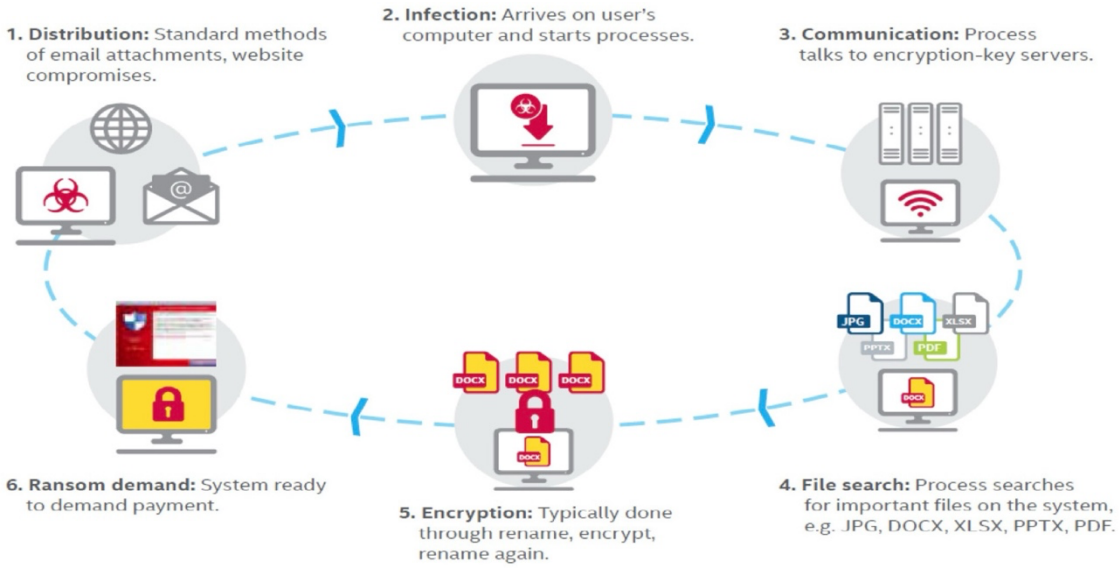
Tyypillinen tietojenkalastelu hyökkäys voidaan jakaa kolmeen eri vaiheeseen: viehe, koukku ja saalis. Kyseinen prosessi on alla kuvatun kaltainen (Jakobsson & Myers 2007, 5)

- Huijausprosessin ensimmäisessä vaiheessa korostuu voimakkaimmin tietojenkalasteluun liittyvä sosiaalisen manipulaation vaikutus, kun kyberhyökkääjä pyrkii parhaansa mukaan vakuuttamaan käyttäjän luovuttamaan luottamuksellista tietoa huijausviestin lähettäjälle. On myös yleistä, että huijausviesti pyritään tekaisemaan jonkin laillisen instituution tekemäksi. Kyberhyökkääjä lähettää tyypillisesti aluksi massapostina huijausviestin eri organisaatioille ja ihmisille, joka sisältää koodatun URL-hyperlinkin, mikä ohjaa kyberhyökkääjän tekemille verkkosivuille ja siellä pyritään saamaan käyttäjä jakamaan henkilökohtaisia tietojaan.
- Huijausprosessin toisessa osassa käyttäjä on siirtynyt verkkosivuille. Verkkosivut on pyritty luomaan niin, että uhri ei kyseenalaistaisi sivujen aitoutta ja tämän seurauksena luovuttaisi mahdollisimman paljon kyberhyökkääjän pyytämiä tietoja.
- Huijausprosessin viimeisessä osiossa kyberhyökkääjä on saanut käsiinsä käyttäjän luottamuksellisia tietoja, joita hän käyttää petolliseen toimintaan esimerkiksi identiteettivarkauteen.

4.1.3 Kiristyshaittaohjelmat

Kiristyshaittaohjelmien tarkoitus on kohdistaa hyökkäys organisaation tiedostoihin tai niihin liittyviin resursseihin, jonka onnistuessa kyberhyökkääjä salaa organisaation datan tehden siitä käyttökelvotonta. Kyberhyökkääjä pyrkii käymään tämän jälkeen kauppaa kaapattujen tietojen kanssa, missä hän voi kiristää organisaatiota esimerkiksi tietovuodolla, avainresurssien lukitsemisella tai vitaalin datan hävittämisellä. Perinteisistä haittaohjelmista poiketen kiristyshaittaohjelmien negatiivisa vaikutuksia voi olla haastavaa poistaa ja jossain tapauksissa ne voivat myös jättää pysyvän jäljen. (Bander ym. 2018, 144–145.)

Alla olevassa kuvassa 2 esitetään miten organisaatio voi joutua kiristyshaittaohjelman kohteeksi.



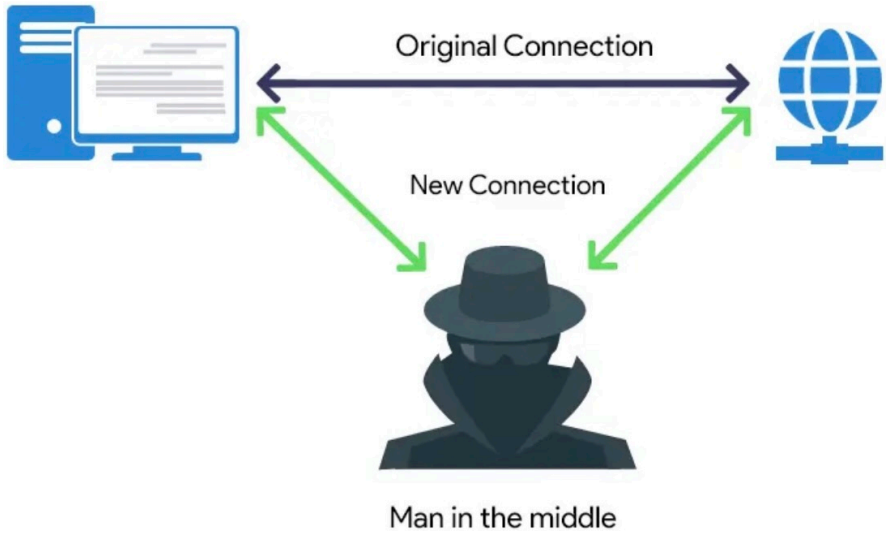
Kuva 3. Kiristyshaittaohjelman tyypillinen elinkaari (Bander ym. 2018, 153).

Traficom (2022, 2) mukaan organisaation tulee varautua proaktiivisesti mahdollisten kiristyshaittaohjelmien varalle, sillä lunnaiden maksaminen tilanteen ratkaisemiseksi ei ole oikea vaihtoehto. Vaikka lunnaat maksettaisiin kyberhyökkääjälle, niin ei ole silti mitään takuita siitä, että hyökkäys loppuisi tai tiedostot palautettaisiin asianmukaisesti. Hyökkäys voi olla myös pelkästään hämäystä, missä kyberhyökkääjän tavoitteena on pelkästään tuhota organisaation tiedot.

4.1.4 Man-In The-Middle

Man-In-The-Middle on haitallinen kyberhyökkäys, jossa hyökkääjä onnistuu saamaan luvattoman pääsyn kahden tai useamman päätepisteen väliseen tietoliikenteeseen. Kyberhyökkääjän pääasiallisena tarkoituksena on siepata viestintäkanavien osapuolten välillä käsitelty data, jonka jälkeen hän pyrkii aiheuttamaan sille vahinkoa joko tarkastelemalla, piilottamalla tai muokkaamalla sitä. (Rahul ym. 2024, 3.)

Alla olevassa kuvassa 3 hyökkääjä on päässyt käsiksi osapuolten väliseen tietoliikenteeseen.



Kuva 4. Man-In-The-Middle hyökkäys (Beagle Security 2020).

MITM- kyberhyökkäykset voidaan toteutukseltaan jakaa kahteen eri suoritusvaiheeseen. Itse MITM-suorituksessa hyökkääjä pyrkii saamaan pääsyn heikosti suojattuun useasti ilmaiseen Wi-Fi-kytkimeen, joita voi sijaita muun muassa julkisissa kahviloissa. Kyseisessä hyökkäyksessä tekijän täytyy olla fyysisesti lähellä kohdetta, jotta hän pystyy purkamaan kohteen salauksen. Hyökkääjän päästyä asiasta tiedottaman asiakkaan verkkoliikenteeseen käsiksi, tapahtuu suorituksen toinen vaihe, nimeltään Man-In-The-Browser (MITB), jossa kyberhyökkääjä pyrkii asentamaan haittaohjelman asiakkaan laitteeseen. Haittaohjelma kerää siihen koodatut tiedot asiakkaan verkkoliikenteestä ja lähettää ne tämän jälkeen kyberhyökkääjälle. (Mallik 2018, 111).

4.1.5 Henkilöstö

Olemme käsitelleet tässä vaiheessa kyberturvallisuuden yleisimpiä ulkoisia uhkia, mutta kyberuhkien viimeisessä kappaleessa pääsemme paneutumaan sisäiseen uhkaan, missä henkilöstö voi aiheuttaa organisaatiolle merkittäviä kyberturvallisuusriskejä.

Monet organisaatioihin kohdistuvista kyberhyökkäyksistä ovat aiheutuneet henkilöstöön liittyvistä haavoittuvuuksista, joiden seurauksena organisaatiolle voi kohdistua huomattavaa taloudellista tappiota sekä maine haittoja. Tämän lisäksi tilannetta pahentaa se, että vaikutukset eivät useasti ole heti havaittavissa. Henkilöstön asianmukainen kouluttaminen on organisaatiolle ensisijaisen tärkeää koska pelkästään teknologolisiin suojatoimenpiteisiin panostamalla ei pystytä poistamaan ihmisten tekemiä inhimillisiä virheitä. (Prümmer ym. 2024, 1.)

Prümmer ym. (2024, 2) jakaa artikkelissaan organisaation sisäisen kyberturvallisuuden neljään eriin käyttäytymismalliin. Nämä käyttäytymismallit liittyvät salasanojen käyttöön, turvallisuuspolitiikan noudattamiseen, sähköpostikäyttäytymiseen ja viestintään, jossa korostuu erityisesti organisaatiokulttuuri.

