TURUN YLIOPISTO
Kauppakorkeakoulu

Pk-yritysten keinot arvioida ja hallita kyberuhkia liiketoiminnan turvaamiseksi

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija(t):
Mohamed Abdullahi

Ohjaaja(t):
KTT Hannu Salmela

7.5.2025
Helsinki

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä(t): Mohamed Abdullahi
Otsikko: Pk-yritysten keinot arvioida ja hallita kyberuhkia liiketoiminnan turvaamiseksi
Ohjaaja(t): KTT Hannu Salmela
Sivumäärä: 73 sivua + liitteet 4 sivua
Päivämäärä: 7.5.2025

Tämä pro gradu -tutkielma tarkastelee, miten pienet ja keskisuuret yritykset (pk-yritykset) arvioivat kyberhyökkäysten vaikutuksia liiketoimintaansa. Tutkimus yhdistää kirjallisuuskatsauksen ja laadullisen empiirisen aineiston, joka on kerätty puolistrukturoitujen asiantuntijahaastattelujen avulla. Tutkimuksen tavoitteena on ymmärtää, millaisia vaikutuksia erityyppisillä kyberhyökkäyksillä, kuten tietojenkalastelulla, kiristysohjelmilla ja palvelunestohyökkäyksillä on pk-yritysten talouteen, operatiiviseen toimintaan ja maineeseen, sekä miten näitä vaikutuksia pyritään arvioimaan ja hallitsemaan käytännössä.

Haastatteluiden perusteella vaikutusten arviointi pk-yrityksissä on usein hajanaista ja perustuu enemmän kokemukseen kuin systemaattisiin malleihin tai viitekehyksiin. Erityisesti tietojenkalasteluhyökkäykset nähtiin merkittävinä riskeinä, joiden torjunta vaatii panostusta työntekijöiden koulutukseen ja kyberturvallisuuskulttuurin kehittämiseen. Tutkielma korostaa myös NIST (National Institute of Standards and Technology) kyberturvallisuuskehikon tarjoamia mahdollisuuksia pk-yritysten arviointikäytäntöjen jäsentämisessä ja parantamisessa. Lopuksi esitetään suosituksia, joiden avulla pk-yritykset voivat kehittää kykyään arvioida, hallita ja toipua kyberhyökkäysten seurauksista tehokkaammin.

Avainsanat: kyberhyökkäykset, vaikutusten arviointi

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

1.1 Johdatus tutkimuksen aiheeseen

Digitalisaation ja internetin laajamittaisen käyttöönoton myötä pienet ja keskisuuret yritykset (pk-yritykset) ovat saaneet uusia mahdollisuuksia liiketoimintansa kehittämiseen ja laajentamiseen. Samalla ne ovat kuitenkin joutuneet kohtaamaan uudenlaisia uhkia, joista yksi merkittävimmistä on kyberhyökkäykset. Kyberhyökkäysten määrä ja monimutkaisuus ovat kasvaneet eksponentiaalisesti viime vuosina, mikä asettaa pk-yritykset erityisen haavoittuvaan asemaan (Bendovschi, 2015). Tämän pro gradu -tutkielman tavoitteena on tarkastella, miten pk-yritykset arvioivat kyberhyökkäysten vaikutusta liiketoimintaansa, ja mitä seurauksia niillä on yritysten toiminnalle, taloudelliselle tilanteelle ja pitkän aikavälin elinvoimaisuudelle.

Pk-yritykset ovat erityisen haavoittuvaisia kyberhyökkäyksille monista syistä. Ponsard et al. (2019) korostavat, että pk-yrityksillä on usein rajoitetut resurssit kyberturvallisuuden ylläpitämiseen, ja niiden tietoturvakäytännöt saattavat olla vähemmän kehittyneitä verrattuna suurempiin organisaatioihin. Tämä tekee niistä houkuttelevan kohteen kyberrikollisille. Pk-yritysten riippuvuus digitaalisista teknologioista tarkoittaa, että kyberhyökkäysten seuraukset voivat olla tuhoisia niiden liiketoiminnalle, aiheuttaen esimerkiksi tietojen menetyksiä, toimintahäiriöitä ja asiakassuhteiden heikkenemistä (Armenia et al., 2021).

Kyberhyökkäykset ovat monimuotoisia uhkia, jotka voivat horjuttaa pk-yritysten liiketoimintaa merkittävillä ja monitahoisilla tavoilla. Koska kyberuhkat kehittyvät jatkuvasti, niin tekevät myös niiden potentiaaliset vaikutukset yritysten toimintaan. Pk-yritysten on yhä tärkeämpää ymmärtää ja arvioida näitä riskejä paitsi säilyttääkseen toimintakykynsä, myös säilyttääkseen luottamuksen sidosryhmiensä keskuudessa. Tässä kontekstissa kyberhyökkäysten vaikutusten arvioinnin tulisi olla integraalinen osa pk-yrityksen riskienhallintastrategiaa. Romanosky (2016) analysoi kyberhyökkäysten taloudellisia seurauksia ja havaitsi, että vaikka monet hyökkäykset aiheuttavat vain vähäisiä menetyksiä, joillakin on potentiaali aiheuttaa laajamittaisia taloudellisia vahinkoja. Tämä korostaa tarvetta järjestelmälliseen lähestymistapaan, kun arvioidaan hyökkäyksen laajuutta ja vaikutusta pk-yrityksen toimintaan.

Riskienhallinnan näkökulmasta kyberhyökkäysten vaikutusten arvioinnissa on huomioitava niin välittömät kuin välilliset seuraukset. On tunnustettu, että vaikutukset eivät rajoitu pelkästään taloudellisiin menetyksiin, vaan ne voivat ulottua liiketoiminnan keskeytymisestä ja mainehaitasta aina asiakasdatan menetykseen (Huang et al., 2018). Siksi pk-yritysten tulisi ottaa huomioon kokonaisvaltainen näkemys kyberhyökkäysten vaikutuksista, mukaan lukien menetetty liiketoiminta ja asiakassuhteiden heikkeneminen (Cavusoglu et al., 2004).

Kyberturvallisuuden maturiteetin kehittäminen on toinen keskeinen tekijä kyberhyökkäysten vaikutusten arvioinnissa. Pk-yritysten tulee investoida paitsi ennaltaehkäiseviin turvatoimiin, myös kykyynsä vastata ja palautua hyökkäyksistä. Investoinnit kyberturvallisuuteen tuottavat parhaimmillaan taloudellisen kasvun, kun ne estävät vakavien rikkomusten ja tietoturvaloukkausten kustannukset. (Collier & D'Anna, 2023).

Standardit ja viitekehykset, kuten NIST:n kyberturvallisuuskehikko, tarjoavat arvokkaita välineitä kyberhyökkäysten vaikutusten arviointiin. Ne tarjoavat yhtenäisen lähestymistavan, jonka avulla pk-yritykset voivat kehittää ja sovittaa kyberturvallisuustoimenpiteensä yhteen liiketoimintaprosessiensa kanssa (NIST, 2018). Standardien noudattaminen voi myös tuoda mukanaan sivuvaikutuksena lisääntynyttä luottamusta asiakkaiden ja liikekumppaneiden keskuudessa, jotka pitävät tietoturvaa yhä tärkeämpänä liiketoimintakumppaneidensa valinnassa.

Vaikutusten arvioinnissa on otettava huomioon myös kyberhyökkäysten psykologiset ja organisatoriset seuraukset. Työntekijöiden tietoturvatietoisuus ja käyttäytyminen ovat keskeisiä tekijöitä kyberturvallisuusriskien hallinnassa, ja niiden rooli on korostunut viimeaikaisessa kirjallisuudessa (Hadlington, 2017). Pk-yritysten on tärkeää edistää turvallisuuskulttuuria, jossa työntekijät ymmärtävät kyberuhkien luonteen ja heidän roolinsa niiden torjunnassa.

Pk-yritykset eivät voi jättää huomiotta kyberhyökkäysten vaikutuksia. Toimialasta riippumatta on välttämätöntä arvioida säännöllisesti kyberuhkien aiheuttamia riskejä ja niiden potentiaalisia vaikutuksia liiketoimintaan. Tämä tutkielma pyrkii asettamaan perustan laajemmalle keskustelulle siitä, miten pk-yritykset voivat lähestyä kyberhyökkäysten vaikutusten arviointia strategisesti ja operatiivisesti, ottaen huomioon

moninaiset ja usein ristiin menevät vaikutukset, joita kyberhyökkäykset voivat aiheuttaa.

Tutkielmassa käsitellään erityyppisiä kyberhyökkäyksiä, kuten haittaohjelmia, phishing-hyökkäyksiä ja palvelunestohyökkäyksiä, ja analysoidaan niiden erityisiä vaikutuksia pk-yrityksiin. Kyberhyökkäysten lisäksi tutkielma pyrkii tarjoamaan kattavan kuvauksen kyberhyökkäysten moninaisista vaikutuksista pk-yrityksiin ja esittelemään keinoja, joilla yritykset voivat valmistautua ja minimoida näiden hyökkäysten aiheuttamat vahingot. Tämän lisäksi teoriaosuudessa tarkastellaan myös keinoja, millä yritykset arvioivat heidän liiketoimintamenetyksiään kyberhyökkäysten jälkeen.

Kyberhyökkäysten merkitys ja vaikutus modernissa liiketoimintaympäristössä on noussut keskeiseksi huolenaiheeksi organisaatioille ympäri maailmaa. Teknologian kehittyessä ja digitalisaation syvetessä, organisaatiot kohtaavat yhä monimutkaisempia kyberturvallisuuden haasteita, jotka voivat uhata niiden taloudellista vakautta, mainetta ja operatiivista tehokkuutta. Kyberhyökkäysten vaikutukset eivät rajoitu pelkästään välittömiin taloudellisiin menetyksiin, kuten varastettuihin varoihin tai lunnasvaatimuksiin. Niiden laajemmat seuraukset voivat ulottua asiakassuhteiden heikkenemiseen, markkina-aseman menetykseen, ja jopa pitkäaikaiseen mainehaittaan. Lisäksi nämä hyökkäykset voivat aiheuttaa vakavia operatiivisia häiriöitä, jotka keskeyttävät päivittäiset toiminnot ja voivat vaikuttaa merkittävästi organisaation kykyyn palvella asiakkaitaan (Uma ja Padmavathi, 2013).

1.2 Tutkimuskysymykset, tavoitteet ja teoreettinen viitekehys

Tutkimuksen tavoitteena on ollut selvittää, miten pk-yritykset arvioivat ja hallitsevat kyberhyökkäysten uhkia liiketoimintansa turvaamiseksi. Koska kyberhyökkäykset ja tietoturvaratkaisut kehittyvät jatkuvasti, yritysten on tärkeää arvioida omaa kyberturvallisuusstrategiaansa ja huolehtia sen jatkuvasta ylläpidosta ja kehittämisestä vastaamaan muuttuvia uhkia. Tutkimuksen pääkysymys on:
Miten pk-yritykset arvioivat kyberhyökkäysten vaikutuksia ja hallitsevat uhkia liiketoimintansa turvaamiseksi?

Tutkimuksen pääkysymyksenä on selvittää, miten pk-yritykset arvioivat ja hallitsevat kyberhyökkäysten uhkia liiketoimintansa turvaamiseksi. Tarkastelun kohteena ovat sekä hyökkäysten aiheuttamat taloudelliset ja maineeseen kohdistuvat vaikutukset, että

yritysten käytännön toimenpiteet kyberturvallisuuden suojaamiseksi ja vahinkojen minimoimiseksi hyökkäystilanteissa.

1.3 Tutkielman toteutus, rakenne ja metodologia

Tämän pro gradu -tutkielman ydin koostuu laadullisesta haastattelututkimuksesta sekä kattavasta kirjallisuuskatsauksesta, jotka yhdessä muodostavat monipuolisen ja syvällisen analyysin kyberhyökkäysten vaikutuksesta organisaation liiketoimintaan. Kirjallisuuskatsauksessa tarkastellaan laajasti olemassa olevaa tutkimusta kyberhyökkäysten vaikutuksista, mukaan lukien aiheeseen liittyvät teoriat, empiiriset tutkimukset ja tapaustutkimukset. Tämä antaa perustan tutkimukselle, jossa kyberhyökkäysten moninaisia vaikutuksia organisaatioihin voidaan ymmärtää ja tarkastella laajemmassa kontekstissa.

Laadullinen haastattelututkimus toteutetaan puolistrukturoituina haastatteluina, joissa on tarkoitus saada syvempi ymmärrys siitä, miten organisaatiot kokevat ja käsittelevät kyberhyökkäyksiä. Haastatteluiden tavoitteena on selvittää, miten kyberhyökkäykset vaikuttavat organisaatioiden päivittäiseen toimintaan, strategisiin päätöksiin, taloudelliseen tilanteeseen ja maineeseen. Haastatteluista saatu data analysoidaan deduktiivisesti kirjallisuuden avulla.

Tutkielman rakenne on suunniteltu tukemaan näitä metodologisia valintoja. Alkuvaiheessa kirjallisuuskatsauksella luodaan perusta tutkimukselle, minkä jälkeen siirrytään haastattelujen yksityiskohtaiseen analyysiin. Analyysivaiheessa keskitytään haastatteluista nousseiden keskeisten teemojen tunnistamiseen ja niiden yhdistämiseen kirjallisuuskatsauksessa esitettyihin aiheisiin ja teorioihin. Lopuksi tutkimuksen yhteenveto ja johtopäätökset tarjoavat kuvan siitä, miten kyberhyökkäykset vaikuttavat organisaation liiketoimintaan, sekä suosituksia ja näkemyksiä tulevaisuuden tutkimuksen suuntaviivoiksi.

Tämän metodologisen lähestymistavan avulla tutkimus kykenee tarjoamaan syvällisen näkemyksen kyberhyökkäysten vaikutuksista, yhdistäen empiirisen datan ja teoreettisen tiedon. Lähestymistapa mahdollistaa kyberhyökkäysten vaikutusten ymmärtämisen sekä organisaation sisäisestä että ulkoisesta näkökulmasta, tarjoten kattavan analyysin ajankohtaisesta ja monimutkaisesta aiheesta.

2 Mitä kyberhyökkäykset ovat?

2.1 Taustaa

Kyberhyökkäykset ovat muodostuneet yhdeksi suurimmista uhista digitaalisessa maailmassa, ja niiden vaikutus ulottuu yksilötasolta kansainväliseen turvallisuuteen. Niiden monimuotoisuus, jatkuvasti kehittyvä luonne ja kyky aiheuttaa laajamittaisia häiriöitä tekevät niistä erityisen vaarallisia. Kyberhyökkäysten taustalla vaikuttavat motiivit vaihtelevat, mutta niitä yhdistää kyky kohdistaa hyökkäyksiä digitaaliseen infrastruktuuriin taloudellisen hyödyn saavuttamiseksi, tiedustelutiedon keräämiseksi, poliittisen vaikuttamisen välineenä tai pelkän tuhon aiheuttamiseksi (Kyberturvallisuuskeskus, 2019).

Pk-yritykset ovat keskeisessä asemassa sekä Suomen että globaalin talouden kehityksessä. Niiden rooli kansantaloudessa on erityisen merkittävä, sillä ne edistävät työllisyyttä, paikallista talouskasvua ja innovaatioita (Elinkeinoelämän keskusliitto, 2024).

Taulukko 1 Kyberhyökkäysten tyypit ja vaikutukset pk-yrityksiin

	Kyberhyökkäystyyppi	Keskeinen motiivi	Tavallinen hyökkäyskeino	Vaikutukset pk-yrityksille
1	Kiristysohjelmat (Ransomware)	Taloudellinen hyöty (lunnaiden vaatiminen)	Tietojenkalastelu	Liikettoiminnan keskeytykset, mainehaitat,
2	Palvelunestohyökkäykseet (DDoS)	Palvelun häirintä tai kiristys	Verkkoliikenteen ylikuormittaminen bottiverkolla	Verkkosivustojen kaatuminen, asiakastyytymättömyys, lunnasvaatimukset
3	Tietojenkalastellu (Phishing))	Tietojen hankkiminen huijaamalla käyttäjää	Sähköpostit, huijauslinkit, sosiaalinen manipulointi	Tunnusten varkaus, tietomurrot, luottamuksen menetys
4	Troijalaiset	Luvaton pääsy ja tietojen varastaminen	Laaja verkkohäiriö palveluihin käyttämällä IoT-laitteita	Järjestelmän haltuunotto, tietovuodot, lisähaittaohjelmien asennus

Taloudellinen hyöty on yksi keskeisimmistä syistä kyberhyökkäysten taustalla. Kiristysohjelmat, kuten WannaCry, ovat esimerkkejä laajamittaisista hyökkäyksistä,

joissa uhrin tiedostot lukitaan ja niiden vapauttamisesta vaaditaan lunnaita. Tällaiset hyökkäykset aiheuttavat suoraa taloudellista vahinkoa, mutta myös laajempia toiminnallisia häiriöitä ja luottamuksen menetystä digitaalisiin järjestelmiin (Chen & Bridges, 2017).

Ransomware-hyökkäykset ovat nousseet yhdeksi suurimmista kyberuhkista pk-yrityksille. Haittaohjelmat, kuten WannaCry ja Netwalker, ovat aiheuttaneet merkittäviä liiketoiminnan keskeytyksiä ympäri maailmaa (Kapoor et al., 2021). Pk-yritykset ovat erityisen haavoittuvia, koska niillä ei usein ole kattavia varmuuskopiointijärjestelmiä tai riittäviä tietoturvaratkaisuja, mikä tekee niistä houkuttelevia kohteita (Kapoor et al., 2022). Vuonna 2020 lähes 51 % maailmanlaajuisista organisaatioista joutui ransomware-hyökkäyksen kohteeksi, mikä korostaa ilmiön vakavuutta myös pienempien yritysten osalta (Dhwana & Narwal, 2029). Lisäksi ransomware hyödyntää usein sosiaalisen manipuloinnin keinoja, kuten tietojenkalastelua, mikä vaikeuttaa torjuntaa erityisesti henkilöstön puutteellisten kyberturvallisuustaitojen vuoksi.

Palvelunestohyökkäykset (DDoS), kuten Dyn DNS -palveluun kohdistunut hyökkäys vuonna 2016, osoittavat, kuinka hyökkääjät voivat ylikuormittaa verkkopalveluita aiheuttaen merkittäviä käyttökatkoja ja taloudellisia tappioita. DDoS-hyökkäykset ovat myös merkittävä uhka pk-yrityksille: hyökkäyksissä yrityksen verkkosivusto tai palvelin tukitaan liikenteellä, jolloin palvelu estyy tilapäisesti tai pysyvästi (Snehi & Bhandari, 2021). Pk-yritykset ovat erityisen haavoittuvia näille hyökkäyksille, koska niillä ei usein ole riittävää infrastruktuuria tai osaamista puolustautua tehokkaasti. Hyökkäyksen seurauksena liiketoiminta voi keskeytyä useiksi tunneiksi tai päiviksi, mikä vähentää asiakasluottamusta ja aiheuttaa pitkäaikaisia mainehaittoja. Joissakin tapauksissa hyökkääjät vaativat myös lunnaita palvelunestohyökkäysten lopettamiseksi, mikä liittää ne kiristyshyökkäyksiin (Kyberturvallisuuskeskus, 2022).