Yleisin haavoittuvuus salasanoihin liittyen syntyy, kun käyttäjät luovat liian helposti arvattavia sekä lyhyitä salasanoja. Heikon salasanan saattelemana voi ulkopuolinen päästä sisään organisaation järjestelmiin ja aiheuttaa tällä vakavaa vahinkoa.

Turvallisuuspolitiikkaan lukeutuu organisaatio kohtaiset käytänteet, johon voi kuulua muun muassa näytön lukitsemispolitiikka sekä tiedostojen jakamiseen liittyvät säännökset. Tietojenkalasteluhyökkäykset ovat erityisesti asia, joka korostuu henkilöstön sähköpostin välityksellä tapahtuvista haavoittuvuuksista.

Yleisesti organisaation kyberturvallisuus viestintä painottuu eri muodoissa järjestettäviin koulutuskampanjoihin, vaikka tutkimusten mukaan nämä eivät ole kovin tehokkaita. Koulutuskampanjoiden ongelmaksi muodostuu liian suppea tiedon määrä sekä vähäinen painoarvo uhkien reagointiin liittyen. Haasteeksi on havaittu myös henkilöstön innostuksen puuttuminen kyseiseen aiheeseen liittyen.

Kaspersky Lab ja B2B International (2017) teettivät kyberturvallisuuteen liittyvän tutkimuksen, jossa he pyrkivät selvittämään henkilöstön roolia osana kyberhyökkäyksiä. Tutkimuksessa oli mukana globaalisti yli viisi tuhatta eri kokoista yritystä. Tulokset olivat seisauttavia, kun organisaatiosta 52 prosenttia koki olevansa sisäisesti vaarassa, joko henkilöstön tietämättömyydestä tai huolimattomuudesta johtuen. Tutkimuksessa oli myös huomionarvoinen kohta, missä oli selvitetty toimintatapoja vahingon sattumisen jälkeen. Tutkimukseen vastanneista jopa 40 prosenttia pyrki salamaan joutuneensa kyberhyökkäyksen kohteeksi, aiheuttaen täten yhä enemmän vahinkoa organisaatiolle.

4.2 Kyberturvallisuuden hallinta

Kyberturvallisuuden hallintaa käsittelevässä luvussa tutkitaan mitä asioita pienyritysten tulisi ottaa huomioon suunnitellessaan kyberstrategiaansa sekä millaisia eri kyberturvallisuuden parhaan käytännön hallintamenetelmiä- ja standardeja voidaan hyödyntää osana organisaation riskienhallintaa.

Pienyritykset kohtaavat merkittävän haasteen kyberturvallisuuden hallinnoinnissa, koska pienissä yrityksissä turvallisuus on jokaisen yksittäisen käyttäjän varassa. Käyttäjien kyberturvallisuuden ymmärryksen puute sekä inhimilliset virheet voivat aiheuttaa pienyrityksille vakavia tietovuotoja. Haastavaksi kyberturvallisuuden hallinnoinnin tekee myös se, että pienyritykset kokevat suuryrityksistä poiketen kyberturvallisuuden investoinnit harkinnanvaraisena kulueränä, eikä välttämättömyytenä pitkän aikavälin kilpailukyvyn säilyttämiselle. Pienyrityksiin enenemissä määrin kohdistuvat kyberhyökkäykset ovat olleet seurasta rajallisista resursseista, tarvittavan teknologian puutteesta sekä kyvyttömyydestä käynnistää hyökkäyksen jälkeen tarvittavia puolustus menetelmiä. (Aurelien 2021, 1–2.)

Aurelien (2021, 1, 7) toteaa väitöskirjassaan, että suuryritysten kehittyneemmät kyberstrategiat ovat olleet osatekijä sille, miksi kyberrikolliset keskittävät enemmän hyökkäyksiä pienyrityksiä kohtaan, joilla on vähemmän resursseja käytettävissä. Pienyritysten kyberturvallisuuden taso ei ole pelkästään kriittistä oman liiketoimintansa jatkuvuuden kannalta, vaan sillä on merkittäviä vaikutuksia myös suuryrityksiin sekä muihin merkittäviin organisaatioihin. Kyberhyökkäyksen uhriksi joutunut pienyritys voi pahimmassa tapauksessa avata kyberrikollisille haitallisen pääsyn kumppani organisaatioon tietoihin.

4.2.1 NIST

National Institute of Standards and Technology (NIST) lukeutuu yhdeksi Yhdysvaltojen vanhimmista fysiikan laboratorioista. NIST perustettiin vuonna 1901 parantamaan Yhdysvaltojen teollista kilpailukykyä, luomalla kriittisiä mittausratkaisuja sekä standardeja. (NIST 2022.)

NIST Cyber security Framework 2.0 asettaa organisaatioille viitekehyksen, miten he pystyvät arvioimaan, ymmärtämään, priorisoimaan ja viestimään tehokkaammin kyberturvallisuustoimistaan. Kyberturvallisuuden viitekehys on teknologia- ja sektorineutraali, joten sen hyödyntäminen on yleisintä strategisella tasolla, osana organisaation riskienhallintaa. (CSF 2.0 2023, 1.)

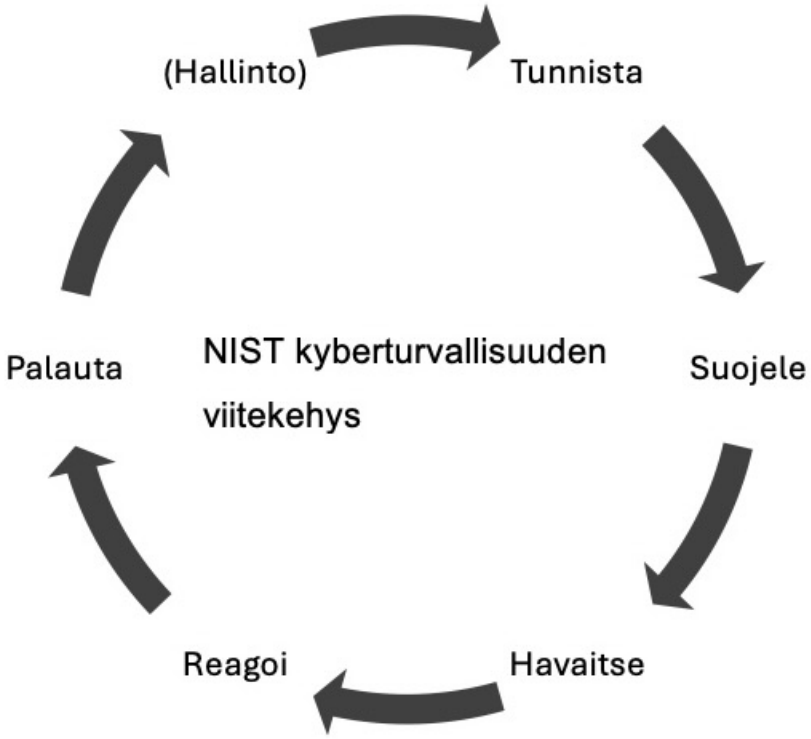
CSF 2.0 (2023) asettaa organisaatiolle rakenteen sekä taksonomian, jota hyödyntämällä voidaan arvioida, ymmärtää, priorisoida ja viestiä tehokkaammin kyberturvallisuusriskeistä. Alla olevassa taulukossa 3 on kuvailtu tarkemmin mitä kyberturvallisuuden taksonomialta haetaan.

Taulukko 3. Kyberturvallisuuden taksonomia mukaillen (CSF 2.0 2023, 2).

Aiheet	Toimintaohjeet
Arvioi ja ymmärrä	Selvitä organisaation nykyinen ja tavoiteltu kyberturvallisuustilanne sekä organisaation olemassa olevat kyberturvallisuusaukot sekä mahdolliset tulevaisuuden uhat.
Priorisoi	Organisoi riittävästi kyberturvallisuuteen liittyviä resursseja, jotka ovat linjassa organisaation mission, ulkopuolisten odotusten ja riskienhallinnan kanssa. Tunnista kyberturvallisuuteen liittyvän työvoiman tarpeet.
Kommunikoi	Varmista tehokas kyberturvallisuuden liittyvä kommunikaatio sisäisten ja ulkoisten osapuolten kanssa. Kyberturvallisuusstandardien- ja ohjeiden esiin tuominen hallinnollisella tasolla.

Taulukon 3 perusteella voidaan todeta, että kyberturvallisuuden ylläpitäminen edellyttää tehokasta kommunikointia eri sidosryhmien välillä, jotta organisaation kyberturvallisuuden hallintaan ohjataan tarpeiden mukaisesti resursseja ja organisaatiossa tiedostetaan hallitsevat kyberturvallisuuden toimintaohjeet.

CSF 2.0 (2023) määrittää lisäksi kyberturvallisuuden viitekehyksen ydintehtävät, jotka on esitetty alla olevassa kuviossa 3.



Kuvio 3. Viitekehyksen ydintehtävät (CSF 2.0 2023, 6).

Kuvion 3 viitekehyksen Ydintehtävien järjestyksen ei ole tarkoitus kuvata sitä, missä järjestyksessä ne tulisi toteuttaa, saati kuvata niiden painoarvon merkitystä.

Hallinto

Hallinto-osion tarkoituksena on määrittää, miten organisaatio onnistuu saavuttamaan viiden muun toiminnon tavoitteet sekä täyttämään sidosryhmien odotukset. Hallintotoimet liittyvätkin vahvasti kyberturvallisuusstrategian ja sen sisällyttämiseen osaksi riskienhallintastrategiaa. (CSF 2.0 2023, 5.)

Tunnista

Tunnista-osiossa pyritään määrittämään organisaation kyberriskien nykytila. Ymmärtämällä oman riskiprofiilinsa, on organisaation helpompaa priorisoida resurssejaan riskienhallinnanstrategian mukaisesti. (CSF 2.0 2023, 5.)

Suojele

Suojele-osion tarkoituksena on suojata omaisuus tunnistetuilta ja priorisoiduilta kyberriskeiltä. Riskejä on tarkoitus priorisoida niiden todennäköisyyksien mukaan ja tämän avulla ne pyritään joko poistamaan kokonaan tai niiden vaikutus halutaan minimoida. Suojelu-osion pääpainona on henkilöstön tiedottaminen ja kouluttaminen sekä ohjelmistojen ja palvelujen suojaaminen. (CSF 2.0 2023, 6.)