Tietojenkalastelu (phishing) on yksi yleisimmistä ja tehokkaimmista keinoista, joilla hyökkääjät pyrkivät saamaan haltuunsa yritysten ja työntekijöiden arkaluonteisia tietoja, kuten kirjautumis- ja maksutietoja. Pk-yritykset ovat erityisen alttiita phishing-hyökkäyksille puutteellisen kyberturvallisuuskoulutuksen ja kehittymättömien tietoturvakäytäntöjen vuoksi. Phishing-hyökkäykset yleistyivät pandemian aikana, kun yritykset siirtyivät nopeasti digitaalisiin työkaluihin ilman riittäviä tietoturvatoimia. ENISA:n mukaan tietojenkalastelu on yleisin kyberhyökkäys pk-yrityksiä vastaan, ja se

voi johtaa vakaviin seurauksiin, kuten taloudellisiin menetyksiin ja mainehaittoihin (ENISA, 2020). Phishing-hyökkäykset tähtäävät henkilökohtaisten tai taloudellisten tietojen paljastamiseen, mikä voi johtaa identiteettivarkauksiin ja taloudellisiin tappioihin (Jansson & von Solms, 2011). Troijalaiset, kuten Zeus ja TrickBot, ovat esimerkkejä haittaohjelmista, jotka on suunniteltu varastamaan pankkitietoja ja muita arkaluonteisia tietoja (Grammatikakis et al., 2021).

Troijalaiset ovat haittaohjelmia, jotka naamioituvat laillisilta vaikuttaviksi sovelluksiksi mutta antavat hyökkääjille pääsyn yrityksen järjestelmiin. Ne voivat aiheuttaa vakavaa vahinkoa varastamalla kriittisiä tietoja tai manipuloimalla järjestelmiä. Troijalaiset voivat myös levittää muita haittaohjelmia yrityksen verkkoon, mikä tekee niistä erityisen vaarallisia pk-yrityksille, joilla ei ole resursseja tehokkaaseen puhdistukseen. Esimerkiksi Djvu-troijalainen on aiheuttanut viime vuosina merkittäviä vahinkoja, hyödyntäen edistyneitä salaustekniikoita ja vaikeuttaen hyökkäysten havaitsemista (Kapoor et al., 2022).

Kyberhyökkäysten torjunta edellyttää jatkuvaa valppautta, kehittyneitä teknologisia ratkaisuja ja kansainvälistä yhteistyötä. Valtioiden, yritysten ja yksilöiden on tehtävä tiivistä yhteistyötä kehittääkseen kestäviä kyberturvallisuusstrategioita, jotka suojaavat digitaalista infrastruktuuria ja vähentävät hyökkäysten aiheuttamia vahinkoja. Koulutus ja tietoisuuden lisääminen ovat keskeisiä tekijöitä kyberrikollisuuden torjunnassa, sillä ne auttavat yksilöitä tunnistamaan ja välttämään potentiaalisia uhkia (NIST, 2018).

2.2 Kyberhyökkäysten tyypit

2.2.1 Kiristysohjelmat (ransomware)

Kiristysohjelmat (ransomware) ovat nousseet yhdeksi merkittävimmistä uhista digitaalisen maailman yrityksille ja yksityishenkilöille. Näiden haittaohjelmien ensisijainen tarkoitus on salata uhrin tiedot tai estää pääsy tärkeisiin tiedostoihin ja vaatia lunnaita tietojen palauttamiseksi. Kiristysohjelmat voidaan jakaa kahteen päätyyppiin: salauskiristysohjelmiin (crypto-ransomware) ja lukituskiristysohjelmiin (locker-ransomware). Salauskiristysohjelmat, kuten WannaCry ja CryptoLocker, käyttävät vahvaa salausta (esim. AES tai RSA) lukitakseen uhrin tiedot, tehden niistä käyttökelvottomia ilman oikeaa purkuavainta. Tietojen palautus edellyttää lunnaita, usein kryptovaluutassa, kuten Bitcoinissa (Dhawan & Narwal, 2019).

Lukituskiristysohjelmat puolestaan estävät pääsyn laitteeseen tai järjestelmään lukitsemalla sen, mutta eivät varsinaisesti salaa tiedostoja.

Ransomware-hyökkäykset käyttävät usein kaksoiskiristystä (double extortion), jossa tietojen salaamisen lisäksi uhkaillaan tiedostojen julkistamisella, ellei lunnaita makseta. Tämä strategia lisää merkittävästi painetta uhrille, erityisesti yrityksille, joiden arkaluonteisten tietojen vuotaminen voisi johtaa merkittäviin mainehaittoihin tai oikeudellisiin seurauksiin (Kumar & Shukla, 2023).

Kiristysohjelmat leviävät useilla eri tavoilla, joista yleisimpiä ovat:

Tietojenkalastelu (Phishing): Yleisin tapa levittää kiristysohjelmia on lähettää uhreille huijausviestejä, jotka näyttävät tulevan luotetuilta tahoilta. Näissä viesteissä on liitteitä tai linkkejä, jotka käynnistävät kiristysohjelman lataamisen ja asentamisen uhrin koneelle. Netwalker-kiristysohjelma hyödynsi pandemiaan liittyviä huijauksia kalastellessaan COVID-19-aiheisia sähköposteja (Kapoor et al., 2022).

Drive-by Download -hyökkäykset: Näissä hyökkäyksissä uhrin ei tarvitse tehdä muuta kuin vierailla vaarallisella verkkosivustolla, jonka kautta haittaohjelma asentuu automaattisesti ilman, että käyttäjä huomaa sitä. Hyökkääjät käyttävät hyväkseen verkkoselainten haavoittuvuuksia (Razaulla et al., 2023).

Etätyöpöytäprotokolla (RDP): Heikosti suojatut RDP-yhteydet mahdollistavat kiristysohjelmien asentamisen suoraan kohdejärjestelmään. Tämä levitystapa on yleistynyt erityisesti kohdennetuissa hyökkäyksissä, joissa pyritään ottamaan haltuun yrityksen kriittisiä järjestelmiä (Wang et al., 2018).

Liiketoiminnan keskeytykset ovat toinen merkittävä seuraus. Monille yrityksille jokainen tunti offline-tilassa voi tarkoittaa merkittäviä tulonmenetyksiä. Pk-yritykset ovat erityisen haavoittuvia, sillä niillä ei usein ole kehittyneitä varajärjestelmiä tai kattavaa tietoturvaa, joka mahdollistaisi nopean palautumisen hyökkäyksen jälkeen (Dhawan & Narwal, 2019). Lisäksi tietojen menetys voi olla pysyvä, jos varmuuskopioita ei ole tai ne on myös saastutettu. Tämän seurauksena yrityksen kyky jatkaa toimintaansa voi vaarantua. Mainehaitat voivat olla vieläkin vakavampia, erityisesti yrityksille, jotka käsittelevät arkaluonteisia tietoja, kuten terveydenhuolto- ja finanssialan yritykset (Hampton et al., 2018).

Kiristysohjelmilta suojautuminen vaatii monitasoisen lähestymistavan. Yksi tehokkaimmista keinoista on säännöllinen varmuuskopiointi, joka mahdollistaa tietojen palauttamisen ilman, että lunnaita tarvitsee maksaa. Varautuminen on kuitenkin usein puutteellista pk-yrityksissä, mikä tekee niistä erityisen haavoittuvia (Kapoor et al., 2022).

Koulutus on toinen tärkeä puolustuskeino. Koska monet kiristysohjelmat leviävät tietojenkalastelun kautta, työntekijöiden kouluttaminen tunnistamaan huijausviestit on olennaista hyökkäysten ehkäisyssä. Lisäksi yritysten tulisi ottaa käyttöön monivaiheinen tunnistautuminen ja verkon segmentointi, jotka voivat rajoittaa haittaohjelman leviämistä ja estää hyökkääjien pääsyn kriittisiin järjestelmiin (Ayesha et al., 2020).

Ransomware-hyökkäysten havaitseminen ja torjuminen on haasteellista, sillä monet nykyaikaiset kiristysohjelmat käyttävät kehittyneitä häivetekniikoita, kuten polymorfiaa ja salattuja C2 (komento- ja ohjaus) -palvelimia. Tutkimukset ovat kuitenkin osoittaneet, että koneoppimista hyödyntävät järjestelmät voivat tunnistaa epäilyttävän käyttäytymisen ja estää haittaohjelmien leviämisen tehokkaammin kuin perinteiset suojausmenetelmät (Kapoor et al., 2022).

Ransomware on nopeasti kehittyvä uhka. Viime vuosina on nähty merkittäviä muutoksia kiristysohjelmien toimintatavoissa, kuten Crimeware-as-a-Service (CaaS) -mallin yleistyminen, jossa kyberrikolliset tarjoavat haittaohjelmia vuokrattaviksi (Daraghi et al., 2019). Tämä malli tekee kiristysohjelmien käytön entistä helpommaksi myös sellaisille hyökkääjille, joilla ei ole teknistä osaamista. Pandemia on edelleen lisännyt ransomware-hyökkäysten määrää, erityisesti terveydenhuollossa ja etätyötä tekevissä yrityksissä (Razaulla et al., 2023). Tulevaisuudessa on todennäköistä, että hyökkäykset muuttuvat yhä kehittyneemmiksi, kohdistuen erityisesti kriittiseen infrastruktuuriin, kuten energia- ja terveydenhuoltoalalle.

Kiristysohjelmat ovat nopeasti kehittyvä ja erittäin tuhoisa kyberuhka, joka kohdistuu sekä yksityishenkilöihin että yrityksiin. Sen leviämismenetelmät ovat moninaisia, ja vaikutukset voivat olla katastrofaalisia, jos tietoturvatoimenpiteitä ei ole riittävästi. Tehokas suojautuminen vaatii varmuuskopiointia, koulutusta ja uusien teknologioiden, kuten tekoälyn ja koneoppimisen hyödyntämistä. Koska kiristysohjelmat kehittyvät jatkuvasti, on tärkeää, että yritykset pysyvät ajan tasalla ja ottavat käyttöön ajantasaisia suojausstrategioita.

2.2.2 Palvelunestohyökkäykset (DoS)

Palvelunestohyökkäykset (Denial of Service, DoS) ja jaetut palvelunestohyökkäykset (Distributed Denial of Service, DDoS) ovat merkittäviä ja yleistyviä kyberuhkia, joiden vaikutukset voivat olla tuhoisia niin organisaatioille kuin julkisille palveluille. Tällaiset hyökkäykset tähtäävät siihen, että kohdepalvelin, -verkkosivusto tai muu palvelu tehdään käyttökelvottomaksi tai sen suorituskykyä heikennetään vakavasti lähettämällä sille valtava määrä pyyntöjä, joita se ei pysty käsittelemään normaalisti. Nämä hyökkäykset voivat tapahtua monella eri tavalla ja hyödyntää monenlaisia teknisiä haavoittuvuuksia, mikä tekee niistä monimuotoisia ja vaikeasti torjuttavia (Snehi & Bhandari, 2021).

Palvelunestohyökkäyksissä keskeistä on ylikuormittaa kohdejärjestelmän resursseja tavalla, joka estää sen normaalin toiminnan. Yksi yksinkertaisimmista tavoista on suoraviivainen verkkoliikenteen lisääminen: hyökkääjä lähettää valtavan määrän verkkopyyntöjä, jotka ylittävät kohteen käsittelykapasiteetin. Tällöin palvelin ei enää pysty vastaamaan laillisille käyttäjille, jolloin koko palvelu voi kaatua. SYN-flood-hyökkäys on esimerkki tällaisesta perusmenetelmästä. Siinä hyödynnetään Transmission Control Protocolin (TCP) kolmivaiheista yhteydenmuodostusprosessia, jossa palvelimelle lähetetään suuri määrä SYN-pyyntöjä ilman aikomusta suorittaa koko yhteyttä loppuun. Tämä johtaa siihen, että palvelin käyttää resurssejaan turhiin yhteyksiin, mikä ylikuormittaa sen (Feigenbaum et al., 2007; Ghazali & Hassan, 2011).

DDoS-hyökkäyksillä voi olla merkittäviä taloudellisia, toiminnallisia ja jopa yhteiskunnallisia vaikutuksia. Taloudelliset tappiot voivat syntyä suoraan tulojen menetyksenä, jos verkkopalvelut ovat poissa käytöstä. Esimerkiksi verkkokaupoille jokainen hyökkäyksen aiheuttama seisokki merkitsee suoraan menetettyjä myyntejä. Lisäksi palvelunestohyökkäykset voivat aiheuttaa suuria taloudellisia tappioita esimerkiksi korjauskustannusten, tietoturvapäivitysten ja lisäresurssien muodossa (Ghazali & Hassan, 2011).

Kuitenkin taloudelliset vaikutukset eivät ole ainoat merkittävät seuraukset. Palvelunestohyökkäykset voivat myös heikentää yrityksen tai organisaation mainetta ja asiakasluottamusta. Asiakkaat saattavat menettää uskonsa yrityksen kykyyn ylläpitää turvallisia ja toimivia palveluja, mikä voi johtaa pitkäkestoisiin mainehaittoihin. Erityisesti finanssialan yritykset, kuten pankit ja maksupalvelut, voivat kokea mittavia

vahinkoja, jos niiden palvelut kaatuvat hyökkäysten vuoksi (Feigenbaum et al., 2007; Garcia-Teodoro et al., 2009). Tällöin asiakassuhteiden menetykset voivat olla vakavia ja pitkäkestoisia, mikä pahentaa taloudellisia tappioita entisestään. Lisäksi palvelunestohyökkäykset voivat aiheuttaa laajoja yhteiskunnallisia häiriöitä, erityisesti jos ne kohdistuvat julkisiin palveluihin tai kriittiseen infrastruktuuriin, kuten sähkö- tai vesiverkkoihin. Esimerkiksi julkiset terveydenhuoltopalvelut tai energiantoimittajat voivat joutua massiivisten hyökkäysten kohteeksi, mikä voi aiheuttaa laajamittaisia häiriöitä koko yhteiskunnalle (Adedeji et al., 2023). Yksi esimerkki tällaisesta oli vuoden 2016 Mirai-hyökkäys, joka aiheutti suuria häiriöitä julkisissa verkkopalveluissa, mukaan lukien valtionhallinnon sivustot ja kansalliset infrastruktuurit.

Palvelunestohyökkäysten torjunta on erityisen haastavaa, koska ne voivat käyttää useita eri menetelmiä ja niiden kohteena voi olla monimutkaisia verkkoinfrastruktuureja. Eräs keskeinen torjuntamenetelmä on anomaly-pohjainen havaitseminen, jossa verkon liikennettä analysoidaan jatkuvasti ja epänormaalit liikennepiikit havaitaan ja käsitellään ennen kuin ne ehtivät aiheuttaa merkittävää vahinkoa (Garcia-Teodoro et al., 2009). Tämänkaltaiset järjestelmät pystyvät tunnistamaan epätavallisen liikenteen ja voivat estää sen, mutta ne eivät ole täydellisiä, koska hyökkäykset voivat käyttää monimutkaisia ja hajautettuja lähestymistapoja liikenteen naamioimiseen.

Viime vuosina tekoäly ja koneoppiminen ovat nousseet tärkeiksi työkaluiksi palvelunestohyökkäysten torjunnassa. Nämä teknologiat voivat analysoida suuria määriä liikennettä ja tunnistaa epäilyttävän käyttäytymisen reaaliaikaisesti. Koneoppimiseen perustuvat järjestelmät pystyvät oppimaan ja mukautumaan jatkuvasti uusiin uhkiin, mikä tekee niistä tehokkaampia erityisesti silloin, kun hyökkäykset muuttuvat ja kehittyvät (Cloudflare, 2014). Lisäksi pilvipohjaiset DDoS-suojausratkaisut ovat yleistyneet. Ne tarjoavat hajautettuja ratkaisuja, jotka voivat jakaa hyökkäyksien aiheuttaman liikenteen useiden palvelimien kesken, mikä vähentää yhden palvelimen ylikuormitusta ja suojaa sitä vakavilta hyökkäyksiltä. Palvelunestohyökkäykset ovat kuitenkin niin monimutkaisia ja laajoja, että yksittäinen puolustusmekanismi ei usein riitä niiden torjuntaan. On tärkeää käyttää useita erilaisia torjuntamenetelmiä yhdessä, kuten reaaliaikaista liikenteen analysointia, poikkeamien havaitsemista, hajautettuja järjestelmiä ja monitasoista suojausta. Koska hyökkäykset kehittyvät jatkuvasti, myös puolustusjärjestelmien on pysyttävä ajan tasalla ja mukaututtava uusiin uhkiin (Feigenbaum et al., 2007; Garcia-Teodoro et al., 2009).

DDoS-hyökkäykset ovat erityisen huolestuttavia tulevaisuuden kannalta, koska ne voivat kohdistua uusiin teknologioihin, kuten esineiden internetiin (IoT) ja muihin kehittyneisiin digitaalisiin infrastruktuureihin. IoT-laitteet, kuten älykodit ja teollisuusautomaatiojärjestelmät, ovat alttiita hyökkäyksille, koska monet niistä ovat heikosti suojattuja ja niitä on helppo väärinkäyttää osana bottiverkkoja (Adedeji et al., 2023). Tämä lisää entisestään palvelunestohyökkäysten riskiä, erityisesti koska IoT-laitteiden määrä kasvaa jatkuvasti ja niiden käyttö laajenee yhteiskunnan eri osa-alueilla.

Palvelunestohyökkäyksissä käytettävät taktiikat voivat olla yksinkertaisia tai erittäin monimutkaisia. Yksinkertaisimmillaan hyökkääjä voi käyttää laitetta lähettääkseen suuren määrän pyyntöjä kohdepalvelimelle, joka ylikuormittuu ja kaatuu. Tyypillinen esimerkki on SYN-flood-hyökkäys, jossa käytetään hyväksi TCP-protokollan yhteydenmuodostusta (Feigenbaum et al., 2007). SYN-floodissa palvelimelle lähetetään jatkuvasti yhteyspyyntöjä ilman tarkoitusta päättää yhteyttä, jolloin palvelin kuluttaa resurssejaan yrittäessään ylläpitää näitä yhteyksiä, kunnes se ylikuormittuu.

Palvelunestohyökkäysten laajamittaisempi versio, DDoS, hyödyntää hajautettua verkkoa tai bottiverkkoa, jossa on suuri määrä laitteita, jotka samanaikaisesti hyökkäävät kohteeseen. Tällainen hyökkäys on huomattavasti vaikeampi torjua, koska se voi käyttää kymmeniä, satoja tai jopa tuhansia laitteita ympäri maailmaa (Adedeji et al., 2023). Yksi tunnetuimmista DDoS-hyökkäyksistä oli Mirai-bottiverkon hyökkäys vuonna 2016, joka kohdistui valtavaan määrään IoT-laitteita ja aiheutti suuria häiriöitä internetin toimintaan, mukaan lukien suurten verkkosivustojen ja palveluiden kaatuminen (Cloudflare, 2014).

DDoS-hyökkäyksissä voidaan käyttää monia eri taktiikoita. Esimerkiksi ICMP-flood hyödyntää Internet Control Message Protocol -protokollaa lähettämällä kohdepalvelimelle suuria määriä ICMP-pyyntöjä, jolloin palvelimen kapasiteetti ylittyy. Toinen esimerkki on DNS-amplifikaatiohyökkäys, jossa hyökkääjä lähettää pieniä DNS-kyselyjä, jotka generoivat huomattavasti suurempia vastauksia, ja kohde hukutetaan näillä vastauksilla (Kambourakis et al., 2007). DNS-amplifikaatiohyökkäykset ovat erityisen vaarallisia, koska ne hyödyntävät kolmansia osapuolia — DNS-palvelimia — tehostaakseen hyökkäystä.

Taloudelliset vaikutukset palvelunestohyökkäyksistä voivat olla merkittäviä. Esimerkiksi hyökkäys voi johtaa merkittäviin liiketoiminnan keskeytyksiin, asiakasmenetyksiin ja mainehaittoihin. Pankkialalla, jossa luottamus on ensiarvoisen tärkeää, palvelunestohyökkäys voi aiheuttaa mittavia mainehaittoja ja asiakkaiden luottamuksen menetystä (Feigenbaum et al., 2007; Garcia-Teodoro et al., 2009). Verkkokaupoille jokainen tunti, jolloin palvelu ei ole käytettävissä, voi merkitä suoria myyntitulojen menetyksiä.

Vaikka palvelunestohyökkäykset voivat olla tuhoisia, niiden torjumiseksi on kehitetty useita puolustusmekanismeja. Yksi tärkeimmistä menetelmistä on anomaly-pohjainen havaitseminen, jossa verkon liikennettä analysoidaan jatkuvasti poikkeamien varalta. Tämänkaltaiset järjestelmät pystyvät tunnistamaan, milloin liikenne on epänormaalia ja voi viitata hyökkäykseen (Garcia-Teodoro et al., 2009). Tämä mahdollistaa sen, että hyökkäys voidaan tunnistaa ja pysäyttää ennen kuin se aiheuttaa merkittäviä vahinkoja.

Toinen tärkeä torjuntakeino on tekoälyn ja koneoppimisen hyödyntäminen DDoS-hyökkäysten torjunnassa. Koneoppimisjärjestelmät pystyvät analysoimaan liikennettä reaaliaikaisesti ja oppimaan havaitsemaan poikkeamia normaalista käyttäytymisestä, mikä tekee niistä erityisen tehokkaita uusien ja kehittyvien uhkien torjunnassa. Tällaiset järjestelmät voivat mukautua jatkuvasti uusiin hyökkäysmuotoihin ja estää hyökkäykset jo alkuvaiheessa (Adedeji et al., 2023).

Kolmas merkittävä puolustuskeino on pilvipohjaisten DDoS-torjuntaratkaisujen käyttö. Nämä ratkaisut hyödyntävät hajautettuja palvelinjärjestelmiä, jotka voivat absorboida hyökkäysliikennettä ja jakaa sen useiden palvelimien kesken. Tämä estää yksittäistä palvelinta ylikuormittumasta ja suojaa sitä hyökkäyksiltä, jotka muutoin voisivat kaataa sen. Pilvipohjaiset ratkaisut ovat erityisen hyödyllisiä suuria ja monimutkaisia hyökkäyksiä vastaan, kuten DNS-amplifikaatiohyökkäykset, joissa hyökkäysliikenne voi kasvaa eksponentiaalisesti (Cloudflare, 2014).

Vaikka palvelunestohyökkäysten torjunta kehittyy jatkuvasti, haasteena on se, että hyökkääjät kehittävät jatkuvasti uusia menetelmiä, joilla ohittaa olemassa olevat suojaukset. Monivaiheiset hyökkäykset, joissa yhdistetään useita eri hyökkäysmuotoja, ovat erityisen vaikeita torjua, koska ne voivat kohdistua useisiin järjestelmän haavoittuvuuksiin yhtä aikaa (Feigenbaum et al., 2007).

Palvelunestohyökkäysten uhka ei ole vain tekninen ongelma; se on myös merkittävä yhteiskunnallinen haaste, koska nämä hyökkäykset voivat kohdistua kriittisiin infrastruktuureihin, kuten energiaverkkoihin, vesihuoltoon ja julkisiin terveyspalveluihin. Esimerkiksi terveydenhuollon järjestelmät ovat erityisen haavoittuvia, koska ne käyttävät usein vanhentuneita tietoteknisiä järjestelmiä ja niiden toimintakatkokset voivat vaarantaa potilaiden turvallisuuden (Cloudflare, 2014). Tämä korostaa tarvetta kehittää entistä tehokkaampia puolustusmekanismeja, jotka pystyvät vastaamaan näihin uhkiin.

Palvelunestohyökkäykset ja niiden kehittyneemmät muodot, kuten DDoS, ovat vakavia uhkia, jotka voivat aiheuttaa merkittäviä taloudellisia ja toiminnallisia haittoja. Näiden hyökkäysten torjuminen vaatii monitasoista lähestymistapaa, joka yhdistää teknologian, koulutuksen ja jatkuvan valmiuden. Koska hyökkäykset kehittyvät jatkuvasti, myös puolustusjärjestelmien on oltava joustavia ja ajan tasalla. Tulevaisuudessa on odotettavissa, että DDoS-hyökkäykset kohdistuvat yhä enemmän uusiin teknologioihin, kuten esineiden internetiin (IoT), mikä korostaa entistä enemmän tarvetta kehittää tehokkaita ja innovatiivisia puolustusratkaisuja.

Taulukko 2 Palvelunestohyökkäysten tyypit

	Hyökkäystyyppi	Kuvaus	Tavoite	Haavoittuvuus
1	SYN-flood	TCP-yhteyspyyntöjä lähetetään ilman aikomusta viimeistellä yhteyttä, ylikuormittaa palvelimen	Ylikuormittaa palvelin resursseillisesti.	TCP-protokollan yhteydenmuodostus
2	ICMP-flood	Lähetetään suuri määrä ICMP-pyyntöjä, jolloin palvelin ei pysty vastaamaan kaikkiin.	Kuluttaa kohdejärjestelmän kaistanleveyttä ja resursseja.	Verkkoprotokollan ICMP-käsittely
3	DNS-amplikaatio	Hyödynnetään kolmansia DNS-palvelimia lähettämään suuret vastaukset uhriin pienen pyynnön	Moninkertaistaa hyökkäyksen voimakkuus heijastuksen avulla.	DNS-palvelimien avoin toiminta
4	Miari-botnet (DDoS)	Käyttää suurta määrää IoT-laitteita (bottiverkko) suorittamaan hajautettu hyökkäys samanaikaisesti.	Laaja verkkohäiriö palveluihin käyttämällä IoT-laitteita.	Heikosti suojatut IoT-laitteet

2.2.3 Tietojenkalastelu

Tietojenkalastelu (engl. phishing) on yksi yleisimmistä ja samalla vaarallisimmista kyberhyökkäysten muodoista, ja sen kohteeksi joutuvat erityisesti pk-yritykset. Tietojenkalastelussa hyökkääjä pyrkii manipuloimaan kohdetta luovuttamaan luottamuksellista tietoa, kuten salasanoja, käyttäjätunnuksia tai muita arkaluontoisia tietoja, usein sähköpostin tai muun viestintäkanavan kautta. Tällaiset hyökkäykset eivät ainoastaan aiheuta suoria taloudellisia menetyksiä, vaan ne voivat myös vaarantaa yrityksen maineen ja asiakassuhteet. Erityisesti pk-yritykset ovat tietojenkalastelun suhteen haavoittuvia, sillä niillä on harvoin riittäviä resursseja suojautua tehokkaasti tällaisilta hyökkäyksiltä (Jansson & von Solms, 2011).

Tietojenkalastelu on lisääntynyt nopeasti viime vuosina, ja tilastojen mukaan se on yksi yleisimmistä kyberuhista, jotka kohdistuvat pk-yrityksiin (Symantec, 2019). Burda et al. (2023) ovat todenneet, että pk-yritykset ovat usein houkuttelevia kohteita, koska ne eivät välttämättä investoi samalla tavalla kyberturvallisuuteen kuin suuremmat organisaatiot. Tämä resurssien puute yhdistettynä kasvavaan kyberuhkien monimuotoisuuteen luo tilanteen, jossa pk-yritykset ovat erityisen alttiita tietojenkalastelulle. Pk-yritysten kohdalla tietojenkalastelu on yksi kustannustehokkaimmista hyökkäystavoista, koska se ei vaadi hyökkääjältä suuria teknisiä resursseja ja voi olla helposti kohdistettavissa. Tietojenkalastelu hyödyntää usein sosiaalista manipulointia, eli yrityksiä huijataan viestinnän kautta luovuttamaan arkaluontoisia tietoja tai lataamaan haittaohjelmia. Tämä tapahtuu usein sähköpostien, tekstiviestien tai jopa sosiaalisen median kautta, ja työntekijät ovat erityisen haavoittuvia näille hyökkäyksille, jos he eivät ole saaneet riittävää koulutusta tai tietoturvatietoisuutta (Burda et al., 2014).

Tietojenkalastelun vaikutukset pk-yrityksille voivat olla huomattavia. Tietojenkalasteluhyökkäykset voivat johtaa taloudellisiin menetyksiin, liiketoiminnan keskeytyksiin ja maineen vahingoittumiseen, mikä on erityisen haitallista pk-yrityksille, joiden maine ja asiakassuhteet ovat usein henkilökohtaisia ja perustuvat luottamukseen. Yrityksen joutuminen tietojenkalasteluhyökkäyksen uhriksi voi heikentää asiakassuhteita ja aiheuttaa merkittäviä kustannuksia tiedon palauttamisesta ja liiketoiminnan jälleenrakentamisesta (Jansson & von Solms, 2011). Erityisesti pk-yritykset, joilla ei ole vahvoja sisäisiä tietoturvakäytäntöjä tai turvallisuuskoulutusta, ovat alttiimpia tietojenkalasteluyrityksille. Bada et al. (2015) painottavat, että vaikka tietojenkalasteluun kohdistetut koulutus- ja tietoisuuskampanjat ovat yleistyneet, ne eivät usein saavuta toivottua vaikutusta pk-yrityksissä. Syynä tähän voi olla kampanjoiden epäyhtenäinen toteutus tai vähäinen työntekijöiden sitoutuminen tietoturvakäytäntöihin. Lisäksi monet pk-yritykset eivät ole tietoisia siitä, kuinka haavoittuvia ne ovat tietojenkalastelulle, ja tämän vuoksi ne eivät tee riittäviä toimenpiteitä estääkseen sen (Burda et al., 2023).

Tietojenkalastelulta suojautuminen vaatii sekä teknisiä että organisatorisia ratkaisuja. Yksi tärkeimmistä suojautumiskeinoista on henkilöstön tietoturvakoulutus, joka auttaa työntekijöitä tunnistamaan ja reagoimaan mahdollisiin tietojenkalasteluyrityksiin. Abawajy (2012) tuo esiin, että työntekijöille suunnatut kyberturvallisuuskoulutukset,

joissa keskitytään erityisesti tietojenkalastelun tunnistamiseen, voivat vähentää merkittävästi yrityksen haavoittuvuutta. Tämä on erityisen tärkeää pk-yrityksissä, joissa kaikilla työntekijöillä voi olla suora vaikutus yrityksen turvallisuuteen. Lisäksi teknologian kehitys tarjoaa pk-yrityksille kustannustehokkaita ratkaisuja, kuten pilvipohjaisia tietoturvapalveluita ja uhkien tunnistusjärjestelmiä, jotka voivat auttaa torjumaan tietojenkalastelua (Symantec, 2019). Nämä teknologiat voivat suojata yrityksen sähköpostijärjestelmiä ja verkkosivuja mahdollisilta hyökkäyksiltä sekä tunnistaa epäilyttävää toimintaa reaaliajassa.

Pk-yritykset voivat hyötyä myös ulkopuolisista palveluista, kuten kyberturvallisuuden hallintapalveluista, jotka tarjoavat tietoturvapalveluita kustannustehokkaasti ja skaalautuvasti. Tämä on erityisen hyödyllistä pk-yrityksille, joilla ei ole omaa kyberturva-asiantuntemusta, mutta jotka tarvitsevat luotettavia suojautumiskeinoja tietojenkalasteluhyökkäyksiä vastaan (Alahmari & Duncan, 2019).

Pk-yrityksillä on yhä haasteita tehokkaiden tietojenkalastelun torjuntastrategioiden luomisessa. Monilla pk-yrityksillä on rajalliset resurssit kouluttaa työntekijöitä tai hankkia kehittyneitä tietoturvaratkaisuja, mikä luo haasteita tietojenkalastelun torjunnalle. Yrityksen tietoturvatietoisuuden lisääminen ja henkilöstön kouluttaminen ovat välttämättömiä, mutta eivät aina riittäviä suojautumistoimenpiteitä. Lisäksi pk-yritysten tulee kehittää selkeitä tietoturvapolitiikkoja ja toimenpidesuunnitelmia, jotka parantavat organisaation sisäistä tietoturvakulttuuria (Bada et al., 2015).

Pk-yritysten tulisi arvioida tietojenkalastelun riskit säännöllisesti ja mukauttaa toimenpiteitään uhkien kehittyessä. Tämä edellyttää jatkuvaa uhkien arviointia ja työntekijöiden koulutuksen päivittämistä, jotta pk-yritykset voivat sopeutua nopeasti muuttuvaan kyberuhkakenttään (Wilson et al., 2022).

2.2.4 Troijalaiset

Troijalaiset, tai troijalaisohjelmat (Trojan horses), ovat haittaohjelmien muoto, jossa hyödynnetään käyttäjän luottamusta manipuloimalla hänet avaamaan tai lataamaan haitallisia tiedostoja. Troijalaiset naamioituvat hyödyllisiksi tai harmittomiksi sovelluksiksi, mutta tosiasiassa ne voivat mahdollistaa luvattoman pääsyn yrityksen järjestelmiin tai kerätä tietoja käyttäjän huomaamatta (López et al., 2020). Troijalaiset eivät leviä itsenäisesti, kuten virukset tai madot, vaan ne tarvitsevat käyttäjän toimia

aktivoituakseen. Tämä tekee troijalaisista erityisen vaarallisia erityisesti pk-yrityksille, joiden tietoturvakäytännöt voivat olla puutteellisia. Troijalaiset ovat nykyään yksi yleisimmistä haittaohjelmatyypeistä, joita pk-yritykset kohtaavat, ja ne voivat aiheuttaa merkittäviä taloudellisia ja toiminnallisia riskejä (López et al., 2020).

Troijalaisohjelmat hyödyntävät usein sosiaalista manipulointia eli huijaustekniikoita, joiden avulla käyttäjä saadaan avaamaan haitallisia tiedostoja. Yleisin hyökkäystapa on tietojenkalastelu, jossa troijalaisohjelma naamioidaan luotettavaksi viestiksi tai liitteeksi (Aleroud & Zhou, 2017). Aleroud ja Zhou (2017) ovat havainneet, että tietojenkalastelun onnistuminen perustuu usein vastaanottajan vähäiseen tietoturvatietoisuuteen ja kiireeseen. Pk-yrityksissä, joissa henkilöstöä ei välttämättä ole koulutettu tietojenkalastelun tunnistamiseen, tämä riski kasvaa entisestään (Abawajy, 2014).

Eräs yleinen troijalaisten muoto on ns. pankkitroijalainen, joka on suunniteltu varastamaan arkaluontoisia tietoja, kuten pankkitunnuksia ja luottokorttitietoja. Lisäksi troijalaiset voivat toimia "takaovina" (backdoors), jotka antavat hyökkääjille pääsyn yrityksen järjestelmiin ilman, että yritys havaitsee tunkeutumista. Tästä seuraa, että hyökkääjä voi asentaa lisäkomponentteja, kuten näppäinpainallusten tallentimia tai kiristysohjelmia, jotka voivat lamauttaa yrityksen toiminnan (Ståhlberg, 2007). Troijalaiset voivat myös estää järjestelmänvalvojia havaitsemasta tunkeutumista pitkiäkin aikoja, mikä tekee niistä erityisen haitallisia ja vaikeasti havaittavia. Kun troijalainen on päässyt yrityksen järjestelmiin, sen poistaminen voi olla haastavaa ilman kehittyneitä turvatoimenpiteitä, joita pk-yrityksillä ei usein ole käytössään (Jin et al., 2018).

Pk-yritykset ovat erityisen haavoittuvia troijalaisille niiden rajallisten resurssien ja usein puutteellisen kyberturvallisuustietoisuuden vuoksi. Richardson ja kumppanit (2020) huomauttavat, että monet pk-yritykset eivät pidä kyberturvallisuutta keskeisenä investointikohteena, mikä tekee niistä alttiita kohteita erityisesti troijalaisille ja muille sosiaalisen manipuloinnin avulla levitettäville uhille. López et al. (2020) mukaan pk-yritykset joutuvat useammin hyökkäysten kohteiksi, sillä hyökkääjät tietävät, että pienemmät yritykset eivät välttämättä investoi tarvittaviin tietoturvatoimenpiteisiin.

Tutkimukset osoittavat, että pk-yrityksillä on harvoin käytössään resursseja tai asiantuntijoita, jotka auttaisivat havaitsemaan ja torjumaan troijalaisohjelmia (Symantec, 2019). Tämä johtaa siihen, että monet troijalaisohjelmat voivat toimia pitkään huomaamattomina, keräten tietoja tai jopa vaarantaen koko yrityksen tietojärjestelmän toiminnan. Erityisesti pankkitroijalaiset, jotka on suunniteltu varastamaan taloudellisia tietoja, voivat olla tuhoisia pk-yrityksille, joiden taloudellinen varmuus voi heikentyä nopeasti tietomurroista johtuvien menetyksien vuoksi.

Troijalaisilta suojautuminen vaatii pk-yrityksissä kokonaisvaltaista lähestymistapaa, jossa yhdistyvät sekä tekniset ratkaisut että henkilöstön koulutus. Useat tutkimukset korostavat henkilöstön kyberturvallisuuskoulutuksen merkitystä. Aleroud ja Zhou (2017) tuovat esille, että kouluttamalla työntekijöitä tunnistamaan tietojenkalasteluyrityksiä yritykset voivat vähentää riskiä, että haittaohjelma pääsee yrityksen järjestelmään.

Pk-yritykset voivat myös hyödyntää kustannustehokkaita teknologiaratkaisuja, kuten pilvipohjaisia tietoturvapalveluita ja virustorjuntaohjelmistoja, jotka auttavat tunnistamaan ja estämään troijalaisia (Chidukwani et al., 2012). Symantecin (2019) mukaan pk-yritysten tulisi pyrkiä käyttämään monikerroksisia turvatoimenpiteitä, kuten palomuureja, tunkeutumisenestojärjestelmiä (IDS) ja ajantasaisia päivityksiä, mikä voi vähentää troijalaisohjelmien onnistumismahdollisuuksia. Ennaltaehkäisevien toimien ohella pk-yritysten on tärkeää toteuttaa säännöllisiä turvallisuustarkastuksia ja pitää ohjelmistot ajan tasalla. Tietoturvapäivitysten laiminlyönti voi tehdä yrityksistä alttiimpia uusille troijalaisvarianteille (Jin et al., 2018).