Havaitse

Havaitse-osion tarkoituksena on etsiä ja analysoida haitallisia poikkeamia ja kyberturvallisuushäiriöitä- ja hyökkäyksiä, mahdollisimman varhaisessa vaiheessa (CSF 2.0 2023, 6).

Reagoi

Reagoinnin tarkoituksena on hillitä kyberhyökkäysten aiheuttamaa vaikutusta. Kyberhyökkäyksiin reagointi sisältää myös tapausten analysoinnin, raportoinnin sekä hallinnoinnin. (CSF 2.0 2023, 6.)

Palauta

Kyberhyökkäyksen jälkeen on tärkeää pystyä palauttamaan toiminta aikaisemmalle tasolle mahdollisimman tehokkaasti sekä mahdollistaa läpinäkyvä raportointi palautustoimien aikana. (CSF 2.0 2023, 6.)

4.2.2 ISO/IEC 27001

Kansainvälinen standardointijärjestö (ISO) ja kansainvälinen sähkötekninen komissio (IEC) ovat kehittäneet yhdessä standardit tietoturvan hallitsemisen parhaista käytännöistä. Standardi ISO/IEC27001 julkaistiin vuonna 2005 ja sitä päivitettiin myöhemmin vuonna 2013. Tietoturvan hallinnan standardi on kehitetty teknologiasta riippumattomaksi sekä toimialaneutraaliksi. Standardi voidaan integroida kaiken kokoisiin organisaatioihin niiden luonteesta riippumatta. (Calder & Gerrard 2013, 12–13.)

ISO/IEC27001-standardi sisältää 14 eri lauseketta, joita on kuvattu liitteessä A. Lausekkeet on esitetty tässä työssä tyylillä A5 – A18. On myös huomionarvoista, että lausekkeiden järjestyksellä ei ole merkitystä. Lausekkeet A1 – A4 on jätetty tästä työstä tarkoituksella pois, koska ne kuuluvat standardiin ISO/IEC27002. (Calder & Gerrard 2013, 28.)

Calder & Gerrard (2013, 62 – 74) standardin ISO/IEC27001 lausekkeet A5 – A18.

A5 Tietoturva

Lausekkeen tarkoituksena on tukea johdon kykyä hallinnoida tietoturvaan liittyviä toimialakohtaisia vaatimuksia, lakeja sekä määräyksiä. Lauseke sisältää tietoturvakäytännöt.

A6 Tietoturvan järjestäminen

Lausekkeen tarkoituksena on muodostaa viitekehys tietoturvan valvonnalle ja toteuttamiselle organisaatiossa. Viitekehykseen laatimisessa tulee ottaa huomioon tietoturvan roolit ja organisaatio kohtaiset käytänteet, ulkoinen raportointi eri sidosryhmille ja viranomaisille sekä varmistaa järjestelmien ja etätyön turvallisuus.

A7: Henkilöstön turvallisuus

Lausekkeessa käsiteltävät vaatimukset voidaan jakaa kolmeen eri osaan: Ensimmäinen osa käsittelee aikaa työllistymisen alussa, jossa halutaan varmistua, että urakoitsijat ja työntekijät ymmärtävät vastuunsa sekä työehtonsa. Toinen osa käsittelee jaksoa työsuhteen aikana, jossa halutaan varmistua, että urakoitsijat ja työntekijät tiedostavat tietoturvaan liittyvät vastuunsa. Viimeisessä vaiheessa halutaan turvata organisaation etu, työsuhteen muutos- tai irtisanoutumisprosessin aikana.

A8: Omaisuuden hallinta

Lausekkeen tarkoituksena on määrittää vastuut organisaation omaisuuden ja datan asianmukaiselle turvaamiselle sekä palauttamiselle. Lauseke sisältää myös ohjeet mediasuhteiden käsittelyyn, johon sisältyy muun muassa median hallussa olevan tiedon luvaton paljastaminen, muuttaminen tai poistaminen.

A9: Pääsyn valvonta

Lausekkeen tarkoituksena on määrittää henkilöstön käyttöoikeuksien hallinta organisaation järjestelmiin ja palveluihin. Lausekkeeseen sisältyy myös muun muassa käyttäjien velvollisuudet todennustietojen turvaamisessa, salasanojen hallinnoinnin sekä lähdekoodin kulunvalvonnan.

A10: Kryptografia

Lausekkeen tarkoituksena on varmistaa kryptografian luottamuksellisuuden, eheyden ja aitouden järjestäminen. Lausekkeeseen sisältyy myös kryptografian käyttöön liittyvät käytännöt sekä avainten hallinta.

A11: Ympäristön fyysinen turvallisuus

Varmistetaan fyysisen pääsyn estäminen organisaation tietojenkäsittelytiloihin, toimistoihin sekä toimitus- ja lastausalueisiin. Fyysisen pääsyn estämisen lisäksi lausekkeessa määritetään organisaation laitteiston turvaaminen. Laitteiston turvaamiseen sisältyy liiketoiminnan jatkuvuuden varmistaminen suojaamalla laitteisto katoamisten, vahingoittumisten tai varkauksien varalta.

A12: Toiminnan turvallisuus

Käsitellään tietojenkäsittelylaitteiden liittyviä turvatoimenpiteitä, johon sisältyy muun muassa suojautuminen haittaohjelmien varalta, tietojen säilyttäminen varmuuskopioinnin avulla, ohjelmistojen asentaminen järjestelmiin sekä tietojärjestelmien asianmukainen auditointi.

A13: Tietoliikenneturvallisuus

Käsitellään tietoliikenteen turvaamista verkoissa ja niitä tukevissa järjestelmissä. Aihepiiri sisältää myös tietoliikenteen turvaamisen ja luottamuksellisuuden säilyttämisen sisäisessä- ja ulkoisessa viestinnässä.

A14: Järjestelmien hankinta, kehittäminen ja ylläpito

Lausekkeessa varmistetaan järjestelmien tietoturvallisuuden kehittäminen ja analysointi sen koko elinkaaren aikana.

A15: Toimittajasuhteet

Määritetään organisaation toimittajasuhteissa käsiteltävän tiedon turvallisuus periaatteet, jotka tulee olla linjassa toimittajasopimusten kanssa.

A16: Tietoturvaloukkausten hallinta

Määritetään tietoturvaloukkauksiin liittyvät toimintaperiaatteet ja vastuut. Tietoturvaloukkauksien hallinnan ja raportoinnin tulee olla johdonmukaista ja tehokasta, jonka lisäksi tapauksia analysoidaan jatkon varalle.

A17: Liiketoiminnan jatkuvuuden hallintaan liittyvät tietoturvanäkökohdat

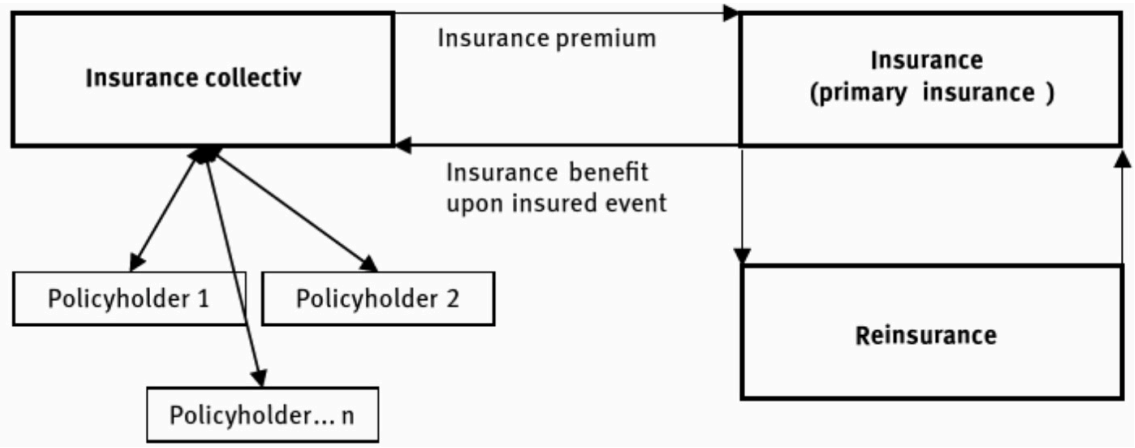
Määritetään tietoturvan jatkuvuuden liittyvät toimintaperiaatteet. Organisaation tulee pyrkiä integroimaan tietoturvan jatkuvuuden turvaaminen osaksi liiketoiminnan jatkuvuuden strategiaa. Tietoturvallisuuden liittyviä epäkohtia tulee pystyä todentamaan, tarkastelemaan ja analysoimaan.

A18: Sääntöjen noudattaminen

Valvotaan että organisaatio toteuttaa tietoturvaa käytäntöjen ja standardien mukaisesti. Varmistetaan että organisaatio noudattaa lakisääteisiä tietoturva- ja sopimusmääräyksiä sekä immateriaalioikeuksia.

4.2.3 Kybervakuuttaminen

Yritykset voivat hyödyntää vakuuttamista osana riskien hallintaa, kun riskiin varaudutaan siirtämällä se vakuutusyhtiölle. Alla olevassa kuvassa 5 on esitetty miten vastuut ja velvollisuudet jakaantuvat vakuuttajan ja vakuutuksen ottajan välillä.



Kuva 5. Vakuutustoiminta havainnollistettuna (Wolke 2017, 99).

Yrityksen täytyy analysoida tarkasti mitä riskejä se haluaa rahoittaa vakuuttamalla, koska vuosittain hoidettavat vakuutusmaksut heikentävät yrityksen tulosta. Yrityksen tulee kiinnittää erityisesti huomiota liiketoiminnan jatkuvuuden kannalta kriittisiin uhkiin, joihin voi kuulua muun muassa yrityksen tuotantolaitoksessa tapahtuva tulipalo tai yrityksen tietoturvaan kohdistuvat kyberhyökkäykset. (Wolke 2017, 98–99.)

OPSEC Oy:n 2019 tuottamassa kybervakuuttamista käsittelevässä blogikirjoituksessa nostetaan esiin, että yrityksen tulisi harkita kybervakuuttamista erityisesti tilanteissa, joissa yritys käsittelee arkaluonteisia tietoja tai jos mahdollinen kyberhyökkäys voisi aiheuttaa yritykselle liiketoiminnan keskeytymisen. Blogikirjoituksessa todetaan myös, että kybervakuuttamiseen liittyvien vakuutusehtojen noudattaminen voi jossain tilanteissa tulla itse riskin turvaamista kalliimmaksi vaihtoehdoksi. (OPSEC 2019.)