Troijalaiset ovat vakava uhka pk-yrityksille, joiden resurssit ja tietoturvaosaaminen eivät usein riitä tehokkaaseen suojautumiseen. Troijalaisohjelmien torjunta pk-yrityksissä vaatii kokonaisvaltaisia strategioita, joihin kuuluvat teknologiset ratkaisut ja henkilöstön koulutus. Koska troijalaiset ja tietojenkalastelu ovat vahvasti kytköksissä toisiinsa, pk-yritysten on tärkeää vahvistaa kyberturvallisuustietoisuutta ja luoda toimiva turvakulttuuri, jotta ne voivat suojautua monimutkaisia ja kehittyviä uhkia vastaan.

2.3 Kyberturvallisuus pk-yrityksissä ja niiden keskeiset elementit

Kyberturvallisuus on yksi tärkeimmistä liiketoiminnan turvaamisen tekijöistä vuonna 2024. Pk-yritykset kohtaavat entistä monimutkaisempia ja useammin kohdistettuja kyberuhkia, kuten ransomware-hyökkäyksiä, tietojenkalastelua ja palvelunestohyökkäyksiä (Bada et al., 2015). Kyberuhkien seuraukset voivat olla vakavia: hyökkäykset voivat pysäyttää liiketoiminnan, aiheuttaa suuria taloudellisia tappioita ja heikentää yrityksen mainetta. Suuret yritykset saattavat kyetä palautumaan tietoturvaloukkauksista nopeammin ja tehokkaammin, mutta pk-yrityksille kyberhyökkäykset voivat olla taloudellisesti kohtalokkaita ja jopa johtaa toiminnan lopettamiseen.

Nykyaikana pk-yrityksillä on vastassaan erityisen suuri määrä teknologisia haasteita. Etätyön yleistyminen, pilvipalveluiden laaja käyttö ja yhä monimutkaisempi digitaalinen infrastruktuuri ovat lisänneet hyökkäyspinta-alaa ja tehneet kyberhyökkäykset helpommin toteutettaviksi. Digitalisaation ja esineiden internetin (IoT) yleistyminen on lisännyt yritysten haavoittuvuutta entisestään. IoT-laitteet ovat usein riittämättömästi suojattuja, ja niiden kautta tapahtuvat hyökkäykset voivat vaarantaa koko yrityksen tietoturvan (Chaudhary et al., 2023).

PK-yritysten kyberturvallisuuden parantaminen edellyttää keskittymistä muutamiin keskeisiin elementteihin, jotka auttavat suojaamaan liiketoimintaa ja tukevat turvallisuuden jatkuvaa kehittämistä.

Riskien arviointi ja hallinta: Riskien arviointi on olennainen lähtökohta kyberturvallisuuden kehittämiselle pk-yrityksissä. Yrityksen on ensin tunnistettava kriittiset tietovarannot ja järjestelmät sekä arvioitava niiden haavoittuvuudet ja altistuminen kyberuhille. Riskienhallinnan avulla yritykset voivat priorisoida suojaustoimenpiteitä ja keskittyä toimenpiteisiin, jotka vastaavat niiden tärkeimpiin tietoturvahaasteisiin. Kuten Srinivas et al. (2019) toteavat, riskienhallintamallit ja -standardit tarjoavat hyödyllisiä puitteita riskien arvioinnille, mutta niiden soveltaminen vaatii resurssien ja osaamisen tasapainottamista erityisesti pk-yrityksissä.

Tietoturvapolitiikat ja henkilöstön koulutus: Tietoturvakulttuuri on keskeinen tekijä turvallisuuden kehittämisessä, ja työntekijöiden tietoisuus uhkista voi vähentää merkittävästi yritykseen kohdistuvia riskejä. Tietojenkalastelu on yleinen kyberuhka,

joka perustuu inhimillisiin virheisiin. Bada et al., (2015) korostavat, että henkilöstön kouluttaminen uhkien tunnistamiseen ja tietoturvapolitiikoiden noudattamiseen auttaa yrityksiä ehkäisemään tietomurtoja ja vahvistaa yrityksen turvallisuuskulttuuria. Yritysten tulisi järjestää säännöllisesti kyberturvallisuuskoulutuksia ja ohjeistaa henkilöstöä tunnistamaan epäilyttävät sähköpostiviestit ja tietojenkalasteluyritykset.

Pääsynhallinta ja käyttöoikeuksien rajoittaminen: Pääsynhallinta tarkoittaa kontrollia siitä, kenellä on pääsy yrityksen tietoihin ja järjestelmiin. Monivaiheinen tunnistautuminen ja roolipohjaiset käyttöoikeudet ovat tehokkaita keinoja varmistaa, että työntekijöillä on pääsy vain niihin tietoihin, jotka ovat olennaisia heidän työtehtäviensä kannalta. Tämä on erityisen tärkeää yrityksissä, joissa järjestelmiä ja tietoja käytetään laajalti etäyhteyksien kautta. Käyttöoikeuksien rajoittaminen vähentää huomattavasti riskiä, että ulkopuoliset henkilöt pääsisivät käsiksi yrityksen tietoihin luvattomasti. (Alasmary et al., 2021).

Varmuuskopiointi ja toipumissuunnitelmat: Ransomware-hyökkäysten yleistyminen on korostanut tehokkaan varmuuskopioinnin ja toipumissuunnitelmien merkitystä. Hyvin suunniteltu varmuuskopiointistrategia mahdollistaa kriittisten tietojen nopean palauttamisen hyökkäyksen jälkeen, mikä minimoi taloudelliset vahingot ja liiketoiminnan keskeytyksen. ENISA (European Union Agency for Cybersecurity, 2021) suosittelee, että yritykset ottavat käyttöön säännöllisen varmuuskopiointikäytännön ja varmistavat, että varmuuskopiot säilytetään erillisessä ympäristössä. Näin varmistetaan, että tiedot voidaan palauttaa nopeasti ja turvallisesti.

Uhkatilanteiden havaitseminen ja reagointi: Uhkatilanteiden varhainen havaitseminen ja tehokas reagointi voivat estää vakavia tietomurtoja ja niiden seurauksia. Pk-yritykset voivat hyödyntää reaaliaikaista valvontaa ja poikkeavuuksien havaitsemisjärjestelmiä, jotka tunnistavat epäilyttävää toimintaa järjestelmissä. Näiden teknologioiden avulla kyberuhkiin voidaan puuttua ennen kuin ne ehtivät eskaloitua ja aiheuttaa vahinkoa. Bada et al., (2015) korostavat, että pienemmille yrityksille myös yksinkertaiset ja helposti hallittavat seurantaratkaisut voivat olla arvokkaita, sillä ne auttavat tunnistamaan uhat ja reagoimaan niihin nopeasti.

Pk-yritysten kyberturvallisuussäädökset ovat kiristyneet erityisesti Euroopan unionin alueella. Vuoden 2023 alussa voimaan astunut NIS2-direktiivi asettaa uusia tietoturvavaatimuksia myös pienemmille yrityksille. Direktiivi edellyttää, että yritykset

varmistavat tarvittavien suojatoimien käytön ja noudattavat tiukkoja raportointivaatimuksia tietoturvaloukkauksista. Nämä vaatimukset asettavat pk-yrityksille haasteita, sillä niiden resurssit ovat usein rajalliset. Srinivas et al. (2019) korostavat, että sääntelyn mukanaan tuomat vaatimukset voivat kannustaa Pk-yrityksiä harkitsemaan ulkopuolisten tietoturvapalveluiden hyödyntämistä. Hallittujen tietoturvapalveluiden (MSSP) käyttö voi tarjota yrityksille asiantuntemusta, jota ne eivät itse pysty tarjoamaan. MSSP-palvelut voivat sisältää muun muassa jatkuvaa tietoturvavalvontaa, riskien arviointia ja tietoturvakonsultointia, mikä mahdollistaa pk-yrityksille kustannustehokkaan tavan täyttää sääntelyn vaatimukset ja parantaa turvallisuuttaan.

Teknologian kehittyessä pk-yritysten kyberturvallisuusvaatimukset muuttuvat entistä monimutkaisemmiksi. Tekoälyä ja koneoppimista hyödyntävät kyberrikolliset pystyvät kehittämään kehittyneempiä hyökkäysmenetelmiä, jotka kohdistuvat yhä tarkemmin yritysten haavoittuvuuksiin. IoT on lisännyt entisestään pk-yritysten haavoittuvuutta, sillä monet IoT-laitteet ovat riittämättömästi suojattuja ja voivat toimia sisäänpääsykohtana yrityksen verkkoon. Saini et al. (2020) korostavat, että tulevaisuudessa pk-yritykset joutuvat lisäämään investointejaan IoT-laitteiden turvallisuuteen ja kehittämään kattavia riskienhallintastrategioita.

Kyberturvallisuuden tulevaisuudessa keskeisiä tekijöitä ovat myös automaattiset uhkien tunnistamis- ja reaktiomallit, jotka voivat auttaa pk-yrityksiä vastaamaan uhkiin nopeammin ja tehokkaammin. Vaikka kehittyneet järjestelmät ovatkin usein suurten yritysten käytössä, skaalautuvat ja edullisemmat ratkaisut ovat tulossa markkinoille myös pienemmille yrityksille. Pk-yrityksillä on mahdollisuus hyötyä pilvipohjaisista tietoturvatyökaluista, jotka mahdollistavat reaaliaikaisen valvonnan ja uhkien havaitsemisen kustannustehokkaasti. Nykyaikana kyberturvallisuus on kriittinen osa liiketoiminnan jatkuvuuden turvaamista erityisesti pk-yrityksille, jotka kohtaavat monimutkaisia kyberuhkia ja kasvavia sääntelyvaatimuksia. Pk-yritysten kyberturvallisuusstrategiat tulisi keskittyä riskienhallintaan, tietoturvapolitiikoihin, pääsynhallintaan, varmuuskopiointiin ja reaaliaikaiseen uhkien seurantaan. Koska monet pk-yritykset eivät pysty ylläpitämään laajoja sisäisiä tietoturvatoimia, ulkopuolisten palveluntarjoajien käyttö voi olla kustannustehokas ja käytännöllinen ratkaisu. Lopulta kyberturvallisuuden integrointi liiketoiminnan strategiseen suunnitteluun on avainasemassa, kun pk-yritykset pyrkivät vastaamaan muuttuviin

uhkiin ja monimutkaistuviin sääntelyvaatimuksiin. Investoimalla tietoturvaan ja kehittämällä kattavia käytäntöjä pk-yritykset voivat vahvistaa suojaustaan ja varmistaa liiketoimintansa jatkuvuuden.

3 Kyberhyökkäysten vaikutuksien arviointi pk-yritysten liiketoiminnassa

Tämän kappaleen tavoitteena on ymmärtää, miten pienet ja keskisuuret yritykset voivat arvioida kyberhyökkäysten vaikutuksia liiketoiminnassaan teorian avulla ennen haastatteluja. Tarkastelun kohteena ovat yleiset vaikutukset, pk-yrityksille erityiset haasteet vaikutusten arvioinnissa, käytettävät arviointimenetelmät sekä kehitettävät ratkaisut, jotka tukevat kyberturvallisuuden ja liiketoiminnan jatkuvuuden hallintaa pk-yrityksissä. Kyberhyökkäysten vaikutusten arviointi on keskeinen osa nykyaikaista riskienhallintaa, ja erityisesti pk-yrityksille se tarjoaa mahdollisuuden varautua hyökkäysten aiheuttamiin häiriöihin liiketoiminnassa. Pk-yritykset muodostavat merkittävän osan kansantaloudesta, mutta niiden kyky vastata kyberhyökkäyksiin on usein heikompi kuin suuryrityksillä, johtuen resurssien ja asiantuntemuksen puutteesta. Samalla niiden kohtaamat uhkat ovat monimuotoisia, vaihdellen tietomurroista palvelunestohyökkäyksiin ja kiristyshaittaohjelmiin. Näiden uhkien arviointi edellyttää systemaattisia menetelmiä, jotka voivat auttaa yrityksiä ymmärtämään hyökkäysten vaikutukset sekä lyhyellä että pitkällä aikavälillä.

Kyberhyökkäysten arviointimenetelmät voidaan jakaa karkeasti kvantitatiivisiin ja kvalitatiivisiin lähestymistapoihin. Kvantitatiiviset menetelmät keskittyvät hyökkäysten taloudellisten vaikutusten mittaamiseen, mukaan lukien menetetty liikevaihto, korjauskustannukset, sakot ja muut oikeudelliset seuraamukset. IBM:n ja Ponemon Instituutin (2023) mukaan tietomurtojen keskimääräiset kustannukset ovat jatkuvasti nousseet, mikä osoittaa selkeästi, että kyberuhkien taloudelliset vaikutukset ovat merkittävä riski kaikenkokoisille yrityksille.

Kvalitatiiviset menetelmät puolestaan tarjoavat syvällisempää ymmärrystä hyökkäysten ei-taloudellisista vaikutuksista, kuten mainehaitoista ja asiakkaiden luottamuksen menettämisestä. Tässä kontekstissa skenaarioanalyysit ja riskiarvioinnit voivat auttaa pk-yrityksiä tunnistamaan potentiaalisia uhkaskenaarioita ja kehittämään ennakoivia strategioita. Kyberriskien arvioinnissa on tärkeää yhdistää teknologiset, liiketoiminnalliset ja organisatoriset näkökulmat, jotta uhkien kokonaisvaltainen vaikutus voidaan hahmottaa. Tämä on erityisen haastavaa pk-yrityksille, joilla on usein rajalliset resurssit ja kyky toteuttaa kattavia suojatoimia. Näissä tilanteissa vaikutusten arvioinnin systemaattiset menetelmät tarjoavat tärkeän työkalun.

Esimerkiksi Business Impact Calculator (BusICalc) -metodologia tarjoaa välineen kyberuhkien vaikutusten kvantifiointiin organisaation kriittisiin liiketoimintaprosesseihin. Tämä mahdollistaa riskinhallinnan priorisoinnin ja auttaa yrityksiä kohdentamaan rajalliset resurssit tehokkaasti toimenpiteisiin, jotka minimoivat suurimmat uhkakuvat (Alves et al., 2023). Lisäksi CENSOR-päätöksenteon tukijärjestelmä korostaa kyberturvallisuusinvestointien optimointia pk-yrityksissä. Tämä malli ottaa huomioon hyökkäysten vaiheittaisen etenemisen, hyökkäysriskiin liittyvän epävarmuuden sekä rajoitetut budjetit. Tutkimukset osoittavat, että kyberturvallisuuteen käytettyjen resurssien määrä ei aina ole suorassa suhteessa riskien pienenemiseen, mikä tekee priorisoinnista entistä tärkeämpää (Tsiodra et al., 2023).

Toinen keskeinen lähestymistapa on liiketoimintaprosessien ja verkostohaavoittuvuuksien välisten suhteiden analysointi. Hyökkäyskarttojen ja riippuvuuskarttojen yhdistämisen avulla voidaan arvioida hyökkäysten vaikutuksia numeerisin pisteytyksin, mikä tarjoaa tarkempia tietoja riskianalyysin tueksi (Cao et al., 2018). Tämänkaltaiset kvantitatiiviset menetelmät mahdollistavat eri uhkaskenaarioiden simuloinnin ja auttavat organisaatioita tunnistamaan kriittiset prosessit, jotka vaativat erityistä suojaa.

Kyberhyökkäysten vaikutusten arviointiin liittyy myös sosio-teknisiä ulottuvuuksia, kuten toimitusketjujen riippuvuudet ja organisatoriset roolit. Agenttipohjaiset mallit voivat mallintaa näitä suhteita organisaation eri tasoilla ja tarjota kokonaisvaltaisen kuvan haavoittuvuuksista ja riippuvuuksista. Tämä lähestymistapa tukee niin eteenpäin kuin taaksepäin tapahtuvaa analyysia, mikä auttaa organisaatioita ennakoimaan ja reagoimaan tehokkaammin erilaisiin uhkaskenaarioihin (Charitoudi & Blyth, 2014).

Lisäksi organisaation kyberturvallisuuskulttuurin ja valmiuksien kehittäminen ovat olennaisia tekijöitä hyökkäysten vaikutusten hallinnassa. Esimerkiksi simulointipohjaiset lähestymistavat, jotka analysoivat hyökkäyksiä organisaation kriittisiin tietoihin ja prosesseihin, auttavat paitsi havaitsemaan haavoittuvuuksia, myös luomaan kohdennettuja parannustoimenpiteitä. Tämä puolestaan vahvistaa organisaation kykyä sietää hyökkäyksiä ja palautua niistä nopeammin (FarahaniNia et al., 2023).

Käytännön työkaluja vaikutusten arviointiin tarjoavat kansainväliset viitekehykset, mm. NIST:n Cybersecurity Framework, mitä hyödynnän tämän tutkielman laatimisessa.

Tämä viitekehys tarjoaa pk-yrityksille selkeän, vaiheittaisen prosessin kyberturvallisuustilanteen arviointiin ja parantamiseen. Viitekehys painottaa erityisesti riskien priorisointia ja resurssien tehokasta kohdentamista, mikä on tärkeää pk-yrityksille, jotka usein joutuvat tasapainottelemaan kyberturvallisuuden ja muiden liiketoiminnallisten tarpeiden välillä. Lisäksi ISO/IEC 27001 -standardi tarjoaa kansainvälisesti tunnustetun viitekehyksen tietoturvallisuuden hallintaan, mikä voi auttaa pk-yrityksiä rakentamaan kokonaisvaltaisen ja tehokkaan tietoturvastrategian (ISO/IEC, 2013).

Pk-yritysten näkökulmasta keskeistä on myös ymmärtää, kuinka arviointimenetelmät voivat tukea päätöksentekoa ja liiketoiminnan strategista suunnittelua. Systemaattiset arviointiprosessit voivat auttaa tunnistamaan haavoittuvia liiketoiminnan osa-alueita ja kehittämään kohdennettuja toimenpiteitä näiden riskien hallitsemiseksi. IBM:n ja Ponemon Instituutin (2023) mukaan nopea reagointi kyberhyökkäyksiin voi vähentää merkittävästi niiden vaikutuksia, minkä vuoksi yritysten tulisi käyttää arviointimenetelmiä myös ennakoivasti. Samalla tutkimukset, kuten Ransbothamin ja Mitran (2009) analyysi kyberhyökkäysten vaikutuksista yritysten markkina-arvoon, osoittavat, että tehokas riskienhallinta voi myös vahvistaa yrityksen mainetta ja lisätä asiakkaiden luottamusta.

Kaiken kaikkiaan kyberhyökkäysten vaikutusten arviointi edellyttää sekä kvantitatiivisten että kvalitatiivisten menetelmien käyttöä. Yhdessä nämä lähestymistavat voivat tarjota pk-yrityksille kattavan ymmärryksen kyberuhkien vaikutuksista ja auttaa niitä kehittämään strategioita, jotka eivät pelkästään suojaa hyökkäyksiltä, vaan myös vahvistavat liiketoiminnan jatkuvuutta ja kilpailukykyä. Kuten tutkielmassa on aikaisemmin mainittu, kyberhyökkäysten vaikutusten arviointi on erityisen haastavaa pk-yrityksille niiden resurssien ja kyberturvallisuusosaamisen rajallisuuden vuoksi. Suurempiin yrityksiin verrattuna pk-yritykset ovat alttiimpia merkittäville liiketoiminnan häiriöille, sillä ne harvoin pystyvät investoimaan yhtä laajasti kyberturvallisuuteen tai sen seurantatyökaluihin. Kyberhyökkäysten riskit voivat ulottua pk-yrityksissä koko liiketoiminnan vaarantamiseen, minkä vuoksi tehokkaiden arviointikeinojen ja varautumissuunnitelmien kehittäminen on erityisen tärkeää.

3.1 Kyberhyökkäysten vaikutukset liiketoimintaan: yleinen viitekehys

Kyberhyökkäykset voivat aiheuttaa moninaisia ja laajoja vaikutuksia yrityksen liiketoimintaan. Näihin vaikutuksiin kuuluvat esimerkiksi taloudelliset tappiot, maineen menetykset, asiakassuhteiden heikkeneminen sekä kriittisten tietojen menetykset. Taloudelliset tappiot voivat syntyä suoraan hyökkäyksistä aiheutuneista vahingoista, kuten liiketoiminnan keskeytyksestä, varkauksista tai tietojen palauttamiskuluista (Amin, 2017). Maineen menetyksellä puolestaan on pitkäaikaisia vaikutuksia asiakassuhteisiin ja uusasiakashankintaan, erityisesti jos asiakkaat kokevat yrityksen olevan haavoittuva tietoturvauhille. Lisäksi kyberhyökkäykset voivat johtaa asiakassuhteiden heikkenemiseen, sillä luottamus yrityksen kykyyn suojata tietoja ja ylläpitää toimintavarmuutta on keskeinen osa asiakaskokemusta. Pk-yrityksille tällaiset menetykset voivat olla kohtalokkaita, sillä ne saattavat olla riippuvaisia pitkäaikaisista asiakassuhteista ja jatkuvasta tulovirrasta. Kyberhyökkäykset voivat vaikuttaa erityisesti teollisuuden kriittisiin infrastruktuureihin, kuten sähköverkkoihin, mikä korostaa kyberturvallisuuden merkitystä monilla aloilla (Huang et al., 2018).

Kyberhyökkäykset ovat kasvava uhka yrityksille, sillä ne voivat vahingoittaa kriittisiä prosesseja, johtaa tiedon vuotamiseen ja aiheuttaa merkittäviä taloudellisia sekä maineeseen liittyviä haittoja. Ymmärtääksemme näiden hyökkäysten liiketoiminnallisia vaikutuksia on tärkeää tarkastella niitä monitasoisesti ja hyödyntää järjestelmällisiä arviointikehyksiä. Esimerkiksi yrityksen kyky suojautua hyökkäyksiltä sekä reagoida niihin määrittää, kuinka vakavia taloudellisia ja toiminnallisia seurauksia yritys kohtaa (Kamiya et al., 2019).

Liiketoiminnallisten vaikutusten arvioinnissa yleiset kehykset, kuten hierarkkiset virtausmallit ja dynaamiset vaikutusarvioinnit, tarjoavat perusteellisen tavan analysoida kyberhyökkäysten vaikutuksia. Hierarkkiset mallit huomioivat paitsi kyberhyökkäyksen yksittäisiin resursseihin kohdistuvat vaikutukset, myös sen, miten vaikutukset leviävät koko järjestelmään. Näin ne tarjoavat realistisemman kuvan hyökkäyksen laajuudesta ja vakavuudesta (Zhu et al., 2019).

Monet tutkimukset korostavat liiketoiminnan avainprosessien haavoittuvuuksien tunnistamista ja niiden liittämistä kyberhyökkäysten vaikutusarviointeihin. Esimerkiksi Bayes-verkkoihin perustuva lähestymistapa voi mallintaa kyberhyökkäysten etenemistä ja arvioida hyökkäyksen vaikutusta fyysisiin prosesseihin. Tällaiset mallit auttavat

yrityksiä valmistautumaan paremmin mahdollisiin riskeihin ja priorisoimaan resurssejaan tehokkaasti (Huang et al., 2018).

Kyberhyökkäysten vaikutukset ulottuvat myös yritysten strategisiin päätöksiin, kuten riskinhallintaan ja investointipäätöksiin. Hyökkäykset, joissa esimerkiksi asiakkaiden taloudellisia tietoja vuotaa, voivat aiheuttaa merkittäviä markkina-arvon menetyksiä sekä myynnin laskua, erityisesti vähittäiskaupan alalla. Tällaiset tilanteet pakottavat yritykset uudelleenarvioimaan riskinhallintaansa ja lisäämään panostuksia tietoturvaan (Kamiya et al., 2019).

Laajempien taloudellisten vaikutusten arvioimiseksi agenttipohjaiset mallit ovat erityisen hyödyllisiä. Nämä mallit simuloivat vaikutuksia toimitusketjujen ja organisatoristen riippuvuuksien kautta, mikä tarjoaa kattavan näkökulman kyberhyökkäysten seurauksiin yrityksen kaikilla tasoilla (Charitoudi & Blyth, 2014).

3.2 Suomalaisten pk-yritysten erityispiirteet vaikutusten arvioinnissa

Pk-yrityksillä on omia erityisiä haasteitaan kyberhyökkäysten vaikutusten arvioinnissa. Usein pk-yrityksillä on rajalliset resurssit, mikä rajoittaa niiden kykyä investoida kattaviin kyberturvallisuusratkaisuihin ja arviointityökaluihin. Toisin kuin suuryrityksillä, pk-yrityksillä ei välttämättä ole erillistä tietoturvahenkilöstöä, vaan vastuu voi kuulua IT-hallinnon tai johdon tehtäviin, jolloin tietoturvaosaaminen ei aina ole syvällistä. Charitoudi ja Blyth (2014) korostavat sosio-teknisen lähestymistavan merkitystä pk-yrityksille, sillä se auttaa yhdistämään ihmisten ja teknologian vuorovaikutuksia sekä organisaation rakenteellisia erityispiirteitä kyberturvallisuudessa (Charitoudi & Blyth, 2014).

Resurssipulan lisäksi osaamisvaje ja järjestelmien hajanaisuus vaikeuttavat hyökkäysten arviointia. Pk-yritykset voivat käyttää useita erilaisia, toisiinsa yhteensopimattomia järjestelmiä, mikä lisää tietoturvahaavoittuvuuksia ja vaikeuttaa keskitettyä tietoturvahallintaa ja -arviointia. Tämä tekee kyberuhkien torjunnasta haastavaa ja voi myös vaikeuttaa riskien arviointia sekä varautumista.

Pk-yritykset muodostavat merkittävän osan Suomen taloudesta, sillä ne edustavat yli 90 % kaikista yrityksistä ja työllistävät suuren osan väestöstä (Tilastokeskus, 2021). Kyberturvallisuusuhkien yleistyessä pk-yritykset ovat kuitenkin osoittautuneet erityisen haavoittuviksi johtuen niiden rajallisista resursseista ja kyberturvallisuusosaamisesta.

Tämä tekee kyberhyökkäysten vaikutusten arvioinnista erityisen haastavaa, sillä monet pk-yritykset kamppailevat jopa perusasioiden hallinnan kanssa, kuten tietoturvakäytäntöjen jalkauttamisessa ja henkilöstön kouluttamisessa.

Pk-yritykset kohtaavat usein haasteita resurssien puutteen vuoksi, mikä rajoittaa niiden mahdollisuuksia investoida kyberturvallisuusratkaisuihin tai asiantuntijoihin. Esimerkiksi useat tutkimukset ovat osoittaneet, että pk-yrityksillä ei ole erillisiä tietoturvaosastoja, vaan kyberturvallisuus jää usein muiden IT-tehtävien oheen. Tämä tilanne altistaa pk-yritykset hyökkäyksille, kuten ransomware- ja phishing-hyökkäyksille, joilla voi olla merkittäviä liiketoiminnallisia vaikutuksia (Emer et al., 2021). Resurssien puutteen lisäksi pk-yritykset kohtaavat vaikeuksia kyberriskien priorisoinnissa. Tämä johtuu usein siitä, ettei yrityksillä ole työkaluja riskien tehokkaaseen arviointiin ja niiden liiketoiminnallisten vaikutusten kvantifiointiin. Yksinkertaistetut työkalut, kuten NIST:n kehykseen pohjautuvat arviointimallit, ovat osoittautuneet hyödyllisiksi tässä kontekstissa, mutta niiden käyttöaste on edelleen alhainen Suomessa (Benz & Chatterjee, 2020).

Pk-yritykset ovat usein osa laajempia toimitusketjuja ja liiketoimintaverkostoja, mikä lisää niiden haavoittuvuutta. Yhden toimijan kyberturvallisuuspuutteet voivat altistaa koko verkoston hyökkäyksille, mikä tekee kyberriskien hallinnasta monitahoisen ongelman. Suomessa tämä on erityisen tärkeää valmistavassa teollisuudessa, jossa pk-yritykset toimivat usein kansainvälisten suuryritysten alihankkijoina (Corallo et al., 2023). Verkostoitumisen lisäksi digitalisaation lisääntyminen kasvattaa riskejä, sillä yhä suurempi osa liiketoiminnasta tapahtuu verkossa.

Ihmisten toiminta ja käyttäytyminen ovat merkittävä osa pk-yritysten kyberriskejä. Työntekijöiden koulutuksen puute ja heikko kyberturvallisuustietoisuus lisäävät inhimillisten virheiden riskiä, kuten huolimattomuutta salasanojen hallinnassa tai sähköpostilinkkien klikkaamisessa (Boletsis et al., 2021). Suomessa Kyberturvallisuuskeskus tarjoaa koulutusmateriaaleja ja -ohjelmia, mutta niiden käyttöönotto pk-yrityksissä on edelleen vähäistä. Inhimillisten tekijöiden ohella johtoryhmän ja omistajien asenteet vaikuttavat merkittävästi kyberturvallisuuskulttuurin syntyyn. Tutkimukset osoittavat, että pk-yritykset, joiden johdolla on parempi ymmärrys kyberriskien vakavuudesta, panostavat enemmän ennaltaehkäiseviin toimiin ja koulutukseen (Neri et al., 2022).

Teknologian ja organisaation yhdistäminen on avainasemassa pk-yritysten kyberturvallisuuden parantamisessa. Erityisesti dynaamiset simulaatiotyökalut, kuten SME Cyber Risk Assessment (SMECRA), auttavat yrityksiä arvioimaan kyberriskien dynamiikkaa ja sopeutumaan jatkuvasti muuttuviin uhkiin (Armenia et al., 2021). Tällaiset ratkaisut ovat erityisen hyödyllisiä Suomessa, jossa monilla pk-yrityksillä on teknologista osaamista, mutta ei välttämättä resursseja investoida ulkopuolisiin asiantuntijoihin.

Suomen pk-yritykset ovat kriittisessä asemassa kyberhyökkäysten vaikutusten arvioinnissa, sillä niiden taloudellinen merkitys on suuri mutta valmiudet usein puutteelliset. Näiden yritysten kyberturvallisuuden erityispiirteet vaativat yksinkertaistettuja ja kohdennettuja ratkaisuja, jotka ottavat huomioon resurssien rajallisuuden, inhimilliset tekijät ja toimitusketjujen monimutkaisuuden. Näiden toimien avulla voidaan parantaa pk-yritysten resilienssiä ja vähentää kyberhyökkäysten liiketoiminnallisia vaikutuksia.

3.3 Arviointimenetelmät ja mittarit kyberhyökkäysten vaikutuksien arvioinnissa

Pk-yritykset voivat hyödyntää erilaisia menetelmiä ja mittareita arvioidakseen kyberhyökkäysten vaikutuksia. Tavallisimpia menetelmiä ovat esimerkiksi taloudellisten tappioiden laskeminen, asiakastyytyväisyyskyselyt sekä liiketoiminnan jatkuvuuden mittaaminen. Taloudellisten tappioiden arviointiin voidaan sisällyttää suorat kustannukset, kuten tietojen palauttaminen tai järjestelmien korjaaminen, ja epäsuorat kustannukset, kuten mainehaitat ja menetetyt asiakassuhteet (Cao et al., 2018).

Kyberturvallisuusvaatimusten täyttäminen edellyttää tehokkaita arviointimenetelmiä ja mittareita, jotka ottavat huomioon yritysten resurssirajoitteet ja kyberuhkien moninaisuuden. Arviointimenetelmät keskittyvät pääasiassa riskien tunnistamiseen, kyberturvallisuusvalmiuksien mittaamiseen ja mahdollisten investointien vaikutusten analysointiin.

Esimerkiksi NIST Cybersecurity Framework (CSF) tarjoaa viitekehyksen, jonka avulla voidaan arvioida kyberturvallisuuden viittä keskeistä osa-aluetta: tunnistaminen, suojaaminen, havaitseminen, reagointi ja palautuminen. Tätä viitekehystä on myös

hyödynnetty tässä tutkielmassa. Tämä viitekehys mahdollistaa yritysten itsearvioinnin ja toiminnan parantamisen. Erityisesti pk-yrityksille on kehitetty yksinkertaistettuja kyselypohjaisia arviointityökaluja, kuten Cybersecurity Evaluation Tool (CET), joka mittaa kyberturvallisuuden kypsyyttä (Benz & Chatterjee, 2020).

Riskien arvioinnissa käytettävät mittarit, kuten uhkavaikutusindeksi ja haavoittuvuusindeksi, auttavat kvantifioimaan kyberturvallisuusriskien vakavuutta. Näitä indeksejä voidaan käyttää vertailemaan eri turvallisuusparannusten tehokkuutta ja perustelemaan resurssien kohdentamista. Kvantitatiiviset arviointimallit, kuten SME Cyber Risk Assessment (SMECRA), tarjoavat dynaamisia menetelmiä riskiprofiilien arviointiin ajan myötä ja kyberturvallisuusinvestointien vaikutusten mittaamiseen (Armenia et al., 2021).

Kyberturvallisuusmittareiden suunnittelussa on tärkeää ottaa huomioon myös järjestelmien sosio-tekniset ulottuvuudet. Tämä sisältää inhimilliset tekijät, organisaation kyvykkyydet ja teknologiset resurssit. Uusi viitekehys, joka yhdistää sosio-tekniset ja uhkapohjaiset näkökulmat, tarjoaa pk-yrityksille yksinkertaistettuja ja mukautettavia ratkaisuja riskienhallintaan (van Haastrecht et al., 2021).

Lisäksi arviointimenetelmissä korostetaan jatkuvaa oppimista ja parantamista. Kyberturvallisuuden tietoisuusohjelmien tehokkuuden mittarit, kuten vaikutus, kestävyys, saavutettavuus ja seurantakyky, ovat keskeisiä ohjelmien toimivuuden arvioinnissa. Näiden mittareiden avulla voidaan seurata ohjelmien vaikutusta organisaatioon ja mukauttaa niitä tarpeen mukaan (Chaudhary et al., 2023).

Pk-yrityksille suunnitellut arviointityökalut, kuten mukautettavat kyberturvallisuuskypsyysmallit, tarjoavat yksinkertaisia ratkaisuja monimutkaisten kyberriskien hallintaan. Esimerkiksi Adaptable Security Maturity Assessment and Standardization (ASMAS) -kehys mahdollistaa pk-yritysten kyberturvallisuuden kypsyyden arvioinnin ja parantamisen, samalla kun se ottaa huomioon niiden erityisvaatimukset (Ozkan & Spruit, 2022).

Arviointimenetelmät ja mittarit auttavat pk-yrityksiä tunnistamaan haavoittuvuudet, priorisoimaan parannukset ja seuraamaan kyberturvallisuuden kehitystä. Niiden avulla voidaan myös tehdä tietoisia päätöksiä investoinneista ja kehittää yrityksen kyberturvallisuusstrategioita pitkällä aikavälillä. Pk-yrityksille yksinkertaistetut

työkalut, kuten manuaaliset riskinarviointimallit ja yksinkertaistetut analyysityökalut, voivat olla käytännöllisiä. Suuremmilla yrityksillä on usein käytössään kehittyneitä analysointivälineitä ja kyberturvallisuusosastoja, jotka voivat hyödyntää monimutkaisia riskinhallintamalleja ja reaaliaikaista analytiikkaa. Pk-yrityksillä voi sen sijaan olla tarve yksinkertaisille ja kustannustehokkaille keinoille, kuten kyberturvallisuuden perustason arvioinnille ja asiakaskyselyille, joilla saadaan arvokasta palautetta tietoturvasta ja mahdollisista kyberhyökkäysten vaikutuksista.

3.4 Haasteet ja kehitystarpeet arviointiprosessissa

Pk-yritysten arviointiprosesseihin liittyy useita haasteita, kuten tarve uusille työkaluille, osaamisen puute ja riittämätön kyberturvallisuustietämys. Resurssien puute voi vaikeuttaa tehokkaiden arviointimenetelmien käyttöönottoa, ja tietoturvasta vastaavilla henkilöillä ei välttämättä ole riittävää koulutusta vaikutusten arviointiin. Esimerkiksi sosio-teknisten mallien hyödyntämistä, joka auttaa pk-yrityksiä hahmottamaan ihmisten ja teknologian väliset vuorovaikutukset organisaatiossa ja arvioimaan niihin liittyviä riskejä tehokkaammin (Charitoudi & Blyth, 2014). Tämän lisäksi toimiala, jolla kyseessä oleva yritys toimii vaikuttaa paljon siihen, miten se arvioi vahinkojaan. Yritys, joka valmistaa tuotteita tehtaalla voi suhteellisen helposti arvioida tapahtuneen menetyksen kyberhyökkäyksen vuoksi, mutta Saas (Software as a Service) yrityksellä voi olla tilanne erilainen.

Kehitysratkaisuina pk-yrityksille voidaan suositella koulutuksen lisäämistä ja yksinkertaisten, mutta tehokkaiden arviointityökalujen kehittämistä. Pk-yritykset voivat hyötyä myös yhteistyöstä konsulttien tai ulkoisten tietoturvatoimijoiden kanssa, jotta ne pystyvät paremmin vastaamaan kyberhyökkäysten haasteisiin ja arvioimaan niiden vaikutuksia. Yhteistyö, koulutus ja edulliset työkalut voivat lisätä pk-yritysten kykyä arvioida ja hallita kyberuhkia samalla, kun ne ylläpitävät liiketoiminnan jatkuvuutta.

3.5 Tutkimuksen teoreettinen viitekehys

Tässä tutkielmassa kyberhyökkäysten vaikutusten arviointia lähestytään NIST Cybersecurity Frameworkin (National Institute of Standards and Technology, 2018) kautta. NIST-kehys valittiin tutkimuksen viitekehykseksi sen laajan kansainvälisen hyväksynnän, käytännönläheisyyden ja erityisesti sen soveltuvuuden pk-yritysten tarpeisiin vuoksi. Kehys tarjoaa systemaattisen ja skaalautuvan lähestymistavan

kyberriskien hallintaan, joka voidaan mukauttaa yrityksen koon, toimialan ja kypsyystason mukaan. Viitekehystä hyödyntäen on rakennettu haastattelurunko, jonka tavoitteena on tarkastella pk-yrityksiä sen mukaisesti.