5 Kyselyn toteutus

Tämän opinnäytetyön tutkimusongelma sai alkunsa, kun heräsi tarve selvittää toimeksiantajan pienyritysasiakkaiden kyberturvallisuuden nykytilaa sekä asenteita ja uskomuksia sitä kohtaan. Toimeksiantajana toimi vakuutusyhtiö. Kyseinen aihe muodostuikin hyvin relevantiksi koska siitä oli heikosti tietoa saatavilla yleisellä sekä toimeksiantajan tasolla. Työskentelen myös itse opinnäytetyön toimeksiantajan yritysasiakkaiden parissa.

Tutkimustyön tavoitteena oli vahvistaa jo teoriaosuudessa käsiteltyjä johtopäätöksiä sekä reflektoida mahdollisimman tarkasti opinnäytetyön tutkimuskysymystä: ”Miten yrityksen kyberuhkiin on varauduttu liiketoiminnan jatkuvuuden kannalta”?

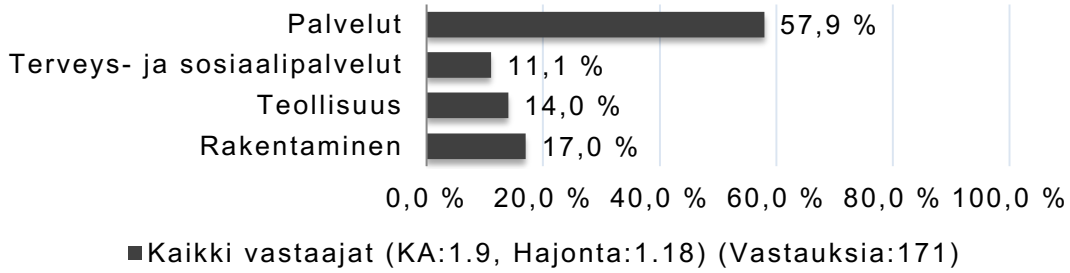
Opinnäytetyön tutkimusstrategiaksi valikoitu kvantitatiivinen survey-tutkimus, jonka tarkoituksena oli kerätä mahdollisimman paljon vastauksia standardoidussa muodossa. Tutkimuksen muodoksi valittiin kyselylomake, jossa kysymykset esitetään samassa järjestyksessä kaikille vastaanottajille ja haastateltavan tulee valita kysymyksistä itselleen parhaiten sopiva vastausvaihtoehto. Kerätyn aineiston tarkoituksena oli kuvailla kohderyhmän kyberuhkiin varautumisen nykytilaa sekä vertailla kyberuhkiin liittyviä asenteita ja uskomuksia muun muassa eri toimialojen välillä. (Hirsjärvi, Remes & Sajavaara 2015, 134, 208.)

Tutkimuksen kohderyhmäksi valittiin 1–9 henkilöä työllistyvät toimeksiantajan yritysasiakkaat. Kyselylomake lähetettiin toimeksiantajan markkinointitiimin avustuksella 5562 asiakkaan sähköpostiosoitteeseen. Kyselylomake oli avoinna 12 päivän ajan ja vastauksia tässä ajassa saatiin 171 kappaletta. Kyselyn vastausprosentiksi muodostui näin 3 %. Olisin henkilökohtaisesti toivonut kyselyyn enemmän vastauksia ottaen huomioon, että kyselylomake lähetettiin yli 5000 asiakkaalle. Saatu vastausmäärä riittää kuitenkin tulosten yleistämiseen kyseisen kohderyhmän kanssa.

5.1 Demografiset tiedot

Tämä kvantitatiivinen tutkimusotos sisälsi 171 eri toimialoilla liiketoimintaa harjoittavaa yritystä, jotka työllistävät alle 10 työntekijää. Kyselylomakkeessa haluttiin selvittää yrityksen pääasiallinen toimiala, henkilöstön määrää, yrityksen liiketoiminnan pitkäikäisyys sekä oliko yritys kohdannut jo aiemmin kyberuhkia.

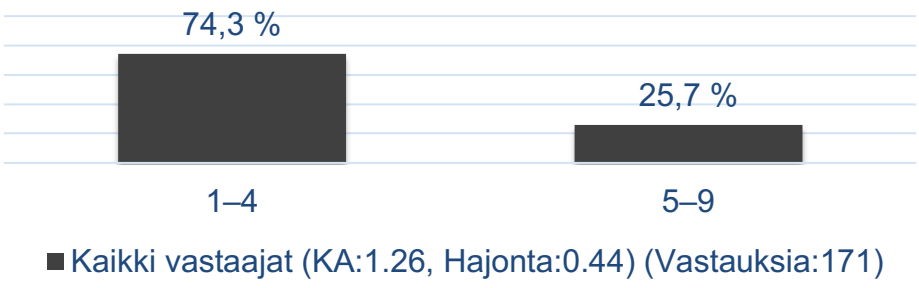
Alla olevassa kuviossa 4 on esitetty kyselyyn vastanneiden toimiala jakauma.



Kuvio 4. Yrityksen toimiala.

Tutkimuksessa nousi esiin, että palvelut olivat toimialoista 57,9 prosentilla yleisin vastausvaihtoehto, jonka jälkeen tulivat rakentaminen 17 prosentilla, teollisuus 14 prosentilla ja tutkimusotoksen pienimpänä terveys- ja sosiaalipalvelut 11 prosentilla. Palveluiden dominanssi tässä kategoriassa voi selittyä sillä, että palvelualan yritykset ovat olleet voimakkaammin osana digitalisoituvaa toimintaympäristöä, joka on myös herättänyt enemmän kiinnostusta tutkimuksen aihetta kohtaan.

Alla olevassa kuviossa 5 on esitetty kyselyyn vastanneiden henkilöstön määrän jakauma.



Kuvio 5. Henkilöstön määrä.

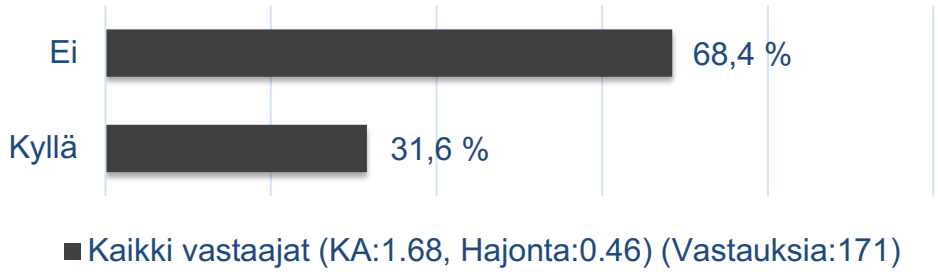
Tutkimukseen vastanneista selkeä enemmistö työllisti 74 prosentilla 1—4 henkilöä, kun 5—9 henkeä työllistäviä oli vain 26 prosenttia vastanneista. Tämä tulos tuli itselleni yllätyksenä, koska teorian mukaan pienimmät yhtiöt ovat yleisesti nähneet kyberturvallisuuden investoinnit harkinnanvaraisempana kulueränä.

Alla olevassa kuviossa 6 on esitetty vastanneiden liiketoiminnan pitkäikäisyyden jakauma

Kuvio 6. Liiketoiminnan pitkäikäisyys.

Tutkimuksesta kävi ilmi, että 21 % vastaajista oli harjoittanut liiketoimintaa 1—5 vuotta, 11 % 5—10 vuotta ja selkeänä enemmistönä 67,8 prosentilla olivat yli 10 vuotta työllistäneet yritykset. Tämä tulos osoittaa sen, että kypsemmissä yrityksissä on panostettu riittävän hyvin riskienhallintaan ja otettu sen myötä erityyppiset uhat huomioon, jotta liiketoimintaa on pystytty jatkamaan.

Alla olevassa kuviossa 7 on esitetty vastanneiden kyberuhkien kohtaamisten jakauma.



Kuvio 7. Onko yrityksessänne kohdattu kyberuhkia esimerkiksi tietojenkalastelua, palvelunestohyökkäyksiä, kiristyshaittaohjelmia, verkkohuijauksia tai jotain muuta?

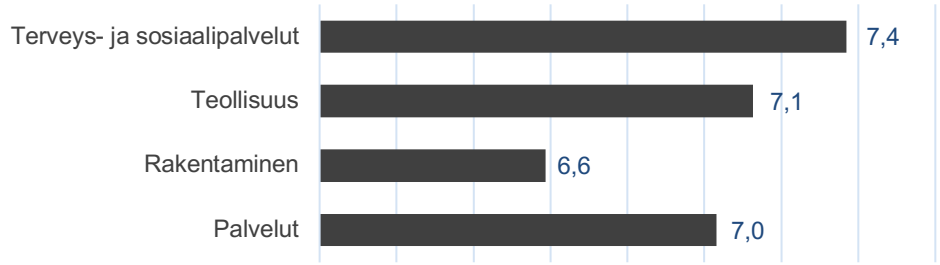
Tutkimuksen mukaan lähes joka kolmas (31,6 %) yritys oli kokenut liiketoiminnassaan kyberuhkia. Kyselyssä ei ollut rajattu tarkemmin sitä, milloin kyberhyökkäys oli sattunut tai minkä laatuinen se oli ollut, mutta saatu tulos kuitenkin tukee hyvin kyberturvallisuuden ajankohtaisuutta.

Tutkimustulokset ovat jaettu neljään osaan, jotka esitän kukin omana alalukunaan. Tulosten jaottelussa hyödynnetään teoriaosuudessa esitettyä kyberturvallisuuden viitekehystä. Tulosten läpikäynti aloitetaan selvittämällä, kuinka hyvin vastaajat kokevat yrityksensä verkko- ja sovellusturvallisuuden olevan hoidettuna. Seuraavaksi selvitetään vastaajien suhtautumista tietoturvallisuuteen ja selvitetään, käsitteleekö yritys tietosuojan mukaisia henkilötietoja. Tämän jälkeen siirrytään selvittämään tutkimuksen kannalta mielenkiintoista kokonaisuutta, missä otetaan selvää henkilöstön roolista osana kyberturvallisuuden hallintaa. Viimeisessä osassa selvitetään opinnäytetyön tutkimuskysymykseen liittyen keskeistä aihetta; miten yritykset ovat varautuneet strategisesta näkökulmasta kyberuhkiin, liiketoiminnan jatkuvuuden kannalta.