Pk-yrityksille, joilla on usein rajalliset resurssit kyberturvallisuuden kehittämiseen, NIST tarjoaa konkreettisen ja selkeästi jäsennellyn mallin, jonka avulla organisaatio voi arvioida, priorisoida ja kehittää tietoturvavalmiuksiaan. Viitekehyksen viisi keskeistä toimintakategoriaa: Tunnista (Identify), Suojaus (Protect), Havaitse (Detect), Reagoi (Respond) ja Palauta (Recover) muodostavat loogisen etenemispolun, jonka avulla yritys voi rakentaa kattavan kyberturvastrategian. Näiden vaiheiden kautta yritys pystyy ensinnäkin ymmärtämään, mitkä omaisuuserät ovat kriittisiä ja alttiita hyökkäyksille, ja toisaalta varautumaan, reagoimaan ja palautumaan tehokkaasti mahdollisista häiriöistä.

Tutkielman näkökulmasta NIST-viitekehys tukee erityisen hyvin sitä tavoitetta, että kyberhyökkäysten vaikutuksia tarkastellaan liiketoiminnan jatkuvuuden ja riskienhallinnan kautta. Esimerkiksi "Identify"-vaihe tukee pk-yrityksiä ymmärtämään, mitkä resurssit ovat liiketoiminnan kannalta elintärkeitä. "Recover"-vaihe puolestaan auttaa suunnittelemaan käytännön toipumistoimenpiteet, mikä on erityisen tärkeää pk-yrityksille, joille pitkään jatkuva häiriö voi olla kohtalokas.

Lisäksi NIST:n kehystä on kehitetty yhteistyössä sekä julkisen että yksityisen sektorin toimijoiden kanssa, mikä tekee siitä käytännönläheisen ja monilla toimialoilla testatun mallin. Tämä on tärkeää, koska pk-yrityksissä teoreettiset mallit jäävät usein hyödyntämättä, elleivät ne ole sovellettavissa suoraan käytännön toimintaan. Viitekehys on myös dynaaminen: se kannustaa jatkuvaan arviointiin ja kehittämiseen. Kyberuhkien jatkuvasti kehittyessä tämä jatkuvan parantamisen periaate tukee pk-yrityksiä pysymään mukana muuttuvassa uhkaympäristössä. (NIST, 2018).

Kuva 1 NIST kyberturvallisuuden viitekehys (2018)

4 Metodologia

Tutkielmassa tutkimus toteutetaan kvalitatiivisena, jonka avulla perehdytään konkreettisesti tutkimuskysymykseen asianomaisilta pk-yrityksiltä. Jokaisella yrityksellä on omanlainen strategia mahdollisiin kyberhyökkäyksiin, joten kvalitatiivinen tutkimus auttaa ymmärtämään ja löytämään vastauksen tutkimuskysymykseen. Kvalitatiivinen tutkimus mahdollistaa syvällisen ymmärryksen kehittämisen tutkittavasta ilmiöstä (Puusa & Juuti, 2020).

Erityisesti kyberhyökkäysten vaikutusten ymmärtäminen pk-yritysten liiketoimintaan edellyttää perusteellista tietoa siitä, miten nämä hyökkäykset koetaan ja mitä seurauksia niillä on yrityksen toiminnalle. Haastattelut pidetään puolistrukturoituna, jotta saadaan mahdollisimman paljon dataa kerättyä. Puolistrukturoidut haastattelut ovat joustavia, mikä mahdollistaa haastateltavien ainutlaatuisten näkökulmien ja kokemusten esiin tuomisen. Puolistrukturoitu haastattelu sopii erityisesti tilanteisiin, joissa halutaan kerätä tietoa tietyistä ennalta määritellyistä teemoista, mutta samalla antaa haastateltaville tilaa ilmaista omia kokemuksiaan ja näkemyksiään. Tämä menetelmä mahdollistaa sekä aineiston vertailtavuuden että syvällisen ymmärryksen tutkittavasta ilmiöstä. Menetelmän joustavuus tekee siitä hyödyllisen erityisesti silloin, kun tutkitaan monimutkaisia tai henkilökohtaisia aiheita pk-yrityksille, joissa haastateltavien ainutlaatuiset näkökulmat ovat arvokkaita. Tämä menetelmä mahdollistaa sen, että haastattelun aikana voidaan syventyä yksityiskohtiin ja seurata keskustelun luonnollista kulkua, mikä on erityisen hyödyllistä, kun tutkitaan yksityiskohtaista aihetta (Puusa & Juuti, 2020).

4.1 Aineistonkeruu

Tutkielman aineistonkeruu on toteutettu kvalitatiivisena tutkimuksena, hyödyntäen laadullisia haastatteluja. Kvalitatiivinen tutkimusmenetelmä mahdollistaa syvällisen ymmärryksen saavuttamisen tutkittavasta ilmiöstä, erityisesti silloin, kun ilmiö on monimutkainen tai huonosti tunnettu. Tämä menetelmä soveltuu erityisen hyvin tilanteisiin, joissa pyritään ymmärtämään yksilöiden tai organisaatioiden kokemuksia ja näkemyksiä (Eriksson & Kovalainen, 2008).

Haastateltavina ovat olleet kuuden eri toimialalla toimivien pk-yritysten asiantuntijat. Tämä monipuolinen otanta mahdollistaa laajan näkökulman saamisen siitä, miten erilaiset pk-yritykset kokevat kyberhyökkäysten vaikutukset liiketoimintaansa. Kyberhyökkäysten vaikutukset voivat vaihdella suuresti eri toimialoilla, ja siksi on tärkeää ymmärtää näitä eroja syvällisesti (Vuori, 2021).

Kvalitatiiviset haastattelut tarjoavat mahdollisuuden saada syvällistä tietoa haastateltavien kokemuksista ja näkemyksistä. Tämä menetelmä mahdollistaa myös uusien näkökulmien esiin tuomisen, joita ei välttämättä ole aiemmin huomioitu (Puusa & Juuti, 2020). Haastattelujen avulla voidaan saada yksityiskohtaista tietoa siitä, miten pk-yritykset havaitsevat ja käsittelevät kyberuhkia sekä millaisia strategioita ne ovat kehittäneet suojautuakseen näiltä uhilta (Savolainen, 2021).

Kokonaisuudessaan kvalitatiivinen tutkimusmenetelmä ja monipuolinen haastateltavien joukko mahdollistavat syvällisen ja kattavan ymmärryksen saamisen kyberhyökkäysten vaikutuksista pk-yritysten liiketoimintaan. Tämä tieto on arvokasta sekä tutkijoille että käytännön toimijoille, jotka pyrkivät parantamaan pk-yritysten kyberturvallisuutta. Taulukossa 3 on eritelty eri haastatellut henkilöt. Pk-yrityksiä on monenlaisia laidasta laitaan, ja heidän suhtautumisensa kyberturvallisuuteen on vaihtelevaa toimialan mukaan. Tämä tuli esille vahvasti haastatteluiden yhteydessä.

Taulukko 3 Haastatellut

Haastateltava	Toimiala	Haastateltavan rooli	Kesto (min)
H1	Tietokoneplit ja pelikonsolit	CFO	42
H2	IT-tuki / Painotalo	Asiakastuki	29
H3	Tilitoimisto	Toimitusjohtaja	25
H4	Liikkeenjohdon konsultointi	Konsultti	35
H5	Konevuokraus	Controller	30
H6	Televiestintä	Asiantuntija	29

4.2 Datan keruumenetelmä ja analyysi

Tämän tutkimuksen tavoitteena on selvittää, miten eri toimialoilla toimivat pk-yritykset ovat omaksuneet kyberturvallisuutta liiketoiminnassaan ja millaisia näkemyksiä asiantuntijoilla on kyberuhkien vaikutuksista yritysten toimintaan. Empiirinen osuus

perustuu laadulliseen tutkimusmenetelmään, ja aineistonkeruu on toteutettu puolistrukturoitujen haastattelujen avulla. Kvalitatiivinen tutkimus mahdollistaa syvällisen ja kontekstisidonnaisen tiedon keräämisen, mikä on erityisen tärkeää, kun tutkitaan ilmiötä, joka on monitahoinen ja jatkuvasti kehittyvä (Eriksson & Kovalainen, 2008).

Tutkimukseen osallistui asiantuntijoita kuudesta eri toimialalla toimivasta pk-yrityksestä. Haastateltavien valinnassa keskeisenä kriteerinä oli se, että henkilö työskentelee asiantuntijana pk-yrityksessä, mutta liiketoiminnan tarkempaa sektoria ei rajattu pois. Tämä lähestymistapa mahdollistaa laajemman ymmärryksen siitä, miten kyberturvallisuutta omaksutaan erilaisissa liiketoimintaympäristöissä ja mitkä tekijät vaikuttavat yritysten valmiuksiin suojautua kyberuhilta. Toimialojen monimuotoisuus tuo tutkimukseen lisäarvoa, sillä aiemmat tutkimukset ovat osoittaneet, että kyberuhkien vaikutukset vaihtelevat huomattavasti eri toimialojen välillä. Esimerkiksi tietointensiivisillä aloilla, kuten rahoitus- ja teknologiasektorilla, kyberturvallisuus on usein strateginen painopiste, kun taas perinteisemmillä toimialoilla, kuten valmistavassa teollisuudessa, tietoturvatoimenpiteet voivat olla vähemmän kehittyneitä (Puusa & Juuti, 2020).

Aiemman kirjallisuuden perusteella on havaittu, että pk-yrityksillä on rajalliset resurssit kyberturvallisuuden hallintaan verrattuna suuriin yrityksiin, mikä tekee niistä haavoittuvampia kyberhyökkäyksille. Tämä tekee tutkimuksen kannalta erityisen tärkeäksi tarkastella, kuinka eri toimialojen pk-yritykset kokevat kyberturvallisuuden merkityksen ja millaisia strategioita ne ovat kehittäneet suojautuakseen mahdollisilta uhilta (Bada et al., 2015).

Haastatteluaineiston analyysi on toteutettu aineistopohjaisesti, hyödyntäen laadullisen sisällönanalyysin periaatteita. Analyysissä pyrittiin tunnistamaan toistuvia teemoja, jotka liittyivät pk-yritysten kokemiin kyberuhkiin sekä niihin kohdistettuihin suojaustoimiin. Aineiston jäsentelyssä hyödynnettiin osittain etukäteen määriteltyjä teemoja kirjallisuuden pohjalta (kuten phishing-hyökkäykset, palvelunestohyökkäykset, koulutus ja teknologiset suojauskeinot), mutta analyysi mahdollisti myös uusien ilmiöiden esiin nostamisen aineistosta. Haastattelut analysoitiin teemoittain, ja niiden sisällöstä etsittiin yhtäläisyyksiä, eroavaisuuksia ja toistuvia käsitteitä, kuten "etätyön riskit", "lokiseuranta" ja "resurssipula". Näiden pohjalta muodostettiin temaattisia

kokonaisuuksia, jotka heijastavat pk-yritysten käytännön keinoja arvioida ja hallita kyberuhkia liiketoimintansa turvaamiseksi. Näiden pohjalta on muodostettu temaattisia kokonaisuuksia, kuten havaintojen tekeminen, reaktiivinen suojaus ja resurssien riittävyys, jotka lopulta ryhmiteltiin laajemmiksi ulottuvuuksiksi kuten uhkien ymmärrys, vaikutusten arviointi ja valmiudet. Menetelmä mahdollistaa sekä empiirisen havainnoinnin että käsitteellisen abstraktion yhdistämisen, mikä tukee tutkimuksen tavoitteita ymmärtää kyberhyökkäysten vaikutusten arviointia pk-yrityksissä.

Koska kyberturvallisuus voi liittyä yritysten liiketoiminnallisiin salaisuuksiin ja mahdollisiin haavoittuvuuksiin, on tutkimuksessa noudatettu tarkkaa eettistä harkintaa. Tutkimukseen osallistuneiden asiantuntijoiden anonymiteetti on turvattu siten, että heidän henkilöllisyyttään ei paljasteta, vaan haastattelutiedot esitetään vain toimialakohtaisella tasolla. Laadullisen tutkimuksen keskeinen eettinen haaste on varmistaa, että haastateltavat tuntevat olonsa turvalliseksi ja voivat puhua vapaasti ilman pelkoa negatiivisista seurauksista. Tästä syystä haastatteluiden yhteydessä on korostettu, että tutkimuksen tavoitteena ei ole arvioida yksittäisten yritysten haavoittuvuuksia, vaan ymmärtää laajemmin pk-yritysten kyberturvallisuusstrategioita ja niiden kehitystä eri toimialoilla (Eriksson & Kovalainen, 2008).

5 Tutkimuksen tulokset

Tässä osiossa esitellään laadullisen haastattelututkimuksen tulokset, joissa tarkastellaan kyberhyökkäysten vaikutuksia pk-yritysten liiketoimintaan. Haastattelut toteutettiin puolistrukturoituina asiantuntijahaastatteluina, ja niiden kohderyhmänä olivat kuuden eri toimialan edustajat: tietokonepelit ja pelikonsolit, painotalo, tilitoimisto, liikkeenjohdon konsultointi, konevuokraus ja televiestintä. Haastateltavat olivat alansa asiantuntijoita ja vastuussa joko yrityksen kyberturvallisuudesta, riskienhallinnasta tai liiketoiminnan strategisesta kehittämisestä.

Tutkimuksen tavoitteena oli ymmärtää, miten eri toimialoilla arvioidaan kyberhyökkäysten vaikutuksia liiketoiminnalle, millaisia haasteita pk-yritykset kohtaavat kyberuhkien hallinnassa sekä mitkä tekijät vaikuttavat yritysten valmiuteen suojautua ja toipua hyökkäyksistä. Koska haastattelut olivat puolistrukturoituja, keskusteluissa nousi esiin sekä toimialakohtaisia erityispiirteitä että laajempia teemoja, jotka ovat keskeisiä kyberhyökkäysten vaikutusten arvioinnissa pk-yrityksissä. Kaikki haastattelut olivat uniikkeja, eikä suuria samankaltaisuuksia esiintynyt. Tämä johtui monipuolisesti valituista toimialoista. Jatkotutkimuksena voisi toteuttaa samat teemahaastattelut toimialan sisällä ja näin saada tarkempia näkemyksiä.

Haastatteluaineiston analyysin perusteella tulokset on jaettu teemoihin, jotka kuvaavat kyberhyökkäysten vaikutuksia eri näkökulmista. Näitä teemoja ovat muun muassa taloudelliset ja operatiiviset vaikutukset, maineeseen ja asiakassuhteisiin kohdistuvat riskit, yritysten nykyiset kyberturvallisuuskäytännöt sekä niiden kehittämistarpeet. Lisäksi tarkastellaan, miten eri toimialat eroavat toisistaan kyberuhkien kohtaamisessa ja arvioinnissa sekä millaisia resursseja ja strategioita pk-yritykset ovat ottaneet käyttöönsä suojautuakseen kyberhyökkäyksiltä.

Seuraavissa alaluvuissa käsitellään haastatteluaineistosta nousseita keskeisiä havaintoja yksityiskohtaisemmin ja vertaillaan eri toimialojen näkökulmia kyberhyökkäysten vaikutusten arviointiin.

5.1.1 Kyberuhkien ymmärrys ja kokemukset

Kaikki kuusi haastateltavaa toivat esiin, että kyberuhat ovat osa arkipäivää, vaikka niiden vakavuus ja ilmenemismuodot vaihtelevat toimialoittain. Keskeisinä uhkina nousivat esiin erityisesti sähköpostin ja tekstiviestien kautta tapahtuva tietojenkalastelu (phishing) sekä siihen liittyvät valelaskut, väärennetyt lähettäjät ja haitalliset linkit tai liitteet. Haastatellut asiantuntijat työskentelevät eri rooleissa – IT-tuessa, hallinnossa, johdossa ja konsultoinnissa – ja kaikilla oli joko omakohtaisia tai kollegoiden kautta havaittuja kokemuksia kyberuhista.

Erityisesti IT-tehtävissä toimivat vastaajat (esim. Helpdesk, IT-tuki) kertoivat saavansa säännöllisesti ilmoituksia epäilyttävistä sähköposteista, jotka usein liittyivät kalasteluun tai huijauslaskuihin. Esimerkiksi yksi haastateltava kuvasi tilannetta näin: "Yleisimmät ovat sähköpostit, joissa on väärennetty lähettäjän osoite työkaverin nimelle." (H2). Toinen haastateltava (H6) painotti, että phishing-viestit ovat "selkeästi yleisin ja merkittävin uhka", ja niihin on reagoitu poistamalla viestit järjestelmistä ja ohjeistamalla käyttäjiä henkilökohtaisesti.

Laajemmin tarkasteltuna uhkat eivät rajoitu pelkästään yksittäisiin sähköpostiviesteihin, vaan osa vastaajista mainitsi myös tekniset hyökkäykset, kuten SQL-injektioyritykset (H1), sekä sisäiset riskit, kuten käyttäjän huolimattomuuden aiheuttamat tietovuodot tai pääsynhallinnan virheet (H4). Näiden osalta riski kohdistuu erityisesti asiakas- ja henkilötietojen suojaamiseen, mikä on kriittistä esimerkiksi tilitoimistoissa ja finanssialalla.

Useampi haastateltava mainitsi myös etätyön yleistymisen pandemian jälkeen merkittävänä kyberuhkien lisääntymisen syynä. Etätyön myötä nousivat esiin esimerkiksi VPN-yhteyksien turvallisuus, kotitoimistojen fyysiset riskit ja työntekijöiden tekninen osaaminen ilman IT-tuen läsnäoloa. Eräs vastaaja totesi: "*Etätyö toi mukanaan haasteita, erityisesti liittyen VPN-yhteyksiin, laitteen fyysiseen turvallisuuteen sekä siihen, kuinka käyttäjät osaavat toimia ilman lähellä olevaa IT-tukea.*" (H6).

Huomionarvoista on, että vaikka monet vastaajat kokivat uhkat konkreettisina ja säännöllisinä, niiden vakavuus vaihteli toimialan mukaan. Pienemmissä yrityksissä, kuten tilitoimisto tai konevuokraamo, ei ollut koettu varsinaisia hyökkäyksiä, mutta

huijaukset ja kalasteluviestit olivat silti tuttuja. Näissä organisaatioissa korostui myös huoli siitä, että valmiudet tunnistaa tai käsitellä uhkia voivat olla heikompia, koska "*tietoturva ei ole arjessa koko ajan näkyvä aihe*" (H5).

5.1.2 Vaikutusten arviointikäytännöt pk-yrityksissä

Kyberhyökkäysten vaikutusten arviointi osoittautui haastatteluissa monitasoiseksi ja osittain jäsentymättömäksi käytännöksi. Yritysten käytännöt vaihtelivat huomattavasti riippuen toimialasta, yrityksen koosta ja organisaation kyberturvallisuustietoisuudesta. Kaikille yrityksille yhteistä oli kuitenkin se, että järjestelmien käytettävyys ja liiketoiminnan jatkuvuus nousivat tärkeimmiksi mittareiksi silloin, kun hyökkäyksen vaikutuksia pyrittiin arvioimaan.

Useissa vastauksissa korostui se, että suoria, mitattavia arviointimalleja tai ennakolta määriteltyjä mittareita ei välttämättä ollut käytössä, vaan arviointi perustui tapauskohtaiseen tarkasteluun ja riskienhallintaan. Esimerkiksi konsultointiyrityksessä toimiva vastaaja kuvasi asiaa seuraavasti: "*Kyberriskit ovat osa projektien ja asiakastyön arviointia... jos järjestelmään kohdistuisi hyökkäys, se voisi vaikuttaa suoraan asiakkuuteen ja maineeseen."* (H4).