5.2 Verkon ja sovellusten turvallisuus

Verkon- ja sovellusten turvallisuudella on tarkoitus suojata tietokoneverkot ulkopuolisilta tunkeutujilta sekä pitää ohjelmistot ja laitteet suojattuina erilaisilta kyberuhilta. Kyselylomakkeessa lähdettiin selvittämään asiakkailta Likertin asteikon mukaan, onko yrityksen ohjelmistot ja/tai laitteistot turvattu riittävän hyvin mahdollisten kyberhyökkäysten varalta? Vastausvaihtoehtona oli 1—10 erittäin heikosti-erittäin hyvin.

Alla olevassa kuviossa 8 vastaajilta kysyttiin, onko yrityksen ohjelmistot ja/tai laitteistot turvattu riittävän hyvin mahdollisten kyberhyökkäysten varalta? Tulokset esitetty toimialoittain.

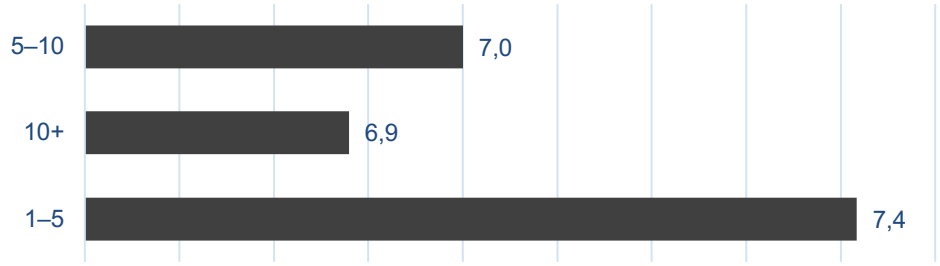


Kuvio 8. Verkon- ja sovellusten turvallisuus toimialoittain.

Kuviosta 8 käy ilmi, että vastaajat kokivat ohjelmistojen ja laitteistojen olevan melko hyvin turvattuna kyberuhkien varalta. Korkeimman arvosanan tähän kysymykseen toimialoista antoi 7,4 keskiarvollaan terveys- ja sosiaalipalvelut ja heikoimman arvosanan 6,6 keskiarvollaan rakentamisen toimiala.

Yrityksen henkilöstön määrän mukaan ei saatu tutkimuksen kannalta mielekästä tulosta, jotta näitä olisi voinut lähteä vertailemaan keskenään. Verkon- ja sovellusten turvallisuuden kysymykseen 1—4 henkilöä työllistävät yritykset antoivat vastaukseksi ka. 7,0 ja 5—9 henkeä työllistävät yritykset vastaukseksi ka. 7,1.

Alla olevassa kuviossa 9 vastaajilta kysyttiin, onko yrityksen ohjelmistot ja/tai laitteistot turvattu riittävän hyvin mahdollisten kyberhyökkäysten varalta? Tulokset liiketoiminnan pitkäikäisyyden mukaan.



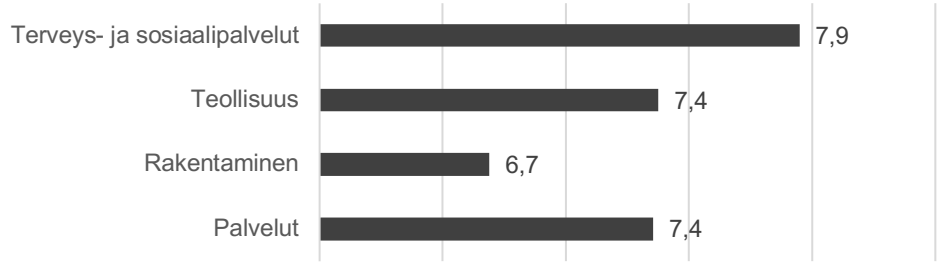
Kuvio 9. Verkon- ja sovellusten turvallisuus liiketoiminnan pitkäikäisyyden mukaan.

Kuviosta 9 käy ilmi, että vastaajat, jotka olivat harjoittaneet liiketoimintaa tästä ryhmästä vähiten (1—5), kokivat 7,4 keskiarvollaan verkon- ja laitteiston turvallisuuden korkeimmaksi. Toisaalla heikommaksi verkon- ja sovellusten turvallisuuden kokivat pisimpään liiketoimintaa harjoittaneet (+10) yritykset 6,9 keskiarvollaan.

5.3 Tietoturvallisuus

Tietoturvallisuudella pyritään varmistamaan yrityksen käsittelemän tiedon yksityisyys, eheys ja saavutettavuus sen siirron ja varastoinnin aikana. Kyselylomakkeessa lähdettiin selvittämään asiakkailta Likertin asteikon mukaan, ”onko yrityksen tietoturvallisuus, johon sisältyy tiedon luottamuksellisuus, eheys ja saavutettavuus suojattu riittävän hyvin”? Vastausvaihtoehtona oli 1—10 erittäin heikosti-erittäin hyvin. Kyselylomakkeessa esitettiin asiakkaille myös kysymys ” Käsitteleekö yrityksenne tietosuoja-asetuksen (GDPR) mukaisia henkilötietoja”? Tähän vastausvaihtoehtona oli KYLLÄ tai EI.

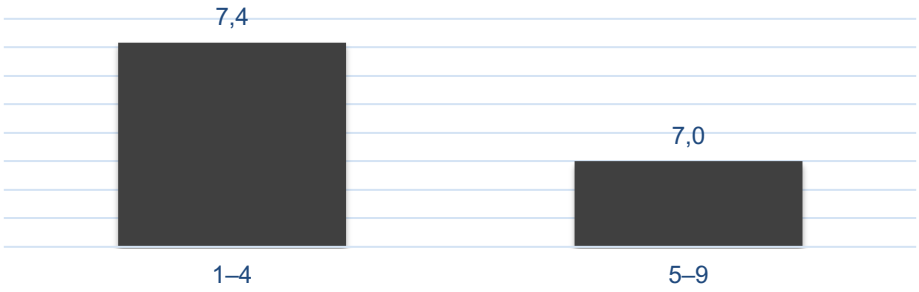
Alla olevassa kuviossa 10 tiedusteltiin vastaajilta, onko yrityksen tietoturvallisuus, johon sisältyy tiedon luottamuksellisuus, eheys ja saavutettavuus suojattu riittävän hyvin? Tulokset toimialan mukaan.



Kuvio 10. Tietoturvallisuus toimialoittain.

Kuviosta 10 käy ilmi, että yleinen luottamus tietoturvallisuuden tasoon on melko korkealla. Parhaimman tuloksen pisteytti terveys- ja sosiaalipalvelut 7,9 keskiarvollaan ja heikoimman arvosanan rakentamisen toimiala 6,7 keskiarvollaan. Tietosuojan alaisia henkilötietoja käsittelevillä yrityksillä ei ollut havaittavissa suoria kausaliteetteja siihen, miten yritykset kokivat oman tietoturvallisuutensa tason.

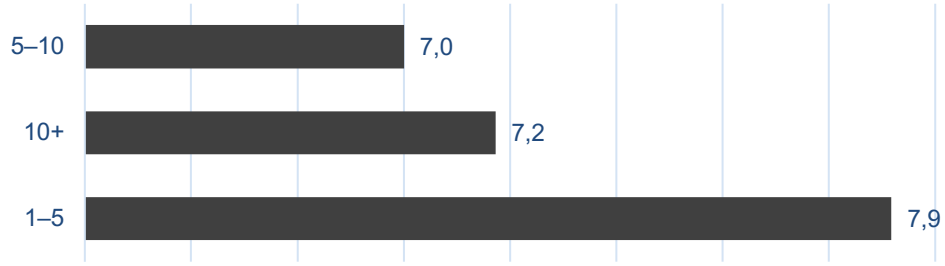
Alla olevassa kuviossa 11 tiedusteltiin vastaajilta, onko yrityksen tietoturvallisuus, johon sisältyy tiedon luottamuksellisuus, eheys ja saavutettavuus suojattu riittävän hyvin? Tulokset henkilöstön määrän mukaan.



Kuvio 11. Tietoturvallisuus henkilöstön määrän mukaan.

Kuviossa 11 käy ilmi, että 1—4 henkilöä työllistävä yritykset kokivat oman tietoturvallisuutensa olevan lievästi korkeammalla tasolla, kuin 5—9 henkilöä työllistävien yritysten osalta. Tietosuojan alaisia henkilötietoja käsittelevillä yrityksiä oli haastavaa lähteä vertailemaan näiden kahden ryhmän välillä, koska 1—4 henkilö työllistäviä yrityksiä oli huomattavasti enemmän.

Alla olevassa kuviossa 12 tiedusteltiin vastaajilta, onko yrityksen tietoturvallisuus, johon sisältyy tiedon luottamuksellisuus, eheys ja saavutettavuus suojattu riittävän hyvin? Tulokset liiketoiminnan pitkäikäisyyden mukaan.



Kuvio 12. Tietoturvallisuus liiketoiminnan pitkäikäisyyden mukaan.

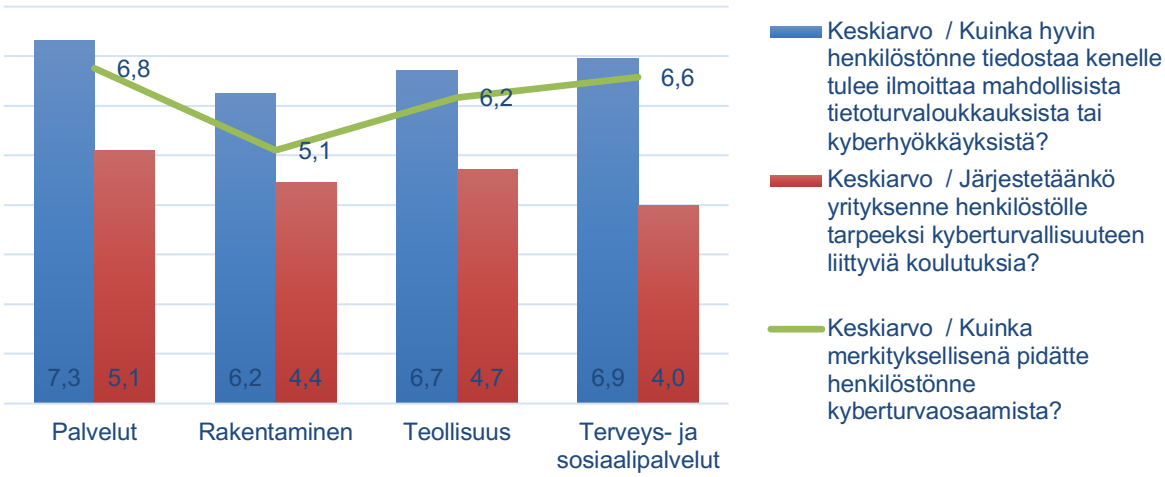
Kuviosta 12 käy ilmi, että parhaimman arvosanan tieturvallisuudesta saivat 1—5 vuotta liiketoimintaa harjoittaneet yritykset ja heikoimman arvosanan 5—10 vuotta liiketoimintaa harjoittaneet yritykset. Tietosuojaan liittyvät kyselyt eivät olleet myöskään tässä kategoriassa vertailukelpoisia.