Osa organisaatioista oli kuitenkin selvästi pidemmällä järjestelmällisessä arvioinnissa. Rahapelialalla toimivassa yrityksessä käytettiin ISO/IEC 27001 -sertifiointia, jonka kautta yritys oli luonut rakenteellisen ja dokumentoidun tavan poikkeamien tunnistamiseen, käsittelyyn ja vaikutusten arviointiin. Tämä malli sisälsi säännölliset auditoinnit, tietoturvatiimin kokoukset ja riskien käsittelyprosessit. Sertifiointi nähtiin paitsi riskienhallinnan välineenä myös asiakasluottamuksen kannalta merkittävänä tekijänä.

Suurin osa vastaajista kertoi, että lokitietojen seuranta ja poikkeamien automaattinen tunnistus olivat keskeisiä teknisiä välineitä vaikutusten arvioinnissa. Esimerkiksi televiestintäalan vastaaja kuvasi tilannetta seuraavasti: "*Jos alkaa tulla oudoista IP-osoitteista kirjautumisyrityksiä, niin järjestelmät osaavat nykyään ne huomata ja laittaa tilin suoraan lukkoon.*" (H2).

Toisaalta tilitoimistoissa ja pienemmissä yrityksissä arviointia ei tehty systemaattisesti, vaan toiminta perustui reaktiiviseen käytäntöön: asioihin puututtiin, kun ongelmia ilmeni. Tällaisessa toimintatavassa kyberhyökkäysten vaikutuksia ei aina ymmärretty liiketoiminnan näkökulmasta kattavasti. Esimerkiksi yksi vastaaja totesi: "*Ei ole varsinaisia seurantajärjestelmiä tai mittareita... tietoturvaan liittyviä asioita hoidetaan tarpeen mukaan*." (H3).

Monissa organisaatioissa vaikutusten arviointia tuettiin sisäisten koulutusten ja tapausten läpikäynnin avulla, jolloin opittiin aikaisemmista tilanteista. Muutamassa yrityksessä oli myös käytössä phishing-simulaatioita tai testejä, joiden avulla pyrittiin arvioimaan organisaation kykyä reagoida hyökkäystilanteisiin. Tämä nähtiin osana ennakoivaa toimintaa, vaikka mitattavaa vaikutusten mallintamista ei useinkaan ollut.

Voidaan todeta, että pk-yrityksissä kyberhyökkäysten vaikutusten arviointi perustuu tyypillisesti yhdistelmään teknisistä valvontakeinoista ja inhimillisestä reagoinnista, mutta arviointikäytännöt ovat vielä kehittymässä. Systemaattinen arviointi näyttää olevan vahvemmin läsnä niissä organisaatioissa, joissa asiakkaat tai sääntely vaativat korkeamman kyberturvallisuustason toteuttamista.

5.1.3 Yrityksen valmiudet ja suojaustoimenpiteet

Haastatteluaineistosta nousee esiin huomattavaa vaihtelua siinä, kuinka pk-yritykset ovat varautuneet kyberhyökkäyksiin ja millaisia suojaustoimenpiteitä ne ovat ottaneet käyttöön. Vaikka teknisiä ratkaisuja, kuten monivaiheinen tunnistautuminen, VPN-yhteydet, lokiseuranta ja palomuurit, mainittiin laajasti, organisatoristen valmiuksien taso ja systemaattisuus erosivat selvästi toimialasta ja yrityksen koosta riippuen.

Monessa organisaatiossa suojaustoimenpiteet perustuvat IT- tai tietoturvatiimin toimiin, jotka tukevat muuta henkilöstöä reaktiivisesti. Esimerkiksi IT-tuessa toimiva vastaaja kuvasi arkea seuraavasti: “*Tietoturvatiimi varoittelee sisäverkossa aina, kun tulee jotain uutta mitä pitää huomioida, ja meidänkin työnä on pitää käyttäjät ajantasalla.”* (H2). Myös muilla toimialoilla oli yleisesti käytössä käytäntö, jossa epäilyttävistä viesteistä tai tapahtumista ilmoitetaan keskitetysti IT:lle, joka arvioi tilanteen ja ohjeistaa tarvittaessa.

Useissa organisaatioissa monivaiheinen tunnistautuminen (2FA/MFA) mainittiin merkittävänä konkreettisena parannuksena viime vuosina. Käyttöönotto on kuitenkin aiheuttanut ristiriitaisia reaktioita: "*2-vaiheisen kirjautumisen käyttöönotto melkein jokaiseen palveluun on jo erittäin suuri +, vaikka käyttäjät saattavat vihata sitä ja aiheuttaa muuten 'ongelmaa' työntekoon*." (H2). Tämä havainnollistaa, kuinka turvallisuustoimet voivat joskus olla ristiriidassa työn sujuvuuden kanssa.

Tietoturvakoulutus ja ohjeistus nousivat toisena keskeisenä suojaustoimenpiteenä. Vastaajat kertoivat osallistuneensa erilaisiin tietoturvatesteihin, web-koulutuksiin, tai saaneensa intranetin kautta ohjeita toimintaan hyökkäystilanteissa. Osassa yrityksiä tietoturvakoulutus oli kuitenkin edelleen satunnaista tai riippuvaista ulkopuolisten toimijoiden tarjonnasta. Konsulttialalla ja rahapelialalla koulutuksia järjestettiin säännöllisesti ja ne olivat osa arjen käytäntöjä: "*Tietoturvaa käsitellään arjessa jatkuvasti. Tuntuu, että on matala kynnys kysyä tai ilmoittaa asioista, jos jokin mietityttää.*" (H4).

Teknisten ratkaisujen ja koulutusten lisäksi osa yrityksistä oli ottanut käyttöön myös dokumentoituja toimintamalleja, kuten kyberturvasuunnitelman, jatkuvuussuunnitelman tai incident response -politiikan. Näitä rakenteita hyödynnettiin erityisesti suuremmissa organisaatioissa, joissa asiakas- tai viranomaisvaatimukset edellyttivät selkeää toimintalinjaa. Esimerkiksi rahapelialalla toimiva yritys nojaa ISO 27001 -standardin mukaisiin käytäntöihin ja käy tietoturvatiimin kesken läpi riskejä kuukausittain (H1).

Sen sijaan pienemmissä yrityksissä – kuten tilitoimistoissa tai konevuokrauksessa – organisatoriset valmiudet olivat usein perustasolla tai epämuodollisia. Toimitusjohtajatasolta todettiin: "*Meillä ei ole varsinaista kyberhyökkäyksiin varautumissuunnitelmaa.*" (H3). Valmiudet nojasivat pitkälti yksittäisten työntekijöiden tarkkaavaisuuteen ja tapauskohtaiseen reagointiin, mikä tekee yrityksestä haavoittuvaisemman varsinkin kohdennetuissa hyökkäyksissä.

Yhteenvetona voidaan todeta, että pk-yritysten suojaustoimenpiteet rakentuvat teknisten ratkaisujen, ohjeistusten ja koulutuksen varaan, mutta käytäntöjen järjestelmällisyys vaihtelee. Erityisesti henkilöstön rooli korostuu: tekniset työkalut eivät yksin riitä, jos työntekijät eivät osaa tunnistaa tai raportoida uhkia ajoissa. Organisatorinen kypsyys

näyttäytyy vahvimpana niissä organisaatioissa, joissa tietoturva on integroitu osaksi päivittäistä työtä ja joissa sen kehittäminen on jatkuva prosessi.

5.1.4 Toimialojen väliset erot ja yhtäläisyydet

Haastatteluaineistosta on nähtävissä, että kyberuhkien kokeminen, vaikutusten arviointi ja suojaustoimenpiteet vaihtelevat paitsi yrityskoosta myös toimialakohtaisten erityispiirteitten takia. Vaikka monia yhteisiä huolia, kuten phishing-hyökkäykset ja käyttäjien erehtyminen, esiintyi kaikilla toimialoilla, tietyt erot korostuivat erityisesti siinä, kuinka systemaattisesti riskejä arvioitiin ja miten niihin varauduttiin.

Tietotekniikkaan ja digitaalisiin palveluihin painottuvilla toimialoilla, kuten tietokonepelien ja rahapelien kehittämisessä sekä televiestinnässä, kyberturvallisuus oli useimmiten tiiviimmin integroituna osaksi organisaation arkea. Näissä yrityksissä oli käytössä sertifioituja tietoturvaviitekehyksiä (esim. ISO 27001), säännöllisiä auditointeja sekä ennakoivia toimenpiteitä, kuten phishing-simulaatioita ja jatkuvaa koulutusta. Esimerkiksi rahapelialalla toimiva haastateltava kertoi: “*Meillä on sertifikaattien myötä pakko seurata ja raportoida riskejä, ja se on arkipäivää riskienhallinnan näkökulmasta.*” (H1).

Tietointensiivisillä aloilla, kuten tilitoimistoissa ja liikkeenjohdon konsultoinnissa, painottuivat erityisesti asiakas- ja henkilötietojen suojaaminen sekä toimintakyvyn säilyttäminen. Kuitenkin näissä yrityksissä resurssien rajallisuus vaikutti siihen, kuinka kattavasti uhkia seurattiin. Tilitoimistoissa esimerkiksi arviointi perustui enemmän yksittäisten työntekijöiden huomiokykyyn kuin keskitettyihin teknisiin järjestelmiin. “*Meillä ei ole varsinaisia mittareita tai suunnitelmia, mutta kyllä epäilyttävät sähköpostit osataan huomata ja ilmoittaa.*” (H3).

Perinteisemmän teollisuuden ja palvelujen aloilla, kuten painotalossa ja konevuokrauksessa, kyberturvallisuus näyttäytyi vähemmän priorisoituna. Näissä yrityksissä ei ollut koettu vakavia hyökkäyksiä, ja tietoturvaan liittyvät toimenpiteet olivat pitkälti reaktiivisia. Valmiudet perustuivat yleiseen tietotekniseen varovaisuuteen ja IT-tuen ohjeistuksiin. Eräs konevuokrausyrityksen edustaja totesi: “*Tietoturva ei ole arjessa koko ajan näkyvä aihe. Se on vähän niin kuin taustalla, mutta ei suoraan liiketoiminnan ytimessä.*” (H5).

Yhtäläisyyksiä löytyi kuitenkin kaikilta aloilta. Kaikki haastateltavat kokivat kalasteluyritykset selkeänä, toistuvana riskinä, ja ne olivat monelle ensimmäinen kontaktipinta kyberuhkiin. Lisäksi monivaiheinen tunnistautuminen (2FA) oli otettu käyttöön lähes kaikissa yrityksissä riippumatta toimialasta – vaikka käyttöönotto ei aina sujunut kitkatta. Samoin pandemian jälkeinen etätyön yleistyminen oli lisännyt kyberriskejä toimialasta riippumatta ja tuonut uudenlaista painetta henkilöstön kouluttamiseen.

Yhteenvetona voidaan todeta, että toimialat vaikuttavat merkittävästi siihen, kuinka vakavasti kyberuhkiin suhtaudutaan, kuinka hyvin niihin on varauduttu ja millä tasolla organisaation valmiudet ovat. Teknologia- ja sääntelyintensiivisillä aloilla on usein paremmat rakenteet ja valmiudet, kun taas perinteisemmillä palvelualoilla tietoturva on usein enemmän yksittäisten toimijoiden varassa. Kaikilla toimialoilla on kuitenkin yhteinen haaste: henkilöstön kyky havaita ja raportoida uhkia ajoissa.

5.1.5 Kehitysehdotukset ja asiantuntijoiden näkökulmat

Haastatelluilta pyydettiin myös näkemyksiä siitä, miten yritysten kyberturvallisuutta voisi kehittää ja kuinka työntekijöitä voitaisiin paremmin valmistaa mahdollisiin uhkiin. Vastauksista nousi esiin useita ehdotuksia, jotka painottuivat erityisesti koulutuksen, tiedottamisen ja käytännönläheisten esimerkkien lisäämiseen. Vaikka osa vastaajista koki nykyiset toimet riittäviksi, moni näki selkeitä kehityskohteita.

Yleisin ehdotus oli säännöllisten tietoturvakoulutusten ja testien jatkaminen ja laajentaminen. Useissa yrityksissä oli käytössä esimerkiksi vuosittainen tietoturvatesti, jonka nähtiin lisäävän työntekijöiden ymmärrystä konkreettisista riskeistä. Yksi haastateltava tiivisti näkemyksen seuraavasti: “*Tietoturvatesti, joka meillä on, ja käyttäjille tiedotteet eri hyökkäysuhkista mitä muille firmoille on tapahtunut, ovat tehokkaita.*” (H2).

Monet vastaajat korostivat myös esimerkkien ja käytännön tapausten merkitystä: pelkkä teoria ei aina riitä, vaan työntekijöitä auttaa eniten ymmärrys siitä, miten kyberhyökkäykset tapahtuvat oikeasti ja mitä seurauksia niillä voi olla. Tässä nähtiin

uutisista poimittujen tapausten hyödyntäminen tärkeänä työkaluna tietoisuuden lisäämiseksi.

Reagointiin liittyvä ohjeistus oli toinen keskeinen kehitysteema. Vaikka useimmat vastaajat tiesivät, kenelle ilmoittaa epäilyttävistä tapauksista, useampi toivoi selkeämpiä ja näkyvämpiä toimintamalleja. "*Itse pitää aina raportoida, mutta voisi olla selkeämpi muistutus tai 'mitä teen kun…' -ohje helposti näkyvillä.*" (H3). Tämä ehdotus ilmentää tarvetta madaltaa kynnystä ilmoittaa epäilyistä ja varmistaa, että kaikki työntekijät tietävät oikean toimintatavan.

Toisaalta osa vastaajista koki, että yrityksen valmiudet ovat jo riittävällä tasolla, ja tärkeintä olisi vain säilyttää nykyinen valppaus ja mukautua uusiin uhkiin. Esimerkiksi rahapelialalla tietoturva koettiin osaksi arjen tekemistä: "*Meillä tietoturva on osa jatkuvaa tekemistä, mutta pitää silti olla hereillä. Uhkat kehittyvät nopeammin kuin suojautuminen.*" (H1).

Yhteisenä huolena nousi esiin se, että uhat muuttuvat jatkuvasti, ja työntekijöiden on vaikea pysyä perässä, ellei yritys tue jatkuvaa oppimista. Samalla moni vastaaja oli tietoinen siitä, että pk-yrityksissä resurssit ovat rajalliset, joten kehitystoimet tulisi kohdistaa juuri niihin osa-alueisiin, joissa ihmisten toiminta vaikuttaa eniten – kuten sähköpostin avaamiseen, salasanojen hallintaan ja raportointiin.

Haastateltavat näkivät työntekijöiden roolin keskeisenä osana kyberturvallisuutta. He toivoivat lisää konkreettista tukea, käytännönläheistä viestintää ja matalan kynnyksen ohjeita epäilyttäviin tilanteisiin reagoimiseksi. Vaikka teknisiä suojauksia pidettiin tärkeinä, ihmisten tietoisuus, koulutus ja kyky toimia oikein muodostivat haastateltavien näkökulmasta tehokkaimman suojan kyberuhkia vastaan.

5.1.6 Haastatteluiden yhteenveto

Tutkimuksen tavoitteena on ollut selvittää, miten pk-yritykset arvioivat ja hallitsevat kyberhyökkäysten uhkia liiketoimintansa turvaamiseksi. Haastatteluaineiston analyysissä on sovellettu laadullista sisällönanalyysia, jossa aineistoa tarkasteltiin aineistopohjaisesti mutta osin myös deduktiivisesti hyödyntäen kirjallisuudessa esiintyviä kyberuhkien ja suojaustoimien luokitteluja. Tämä lähestymistapa mahdollisti

sen, että yksittäisten haastateltavien kokemuksista ja näkemyksistä voitiin tunnistaa keskeisiä teemoja, kuten kyberuhkien tunnistaminen, suojauskäytännöt ja resurssirajoitteet. Näiden pohjalta muodostui kokonaiskuva siitä, miten pk-yritykset kokevat kyberuhat ja miten ne pyrkivät arvioimaan ja hallitsemaan niiden vaikutuksia liiketoimintaansa.
Tulosten perusteella yleisin ja toistuvin havainto liittyi phishing-hyökkäyksiin, jotka mainittiin kaikissa kuudessa haastattelussa. Kalasteluyritykset koettiin konkreettisena ja toistuvana uhkana riippumatta toimialasta, ja ne näyttäytyivät myös ensisijaisena kontaktipintana kyberhyökkäyksiin. Tämä havainto on linjassa aiemman tutkimuksen kanssa, jonka mukaan tietojenkalastelu on pk-yrityksille yleisin ja kustannustehokkain hyökkäystapa (ENISA, 2020; Jansson & von Solms, 2011). Kalasteluun liittyvät ilmiöt kuten valelaskut ja väärennetyt lähettäjät mainittiin useassa haastattelussa, ja ne ovat usein ensimmäinen merkki mahdollisesta laajemmasta hyökkäyksestä.

Haastattelut osoittivat myös, että etätyön yleistyminen pandemian jälkeen on lisännyt tietoturvariskejä. Työskentely kotitoimistoista, puutteellisesti suojatuilla verkoilla ja laitteilla, on lisännyt riskiä paitsi phishing-viesteihin reagoimisessa, myös vääränlaisen käyttäytymisen yleistymisessä. Tämä on havaittu myös aiemmassa kirjallisuudessa, jossa on korostettu sosiaalisen manipulaation tehostumista etätyöaikana (Burda et al., 2023).

Analyysin seuraava keskeinen havainto liittyy siihen, että kyberhyökkäysten vaikutusten arviointi oli useimmiten epämuodollista ja tapauskohtaista. Vain harvoissa yrityksissä oli käytössä muodollisia mittareita tai rakenteita, kuten riskianalyysejä tai palautumissuunnitelmia. Tämä on yhteneväinen esimerkiksi Romanoskyn (2016) näkemyksen kanssa, jonka mukaan pk-yrityksissä vaikutusten arviointi jää usein reaktiiviseksi, eikä sitä integroida osaksi strategista riskienhallintaa. Haastatteluissa vaikutuksia arvioitiin ensisijaisesti järjestelmien käytettävyyden, asiakaspalvelun toimivuuden ja maineen kannalta, mutta taloudelliset mittarit, kuten tappioiden arviointi euroissa, jäivät useimmiten käyttämättä.

Toisaalta useimmissa yrityksissä oli otettu käyttöön teknisiä suojaustoimenpiteitä, kuten lokitietojen seuranta, monivaiheinen tunnistautuminen (2FA) ja haitallisen liikenteen automaattinen esto. Näiden käyttö oli kuitenkin vaihtelevaa, eikä niitä aina tuettu

organisaatiotasoisella tietoturvastrategialla. Esimerkiksi NIST:n kyberturvallisuuskehikko (2018), jota tutkielman viitekehyksessä hyödynnetään, korostaa vaikutusten arvioinnin ja toipumisen suunnitelmallisuutta – mutta vain yhdessä haastatellussa yrityksessä viitattiin eksplisiittisesti standardoidun viitekehyksen käyttöön.