5.4 Henkilöstö

Henkilöstön kyberturvallisuuden ymmärryksen puute sekä inhimilliset virheet voivat aiheuttaa vakavia tietovuotoja. Yksilönvastuu korostuu erityisesti pienyritysten kyberturvallisuuden ylläpidossa. Kyselylomakkeessa lähdettiin selvittämään asiakkailta Likertin asteikon mukaan vastauksia kolmeen eri kysymykseen. Ensimmäisenä kysymyksenä esitettiin: ” kuinka hyvin henkilöstö tiedostaa kenelle tulee ilmoittaa mahdollisista tietoturvaloukkauksista tai kyberhyökkäyksistä”? Vastausvaihtoehto tähän oli 1—10 erittäin huonosti - erittäin hyvin. Seuraavan kysymyksenä oli: ”järjestetäänkö yrityksenne henkilöstölle tarpeeksi kyberturvallisuuteen liittyviä koulutuksia”? Vastausvaihtoehto tähän oli 1—10 täysin eri mieltä-täysin samaa mieltä.

Viimeisenä kysymyksenä oli: ”kuinka merkityksellisenä pidätte henkilöstönne kyberturvaosaamista”? Vastausvaihtoehto tähän oli 1–10 ei ollenkaan merkityksellinen – erittäin merkityksellinen.

Alla olevassa kuviossa 13 on esitetty henkilöstöön liittyvien kysymysten tulokset. Tulokset esitetty toimialoittain.



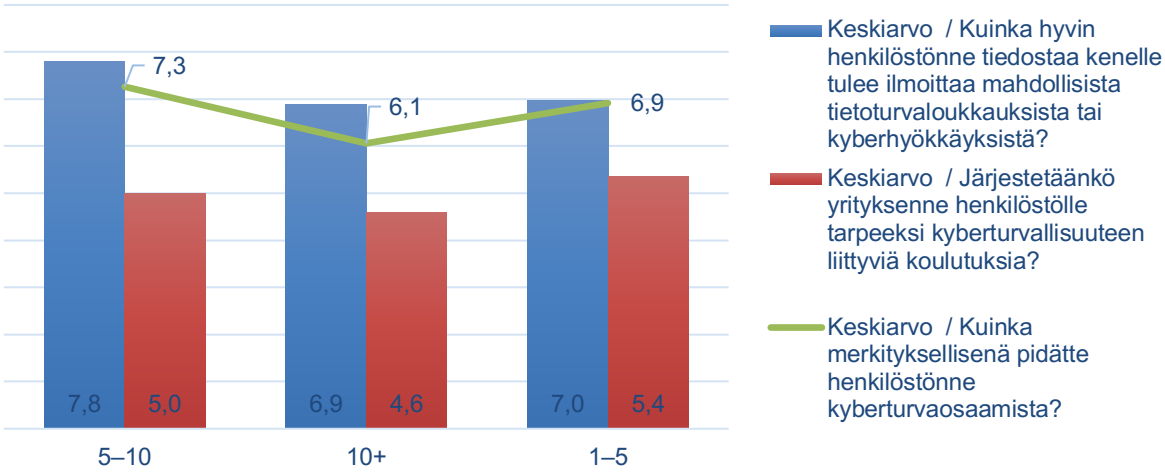
Kuvio 13. Henkilöstö ja kyberuhat toimialoittain.

Kuvion 13 perusteella voidaan todeta, että toimialana palvelut pitivät merkityksellisimpänä henkilöstön kyberturvaosaamista. Tämä oli myös linjassa sen kanssa, että palvelujen toimialan vastaajat kokivat henkilöstönsä saavan muihin toimialoihin verrattuna enemmän kyberturvallisuuteen liittyvää koulutusta sekä henkilöstö tiedostaa parhaiten kenelle mahdollisista tietoturvaloukkauksista tulee tehdä yrityksen sisällä ilmoitus. Pienimmän painoarvon henkilöstön kyberturvaosaamisella antoi selkeällä erolla muihin nähden rakentamisen toimiala. Rakentamisen toimialalla tiedostettiin myös heikoiten, kenelle tietoturvaloukkauksista tulee ilmoittaa. Huonoimman arvosanan henkilöstön kouluttamiselle antoi terveys- ja sosiaalipalveluiden toimiala.

Yrityksen henkilöstön määrän mukaan tulokset olivat lähes identtiset 1—4 työllistävien ja 5—9 työllistävien välillä, jonka puolesta niiden välinen vertailu ei tuottanut toivottua tulosta tämän tutkimuksen osalta.

Henkilöstön kyberturvaosaamiselle 1—4 henkilöä työllistävät yritykset antoivat kysymysten keskiarvoksi 6,4, kun 5—9 henkilöä työllistävien keskiarvoksi muodostui 6,3. Kyberturvallisuuden koulutuksiin liittyvään kysymykseen antoivat molemmat eri kategoriat keskiarvoksi 4,8. Tietoturvaloukkauksien ilmoittamiseen liittyvälle kysymykselle 1—4 työllistävät yritykset antoivat keskiarvoksi 7,0 ja 5—9 henkeä työllistävät 7,1.

Alla olevassa kuviossa 14 on esitetty henkilöstöön liittyvien kysymysten tulokset. Tulokset esitetty liiketoiminnan pitkäikäisyyden mukaan.



Kuvio 14. Henkilöstö ja kyberuhat liiketoiminnan pitkäikäisyyden mukaan.

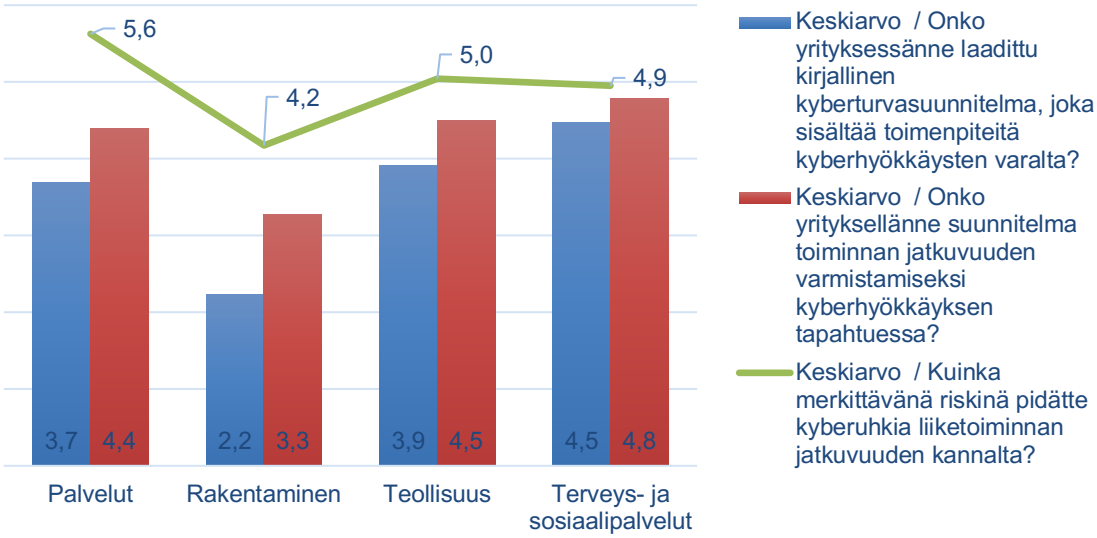
Kuviosta 14 huomataan, että yli 10 vuotta liiketoimintaa harjoittaneet yritykset antoivat pienimmän painoarvon henkilöstön kyberturvaosaamiselle 6,1 keskiarvollaan. Yli 10 vuotta liiketoimintaa harjoittaneet yritykset antoivat pienimmän keskiarvon (6,9) tietoturvaloukkauksien ilmoittamiseen liittyvälle kysymykselle sekä kyberturvallisuuden koulutuksiin liittyvälle kysymykselle keskiarvolla 4,6. Merkityksellisimpänä henkilöstön kyberturvallisuuden osaamista pitivät 7,3 keskiarvolla 5—10 vuotta liiketoimintaa harjoittaneet yritykset. 5—10 vuotta liiketoimintaa harjoittaneet yritykset antoivat myös korkeimman arvosanan (7,8) tietoturvaloukkauksien ilmoittamiseen liittyvälle kysymykselle. Parhaimman arvosanan kyberturvallisuuteen liittyvistä koulutuksista antoivat 1—5 henkilö työllistävät yritykset 5,4 keskiarvollaan.

5.5 Kyberstrategia

Liiketoiminnan jatkuvuuden näkökulmasta yrityksellä olisi hyvin tärkeää olla määritetty strategia ja käytänteet siitä, miten liiketoiminta voi jatkua ilman mahdollisesti menetettyjä resursseja sekä suunnitelma toimintakyvyn palauttamiselle samalle tasolle, kuin ennen kyberhyökkäyksen sattumista.

Kyselylomakkeessa lähdettiin selvittämään asiakkailta Likertin asteikon mukaan vastauksia kolmeen eri kysymykseen, jonka lisäksi asiakkailta kysyttiin omistaako heidän yrityksensä kybervakuutusta. Ensimmäisenä kysymyksenä esitettiin: ” kuinka merkittävänä riskinä pidätte kyberuhkia liiketoiminnan jatkuvuuden kannalta”? Vastausvaihtoehto tähän oli 1—10 ei ollenkaan merkityksellinen-erittäin merkityksellinen. Seuraavana kysymyksenä esitettiin: ”onko yrityksessänne laadittu kirjallinen kyberturvasuunnitelma, joka sisältää toimenpiteitä kyberhyökkäysten varalta”? Vastausvaihtoehto tähän oli 1—10 täysin eri mieltä-täysin samaa mieltä. Kolmantena kysymyksenä esitettiin: ” onko yrityksellänne suunnitelma toiminnan jatkuvuuden varmistamiseksi kyberhyökkäyksen tapahtuessa”? Vastausvaihtoehto tähän oli 1—10 täysin eri mieltä-täysin samaa mieltä.

Alla olevassa kuviossa 15 on esitetty kyberstrategiaan liittyvien kysymysten tulokset. Tulokset esitetty toimialan mukaan.

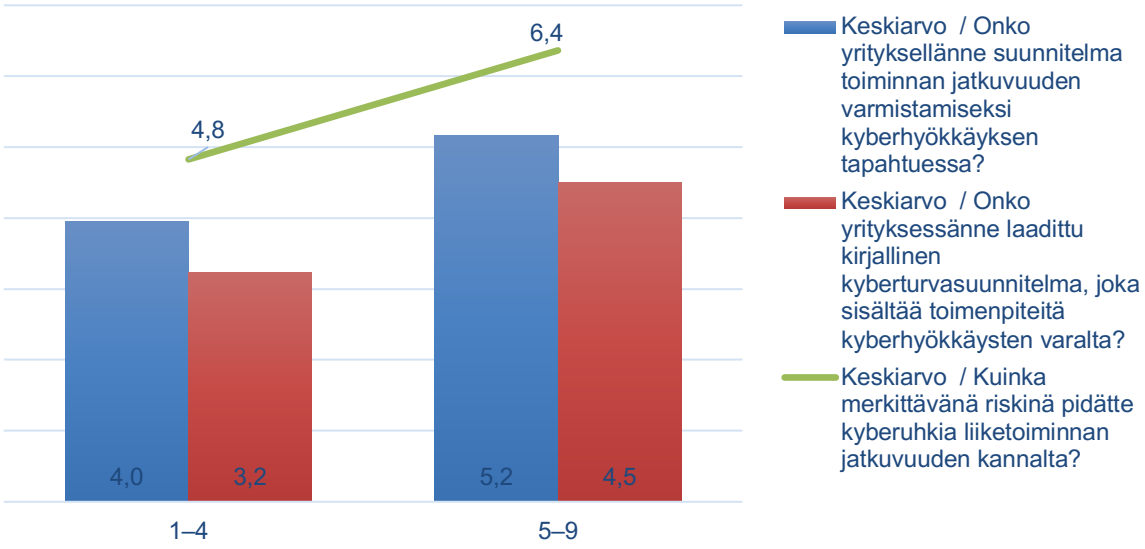


Kuvio 15. Kyberuhat ja liiketoiminnan jatkuvuus toimialoittain.

Kuvion 15 perusteella voidaan todeta, että palvelujen toimiala pitää kyberuhkia merkittävimpänä uhkana liiketoiminnan jatkuvuuden kannalta 5,6 keskiarvollaan mutta on vasta kolmantena liiketoiminnan jatkuvuuden varautumiseen puoltavien vastausten kanssa. Toimialana rakentaminen pitää kyberuhkia vertailu ryhmästään vähiten merkityksellisenä 4,2 keskiarvollaan. Rakentamisen toimialan vastaukset liiketoiminnan jatkuvuuden varmistamiseen liittyen ovat myös selkeästi alhaisempia vertailuryhmiinsä nähden. Vastausten mukaan toimialana terveys- ja sosiaalipalvelut ovat parhaiten arvioineet oman varautumisensa liiketoiminnan jatkuvuuden kannalta, mutta vastausten keskiarvoa voidaan silti pitää hyvin neutraalina.

Kybervakuutuksia oli toimialan mukaan palveluilla 6 kappaletta, rakentamisella 3 kappaletta, teollisuudella 1 kappale ja terveys- ja sosiaalipalveluilla 1 kappale.

Alla olevassa kuviossa 16 on esitetty kyberstrategiaan liittyvien kysymysten tulokset. Tulokset esitetty henkilöstön mukaan.

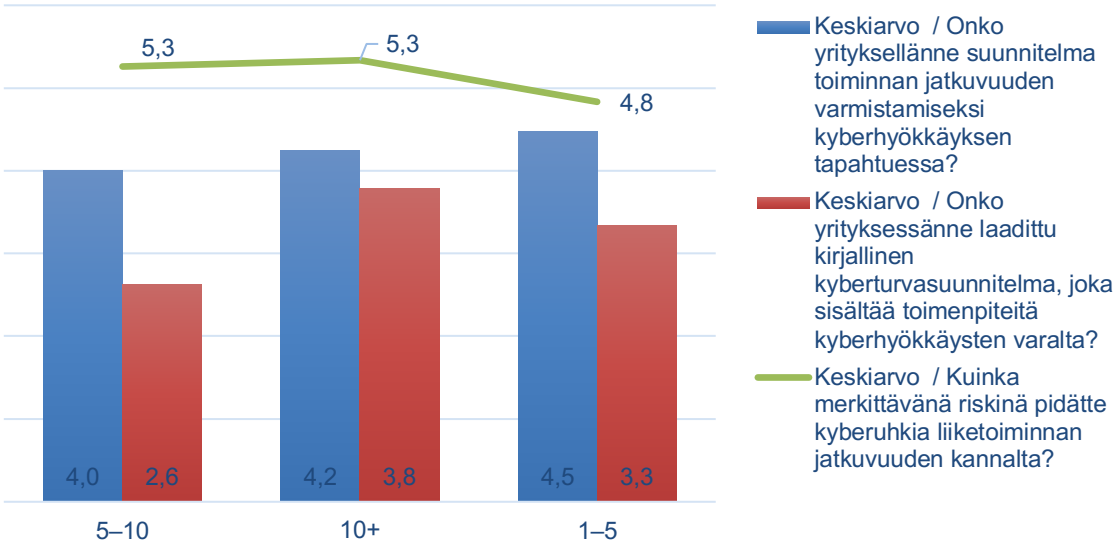


Kuvio 16. Kyberuhat ja liiketoiminnan jatkuvuus henkilöstön määrän mukaan.

Kuvion 16 perusteella voidaan todeta, että 5—9 henkilöä työllistävät yritykset pitävät kyberuhkia 6,4 keskiarvollaan merkityksellisempinä uhkina verrattuna 1—4 henkilöä työllistäviin yrityksiin. 5—9 henkilöä työllistävät yritykset antoivat myös korkeammat arvosanat liiketoiminnan jatkuvuuteen varautumiseen liittyviin kysymyksiin.

Kybervakuutuksia oli 1—4 henkilö työllistävillä yrityksillä 6 kappaletta ja 5—9 henkilöä työllistävillä yrityksillä 5 kappaletta.

Alla olevassa kuviossa 17 on esitetty kyberstrategiaan liittyvien kysymysten tulokset. Tulokset esitetty liiketoiminnan pitkäikäisyyden mukaan.



Kuvio 17. Kyberuhat ja liiketoiminnan jatkuvuus liiketoiminnan pitkäikäisyyden mukaan.

Kuviosta 17 voidaan todeta, että 1—5 vuotta liiketoimintaa harjoittaneet yritykset pitivät kyberuhkia liiketoiminnan jatkuvuuden kannalta lievimpänä uhkana 4,8 keskiarvollaan. 5—10 ja yli 10 vuotta liiketoimintaa harjoittaneet yritykset antoivat molemmat samaiselle kysymykselle keskiarvoksi 5,3. Kyberturvasuunnitelman kysymykseen antoivat 5—10 vuotta liiketoimintaa harjoittaneet yritykset poikkeuksellisen huonon tuloksen 2,6 keskiarvollaan. Parhaimman arvosanan liiketoiminnan jatkuvuuden varautumiselle kyberuhilta antoivat 1—5 vuotta liiketoimintaa harjoittaneet yritykset.

Kybervakuutuksia oli 1—5 vuotta liiketoimintaa harjoittaneilla yrityksillä 3 kappaletta ja yli 10 vuotta liiketoimintaa harjoittaneilla yrityksillä 8 kappaletta.

6 Yhteenveto

Kyberuhat lisääntyvät keskuudessamme voimakkaasti, kun kyberrikolliset koettelevat jatkuvasti julkisen sekä yksityisen sektorin riskienhallinnan resilenssiä. Tämän opinnäytetyön aihe rajattiin käsittelemään suomalaisten alle 10 henkilöä työllistävien yritysten kyberturvallisuuden nykytilaa, osana yritysten riskienhallintaa. Opinnäytetyön tutkimuskysymyksestä saatiin tehtyä yleistäviä johtopäätöksiä, joita tuon myös esiin tässä yhteenvedon kappaleessa.

Opinnäytetyössä toteutetussa kyselylomakkeessa selvitettiin kvantitatiivisten menetelmien avulla, miten lisääntyneet kyberturvallisuusriskit ovat näkyneet yritysten liiketoiminnassa ja miten niihin on varauduttu. Yritysten asenteita ja uskomuksia kyberturvallisuutta kohtaan tuo osittain esiin pelkästään se, että kyselyn vastausprosentiksi muodostui vain noin kolme prosenttia. Tutkimuksen reliabiliteetin näkökulmasta vastauksia tuli onneksi suhteessa määrällisesti paljon, kun itse kyselylomake lähetettiin verrattain suurelle massalle.

Tutkimuksessa kävi ilmi, että lähes joka kolmannes (31,6 %) vastanneista pienyrityksistä oli kohdannut liiketoiminnassaan kyberuhkia. Silti pienyritykset pitivät kyberuhkia liiketoiminnan jatkuvuuden kannalta hyvin neutraalina uhkana 5,2 keskiarvollaan. Vastanneiden hyvin neutraali suhtautuminen kyberuhkiin liittyen tuo osittain esiin myös vakuutusyhtiön näkökulmasta sen, miksi vain noin 6 prosenttia vastanneista oli siirtänyt osan kyberuhkien hallinnasta vakuutusyhtiölle, kybervakuutuksen muodossa.

Pienyritykset antoivat kyselomakkeen eri kategorioista selkeästi heikoimmat arvosanat kyberturvallisuuden strategiseen suunnitteluun liittyviin kysymyksiin. Yrityksiltä kysyttiin, että onko heidän organisaatiossansa laadittu kirjallinen kyberturvasuunnitelma, joka sisältää toimenpiteitä kyberhyökkäyksen varalta. Vastausten keskiarvo tähän kysymykseen oli koko kyselyn matalin 3,6 keskiarvolla.

Toisessa kysymyksessä yrityksiltä kysyttiin, että onko yrityksellänne suunnitelma toiminnan jatkuvuuden varmistamiseksi kyberhyökkäyksen tapahtuessa. Vastausten keskiarvoksi muodostui ainoastaan 4,3. Vastausten tulokset muodostavat huomattavan uhan pienyrityksille, koska kyberturvallisuutta ei ole selkeästi integroitu riittävän tehokkaasti osaksi yleistä riskienhallinnan suunnitelmaa.

Kyseiset tulokset ovat linjassa myös teoriaosuuden kanssa, jonka mukaan pienyrityksiin enenemissä määrin kohdistuvat hyökkäykset ovat seurausta rajallisista resursseista sekä kyvyttömyydestä käynnistää tarvittavia puolustusmenetelmiä kyberhyökkäyksen jälkeen. Opinnäytetyön mukaan pienyritysten kyberturvallisuuden hallinnointia hankaloittaa myös se, että pienyritykset kokevat yleisesti kyberturvallisuuden investoinnit harkinnanvaraisena kulueränä.

Yhtenä keskeisenä osa-alueena opinnäytetyössä tutkittiin henkilöstön roolia osana kyberturvallisuuden riskienhallintaa. Kyselylomakkeessa esitettiin yrityksille kysymys, jossa pyydettiin määrittämään se, kuinka merkityksellisenä henkilöstön kyberturvaosaamista yrityksissä pidetään. Vastausten keskiarvoksi saatiin tähän kysymykseen 6,4. Yrityksissä ei olla annettu teettämässäni kyselyssä tarpeeksi suurta painoarvoa sille, kuinka suuren kyberuhan työntekijöiden osaamisen puute voikaan aiheuttaa. Tulos on kuitenkin osittain linjassa teoriaosuudessa esitetyn vastaavanlaisen kyselytuloksen kanssa. Opinnäytetyön teoriaosuudessa esiin tuodun kyselyn mukaan 52 prosenttia vastanneista yrityksistä koki olevansa sisäisesti vaarassa, työntekijöiden heikon kyberturvaosaamisen vuoksi.

Kyselylomakkeesta saadut tulokset ja niiden pohjalta muodostettu analyysi tukevat lopullista johtopäätöstä sitä, että pienyritysten kyberuhkiin liittyvä riskienhallinta ja siihen perustuva liiketoiminnan jatkuvuuden varmistaminen ei ole nykyisellä tasolla riittävän hyvää. Mielenkiintoisia jatkotutkimusaiheita voisivat olla laadulliset kyberturvallisuuden tutkimukset, joissa pyrittäisiin syventymään entistä tarkemmin yritysten kyberturvallisuuden hallintaan liittyviin kysymyksiin sekä mahdollisiin kehitysehdotuksiin. Kyberturvallisuus osana pienyrityksen riskienhallintaa tutkimus ja siihen liittyvä prosessi oli lopulta onnistunut kokonaisuus. Oma tietämykseni kyberturvallisuuteen ja riskienhallintaan kohtaan kehittyi valtavasti tämän opinnäytetyön kirjoittamisen aikana, josta koin saavani myös valtavasti hyötyä ammattitaitoni kehittämisen näkökulmasta.

Haluan tämän työn lopussa kiittää opinnäytetyön toimeksiantajaa, joka mahdollisti tämän hyvin käytännönläheisen tutkimuksen toteuttamisen ja siihen vaadittavien resurssien järjestämisen parhaalla mahdollisella tavalla. Suuri kiitos kuuluu myös opinnäytetyöni ohjaajalle, jonka ohjeistuksen avulla pääsin tähän pisteeseen.

Lähteet

Aurelien, J. 2021. Exploring effective defensive cybersecurity strategies for small businesses. Department of Doctoral Studies. Computer Science. Colorado Technical University. Viitattu 16.02.2024. https://www.proquest.com/business/docview/2649015610/351BFBB94AA64DA9PQ/2?accountid=14446&sourcetype=Dissertations%20&%20Theses

Allianz 2024. Allianz Risk Barometer Identifying the major business risks for 2024. Viitattu 19.01.2024. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

Bander, A. S. A-R.; Mohd, A. M. & Syed, Z. M. S. 2018. Ransomware threat success factors, taxonomy, and countermeasure: A survey. Computers & Security. Vol 74, 144-145, 153.

Beagle Security 2020. Man-in-the-middle (MITM) Attack: Types, Techniques, and prevention. Viitattu 06.02.2024. https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html

Calder, A. & Gerrard, L. 2013. ISO27001/iso27002:2013: A Pocket Guide. E-kirja Ebook Central Perpetual-kirjapalvelussa. Uudistettu painos. Vaatii kirjautumisen palveluun. Viitattu 09.02.2024. https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=1463579

CISA 2021. Understanding Denial-of-Service attacks. Viitattu 29.01.2024. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

The FBI 2012. Combating threats in the cyber world. Viitattu 12.05.2024. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Hirsjärvi, S.; Remes, P. & Sajavaara, P. 2015. Tutki ja kirjoita. 20. painos. Porvoo: Bookwell Oy.

Jakobsson, M. & Myers, S. 2007. Phishing and Countermeasures: Understanding the increasing problem of electronic identity theft. New Jersey: John Wiley & Sons, Inc.

Juvonen, M.; Koskensyrjä, M.; Kuhanen, L.; Kämppi, P. & Talala, T. 2023. Yrityksen riskienhallinta. Helsinki: Aalto University Executive Education Oy.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Viro: Meedia ZOne Oü. Viitattu 13.03.2024. https://turkuamk.finna.fi/Record/turkuamk_electronic.995673481405970?sid=4164425208. Vaatii käyttäjätunnuksen.

Kaspersky Daily. 2017. The human factor in IT security: How employees are making businesses vulrenable from within. Viitattu 31.01.2024. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kaspersky Labs. 2019. What is Cyber-Security? Viitattu 26.01.2024 https://usa.kaspersky.com/resource-center/definitions/what-is- cyber-security

Kyberhyökkäys vei yrityksen koko datan kotisivuja myöten – Asiantuntijat vastaavat, onko pilvi niin turvallinen kuin on ajateltu. Viitattu 17.01.204 https://www.kauppalehti.fi/uutiset/kyberhyokkays-vei-yrityksen-koko-datan-kotisivuja-myoten-asiantuntijat-vastaavat-onko-pilvi-niin-turvallinen-kuin-on-ajateltu/c9be6ea6-9245-4933-8d51-ceddd356f304

Kyberhyökkäykset ovat nyt suurin uhka suomalaisten mielissä, tuore tutkimus paljastaa. Viitattu 17.01.2024 https://www.kauppalehti.fi/uutiset/kyberhyokkays-vei-yrityksen-koko-datan-kotisivuja-myoten-asiantuntijat-vastaavat-onko-pilvi-niin-turvallinen-kuin-on-ajateltu/c9be6ea6-9245-4933-8d51-ceddd356f304

Limnéll, J. Majewski, K. Salminen. M. & Samani, R. 2015. Cyber security for decision makers. Käännöstoimisto Pikakääntäjä. Jyväskylä: Docento.

Mallik, A. 2018. Man-In-The-Middle-Attack: Understanding in simple words: A Survey. Cyberspace: Jurnal Pendidikan Teknologi Informasi. Vol 2, 111.

Mattila, J. Ali-Yrkkö, J. & Seppälä, T. 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? Muistio. No 93, 3, 8. Viitattu 17.01.2024 https://www.etla.fi/wp-content/uploads/ETLA-Muistio-Brief-93.pdf

Merna, T. & Al-Thani F. 2008. Corporate risk management. Uudistettu painos. John Wiley & Sons, Incorporated. Viitattu 22.03.2024. https://ebookcentral.proquest.com/lib/turkuamk-ebooks/reader.action?docID=470193. Vaatii käyttäjätunnuksen.

NIST. 2022. About Nist. Viitattu 05.02.2024. https://www.nist.gov/about-nist

NIST. 2023. The Nist Cybersecurity Framework 2.0. National Institute of Standards and Technology, Gaithersburg, MD. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. Viitattu 05.02.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

OPSEC 2019. Tarvitseeko yritys tietoturvavakuutuksen. Viitattu 25.04.2024. https://www.opsec.fi/fi/2019/03/14/kuukauden-kysymys-tarvitseeko-yritys-tietoturvavakuutuksen/

Pinto, C.A. Magpili, L. & Jaradat, R.M. 2015. Operational Risk Management. New York: Momentum Press Engineering. Viitattu 21.03.2024. https://ebookcentral.proquest.com/lib/turkuamk-ebooks/reader.action?docID=4013264. Vaatii käyttäjätunnuksen.

Prümmer, J. van Steen, T. & van den Berg, B. 2024. A systematic review of current cybersecurity training methods: A survey. Computers & Security. Vol 136, 1.

Rahu, K. Rajeeb, D. Kevin, G. Arun, B. & Uday, P.S. 2024. Adaptive control for cyber-physical systems under man-in-the-middle attacks with false data injections. A survey. Journal of the Franklin Institute. Vol 361, 3.

Shimpi, P. 2001. Integrating Corporate Risk Management. New York: TEXERE LLC.

Traficom. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 17.01.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficom. 2022. Toimintaohje – Kiristyshaittaohjelma. Viitattu 31.01.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf

Wolke, T. 2017. Risk management. Berlin: De Gruyter Oldenbourg. Viitattu 04.04.2024. https://ebookcentral.proquest.com/lib/turkuamk-ebooks/reader.action?docID=5144613. Vaatii käyttäjätunnuksen.

Wen-Lung, S. Xiaoqun, W. & Fei. Z. 2023. What are the trend and core knowledge of information security? A citation and co-citation analysis. A survey. Information & Management. Vol 60, 2.