Koulutus ja tiedottaminen työntekijöille nousivat haastatteluissa tärkeimmäksi keinoksi torjua uhkia organisaatiotasolla. Useampi haastateltava mainitsi tietoturvatestien, sisäisten viestien ja arjen neuvonnan merkityksen erityisesti phishingin torjumisessa. Tämä vahvistaa Hadlingtonin (2017) ja Bada et al. (2015) esittämää näkemystä, jonka mukaan käyttäjien käyttäytyminen ja tietoisuus ovat keskeisiä tekijöitä organisaation kyberturvallisuuden kokonaisvalmiudessa.

Toimialojen välillä havaittiin merkittäviä eroja siinä, kuinka pitkälle kyberturvallisuus oli integroitu osaksi liiketoiminnan johtamista. Esimerkiksi rahapeli- ja televiestintäalalla toiminut yritys noudatti selkeästi dokumentoituja ja sertifioituja tietoturvakäytäntöjä, kun taas perinteisemmillä toimialoilla – kuten konevuokrauksessa tai tilitoimistoissa – turvallisuustoimet perustuivat yksittäisten työntekijöiden huomiokykyyn ja IT-tuen osaamiseen. Tämä on linjassa Ponsard et al. (2019) ja Armenia et al. (2021) kanssa, jotka osoittavat, että resurssien ja kyberkypsyystason erot ovat merkittäviä pk-sektorilla.

Alla oleva kooste tiivistää keskeiset haastatteluista nousseet teemat ja niiden yleisyyden:

Taulukko 4 Kooste haastatteluista

Teema	Mainittu (x/6)
Phishing-hyökkäykset	6/6
Etätyön riskit	4/6
Lokiseuranta ja automaattinen tunnistus	5/6
2FA / monivaiheinen tunnistautuminen	6/6
Tietoturvatestit / koulutus	5/6
Kyberhyökkäysten liiketoimintavaikutusten arvio-inti	3/6

Dokumentoitu varautumissuunnitelma	2/6
Sertifioitu viitekehys (esim. ISO 27001)	1/6
IT-tuen aktiivisuus ja ohjeistus	4/6
Käyttäjien oma-aloitteisuus ja valppaus	5/6
Phishing-simulaatiot / testit	2/6
Tietoturvatiimin olemassaolo	3/6

Phishing-hyökkäykset (6/6)

Kaikki kuusi haastateltavaa nostivat phishing-hyökkäykset keskeisimmäksi kyberuhkaksi, johon he olivat työssään tai organisaatiossaan käytännössä toistuvasti kohdanneet. Phishing ilmenee erityisesti väärennettyinä lähettäjäosoitteina, tekaistuina työkaverin nimissä lähetettyinä sähköposteina, huijauslaskuina sekä linkkeinä, jotka ohjaavat kirjautumissivustoille tunnusten kalastelua varten. Useissa vastauksissa korostui se, että phishing on "arkiuhka", joka toistuu kuukausittain ja on tuttu suurimmalle osalle henkilöstöä.

Ilmiön yleisyys liittyy sen tekniseen yksinkertaisuuteen ja siihen, että se kohdistuu nimenomaan inhimilliseen toimintaan. Kuten ENISA (2020) ja Jansson & von Solms (2011) tuovat esiin, phishing on edelleen pk-yritysten yleisin ja tehokkain kohdehyökkäys, erityisesti silloin, kun henkilöstön tietoturvatietoisuus on puutteellista. Myös Hadlingtonin (2017) mukaan tällaiset sosiaaliseen manipulointiin perustuvat hyökkäykset ovat vaarallisimpia juuri siksi, että ne onnistuvat usein ilman teknisten suojausten murtamista.

Phishingin torjunnassa keskeiseksi tekijäksi nousi koulutus ja henkilöstön reagointikyky. Yritykset, joissa käytettiin tietoturvatestejä ja simulaatioita, kokivat pystyvänsä paremmin valmistamaan henkilöstöä tunnistamaan uhkia. Kuitenkin vain

kahdessa organisaatiossa mainittiin phishing-simulaatioiden käyttö koulutuksen välineenä, mikä viittaa kehitystarpeeseen myös tässä osa-alueessa.

Haastateltavat kuvasivat myös, kuinka kalasteluyritykset usein havaitaan joko henkilöstön oma-aloitteisesti tai vasta, kun käyttäjän tunnus menee lukkoon epäilyttävien kirjautumisyritysten vuoksi. Tämä tukee näkemystä siitä, että vaikka teknisiä suojauskeinoja, kuten 2FA ja lokiseuranta, on käytössä, ensisijainen puolustuslinja muodostuu edelleen henkilöstön toiminnasta ja valppaudesta.

Phishing-hyökkäykset muodostavat merkittävimmän ja konkreettisimman kyberuhan pk-yrityksille. Niiden torjuminen edellyttää teknisten kontrollien ohella erityisesti jatkuvaa koulutusta, tietoisuuden lisäämistä ja organisaation reagointikyvyn kehittämistä. Phishing toimii tässä aineistossa myös esimerkkinä siitä, miten kyberuhkien arviointi ja hallinta perustuvat sekä teknisiin että inhimillisiin tekijöihin, joiden tasapaino on ratkaiseva organisaation resilienssin kannalta.

Etätyön riskit (4/6)

Neljä haastateltavaa toi esiin etätyön tuomat uudet tai korostuneet kyberturvallisuusriskit, erityisesti pandemian jälkeen, jolloin etätyö yleistyi nopeasti ja pysyvästi. Etätyöhön liittyviä riskejä kuvattiin muun muassa työskentely-ympäristön valvomattomuuden, laitteiden yhteiskäytön ja teknisen tuen etäisyyden kautta. Yksi vastaajista totesi: “Huijaukset lähti huomattavaan nousuun, kun muutenkin sähköpostit ja muut elektroniset kanssakäymiset nousi”, mikä havainnollistaa, kuinka etätyö lisää sähköisten viestintäkanavien haavoittuvuutta sosiaaliselle manipuloinnille.

Etätyö tuo mukanaan tilanteen, jossa työntekijät joutuvat tekemään nopeita päätöksiä ilman kollegoiden tai IT-tuen tukea. Tämä luo riskin, jossa inhimilliset erehdykset pääsevät toteutumaan helpommin. Hadlingtonin (2017) mukaan etätyöympäristöissä korostuvat erityisesti henkilöstön oman vastuun ja tietoisuuden merkitys, sillä tekninen valvonta ei tavoita kaikkia arjen tilanteita. Burda et al. (2023) ovat tuoneet esiin, että etätyön psykososiaalinen kuormitus, esimerkiksi perhe-elämän ja työn yhdistäminen, voi heikentää keskittymistä ja lisätä virhealttiutta.

Käytännössä osa haastateltavista kertoi, että etätyön vuoksi järjestelmiin oli otettu käyttöön lisäsuojausta, kuten VPN-yhteydet ja kaksivaiheinen tunnistautuminen (2FA). Näistä huolimatta todettiin, ettei kaikkia etätyöhön liittyviä riskejä ollut täysin ymmärretty tai analysoitu. Esimerkiksi kotiverkkojen suojaus, henkilökohtaisten laitteiden käyttö sekä työn ja vapaa-ajan rajojen hämärtyminen olivat edelleen haavoittuvuuksia, joita ei kattavasti hallittu.

NIST:n (2018) viitekehys korostaa, että muuttuvat työskentelytavat edellyttävät uutta riskien tunnistamista ja jatkuvaa arviointia. Etätyön kohdalla tämä tarkoittaa, että yritysten tulisi tunnistaa, dokumentoida ja päivittää uhkakuvia aktiivisesti, ei vain reagoida tapahtuneisiin poikkeamiin. Haastatteluista kävi ilmi, että tätä ei useinkaan tehty systemaattisesti, vaan varautuminen oli enemmän reaktiivista ja hajautunutta.

Etätyö on tuonut pk-yrityksille uusia tietoturvahaasteita, joihin ei vielä kaikilta osin ole ehditty tai osattu vastata. Teknologiset ratkaisut ovat tärkeitä, mutta niihin on liityttävä myös prosesseja, koulutusta ja viestintää, jotta etätyön riskejä voidaan hallita kokonaisvaltaisesti ja ennakoivasti.

Tietoturvatestit ja koulutus (5/6)

Viisi haastateltavaa kuudesta mainitsi, että heidän organisaatiossaan henkilöstön koulutukseen ja tietoisuuden lisäämiseen liittyvät toimet olivat osa kyberturvallisuuden ylläpitämistä. Käytännöt vaihtelivat suuresti: jotkut yritykset hyödynsivät vuosittaisia tietoturvatestejä tai verkkokoulutuksia, kun taas toiset järjestivät tietoiskuja ja lähettivät säännöllisiä tiedotteita ajankohtaisista uhkista.

Koulutuksen merkitys nähtiin tärkeänä erityisesti siksi, että suurin osa uhista kohdistuu käyttäjiin. Hadlingtonin (2017) tutkimuksen mukaan työntekijän tietoturvakäyttäytyminen muodostuu monista tekijöistä, joihin voidaan vaikuttaa vain koulutuksen ja organisaatiokulttuurin kautta. Sama käy ilmi myös Bada et al. (2015) tutkimuksesta, jossa korostetaan käyttäjän roolia ensilinjan puolustajana.

Erityisesti phishingin torjumisessa koulutuksella on olennainen merkitys. Useat haastateltavat mainitsivat, että koulutuksen avulla henkilöstö osaa nykyään paremmin

tunnistaa huijausviestit ja epätavallisen viestinnän. Lisäksi osassa yrityksiä oli otettu käyttöön phishing-simulaatioita, joiden avulla testattiin henkilöstön valppautta käytännön tilanteissa. Kuitenkin näitä simulaatioita käytti vain kaksi yritystä, mikä osoittaa, että käytännönläheinen koulutus ei ole vielä vakiintunut toimintatapa.

Haastateltavat pitivät koulutusta usein riittävänä, mutta samaan aikaan toivottiin lisää konkreettisia esimerkkejä ja ajankohtaista tietoa uhkakuvista. Tämä viittaa siihen, että koulutuksen tulee olla jatkuvaa ja reaktiivista – ei vain ennalta laadittua, vaan myös ajankohtaiseen uhkaympäristöön vastaavaa. Koulutus ja henkilöstön sitouttaminen ovat kriittisiä osia pk-yritysten kyberturvallisuusstrategiaa. Tietoturvatestit ja simulaatiot tarjoavat tehokkaan tavan kehittää organisaation kykyä reagoida uhkiin ja ovat näin ollen olennainen osa resilienssin rakentamista.

Kyberhyökkäysten vaikutusten arviointi (3/6)

Vain kolme kuudesta haastateltavasta toi esiin, että heidän yrityksessään arvioidaan järjestelmällisesti kyberhyökkäysten vaikutuksia liiketoimintaan. Usein vaikutusten arviointi perustui yksittäisiin poikkeustapauksiin, eikä arviointi ollut osa jatkuvaa riskienhallinnan prosessia. Näissä yrityksissä vaikutuksia pohdittiin lähinnä siltä osin, kuinka hyökkäykset vaikuttaisivat asiakaspalvelun jatkuvuuteen, liiketoimintaprosessien keskeytyksettömyyteen tai yrityksen maineeseen.

Tämä havainto tukee Romanoskyn (2016) analyysia, jonka mukaan monet pk-yritykset eivät kykene kvantifioimaan kyberhyökkäysten vaikutuksia systemaattisesti. Vaikka uhkia osataan tunnistaa ja torjua, niiden mahdollisia liiketoiminnallisia seurauksia ei aina kyetä arvioimaan. Tämä voi johtaa siihen, että riskienhallinnan ja strategisen päätöksenteon välillä on katkos – erityisesti, kun konkreettisia mittareita ei ole määritelty.

Haastateltavat, jotka arvioivat vaikutuksia järjestelmällisemmin, tekivät sen usein ulkoisten vaatimusten, kuten sertifiointien tai asiakasvaatimusten vuoksi. Erityisesti ISO 27001 -sertifioidussa organisaatiossa vaikutusten arviointi oli dokumentoitu osa tietoturvakäytäntöjä.

Yhteenvetona voidaan todeta, että kyberhyökkäysten vaikutusten arviointi ei ole pk-yrityksissä vielä systemaattisesti jäsenneltyä. Arviointi tapahtuu pääosin tapauskohtaisesti ja jää usein teknisten ratkaisujen varaan ilman laajempaa liiketoimintanäkökulmaa.

Dokumentoitu varautumissuunnitelma (2/6)

Kaksi haastateltua mainitsi, että heidän organisaatiollaan oli olemassa kirjallinen varautumissuunnitelma kyberhyökkäysten varalle. Useimmissa tapauksissa kuitenkin varautuminen perustui enemmän yleiseen toimintakulttuuriin ja epämuodollisiin käytäntöihin kuin dokumentoituihin prosesseihin. Tämä viittaa siihen, että systemaattinen toipumissuunnittelu on edelleen vähäistä.

NIST:n kyberturvallisuusviitekehyksen (2018) "Respond"- ja "Recover"-vaiheet korostavat sitä, että kyberhyökkäyksiin tulee varautua ennalta määritellyin toimintamallein, jotta häiriöistä voidaan palautua tehokkaasti. Tämä ajattelu ei vielä näkynyt vahvasti aineistossa, mikä voi johtua sekä resurssien rajallisuudesta että kokemuksen puutteesta.

Yrityksissä, joissa varautumissuunnitelma puuttui, luotettiin usein siihen, että IT-tuki hoitaa tilanteet tai että tekniset järjestelmät (kuten tilin automaattinen lukitus) riittävät suojaksi. Tällainen lähestymistapa voi kuitenkin johtaa siihen, että laajemmat vaikutukset jäävät arvioimatta ja toipumista ei suunnitella riittävän kattavasti. Dokumentoitu varautuminen on harvinaista, vaikka sen merkitys on olennainen organisaation kyberresilienssin rakentamisessa.

Sertifioitu viitekehys, esim. ISO 27001 (1/6)

Ainoastaan yksi haastateltavista työskenteli organisaatiossa, jossa oli käytössä sertifioitu kyberturvallisuusviitekehys (ISO 27001). Tällöin kyberturvallisuus oli integroitu koko liiketoiminnan prosesseihin ja arviointikäytännöt oli dokumentoitu osaksi päivittäistä työtä.
Tämä tukee Ponsard et al. (2019) ja Armenia et al. (2021) esittämiä havaintoja siitä, että sertifioidut viitekehykset tukevat pk-yrityksiä systemaattisessa riskienhallinnassa ja

turvallisuustoimien jatkuvassa kehittämisessä. Samalla kuitenkin voidaan todeta, että näiden käyttöönotto on pk-sektorilla vielä hyvin vähäistä.

Sertifikaatin puuttuminen ei välttämättä tarkoita, että yritys ei hoitaisi tietoturvaa, mutta sen avulla on mahdollista luoda järjestelmällinen ja mitattava pohja jatkuvalle kehittämiselle ja ulkoiselle uskottavuudelle. Näin ollen sertifiointi toimii paitsi sisäisenä ohjauksen välineenä myös kilpailuetuna esimerkiksi asiakassuhteissa.

IT-tuen aktiivisuus ja ohjeistus (4/6)

IT-tuki nousi tärkeäksi toimijaksi etenkin pienemmissä yrityksissä, joissa ei ollut omaa tietoturvatiimiä. Neljä haastateltavaa mainitsi, että IT-henkilöstö vastaa kyberturvallisuuteen liittyvästä neuvonnasta, ohjeistuksesta ja ensivasteesta poikkeustilanteissa. Tällaisissa tilanteissa IT-tuen rooli on ratkaiseva, sillä he ovat usein ensimmäinen kontakti, jolta työntekijät saavat neuvoja esimerkiksi epäilyttävän viestin saatuaan. Samalla tämä osoittaa, että tekninen osaaminen on keskittynyt harvoille, mikä voi aiheuttaa haavoittuvuutta resurssien ollessa rajalliset.

IT-tuki toimii käytännön "suojauskerroksena", joka tukee sekä teknistä toteutusta että käyttäjien toimintaa. Heidän aktiivinen viestintänsä uusista uhkista ja toimintamalleista vahvistaa tietoturvatietoisuutta koko organisaatiossa.

Käyttäjien oma-aloitteisuus ja valppaus (5/6)

Viisi haastateltavaa korosti, että käyttäjien oma-aloitteinen toiminta, kuten epäilyttävien viestien raportointi ja yleinen valppaus, on merkittävä osa organisaation kyberresilienssiä. Työntekijöiden halukkuus ja kyky reagoida oikein nähdään keskeisenä onnistumisen edellytyksenä. Hadlingtonin (2017) mukaan tietoturvapoikkeamien tehokas havaitseminen ja raportointi edellyttävät sekä tietoa että asennetta, ja nämä muodostuvat ennen kaikkea kulttuurista ja koulutuksesta. Organisaatiot, joissa valppaus oli sisäistetty arjen käytäntöihin, vaikuttivat olevan parhaiten varautuneita uhkiin.

Phishing-simulaatiot / testit (2/6)

Kuten aiemmissa osioissa on mainittu, vain kahdessa yrityksessä oli käytössä phishing-simulaatioita osana henkilöstön koulutusta. Näissä organisaatioissa työntekijöitä altistettiin tarkoituksella huijaussähköpostien kaltaisille viesteille, joiden tarkoitus oli testata käyttäjien kykyä tunnistaa epäilyttäviä viestejä ja raportoida niistä. Tämä koettiin tehokkaaksi tavaksi lisätä tietoisuutta ja valmistautua todellisiin uhkiin.

Haastateltavat, joiden organisaatioissa näitä simulaatioita käytettiin, pitivät niitä konkreettisina ja opettavaisina. Ne herättivät keskustelua ja antoivat suoraa palautetta käyttäjien toiminnasta. Tämä puolestaan auttoi luomaan avoimempaa tietoturvakulttuuria. Vaikka simulaatiot voivat alkuun herättää hämmennystä tai ärtymystä, ne toimivat tehokkaana työkaluna silloin, kun ne ovat osa jatkuvaa ja rakentavaa oppimisprosessia.

Suurimmassa osassa pk-yrityksistä tällaista käytäntöä ei kuitenkaan ollut otettu käyttöön, mikä viittaa siihen, että resursseja tai osaamista ei aina ole hyödynnetty täysimääräisesti.

Tietoturvatiimin olemassaolo (3/6)

Kolme organisaatiota mainitsi erillisen tietoturvatiimin olemassaolon, mikä viittaa tietoturvan institutionaaliseen asemaan kyseisissä yrityksissä. Näissä organisaatioissa tietoturva ei ollut vain IT-osaston vastuulla, vaan sitä hallinnoitiin systemaattisesti erillisen toiminnon kautta. Tämä mahdollisti aktiivisen tiedottamisen, koulutusten suunnittelun ja uhkien jatkuvan seurannan.

Tietoturvatiimin olemassaolo mahdollistaa sen, että kyberturvallisuutta johdetaan strategisesti eikä ainoastaan operatiivisesti. Tällöin voidaan suunnitella pitkäjänteisiä kehitystoimia, arvioida riskien vaikutuksia liiketoimintaan ja rakentaa palautumismalleja häiriötilanteita varten. Tämä on linjassa Collierin ja D’Annan (2023) näkemyksen kanssa, jonka mukaan tietoturvan vakiinnuttaminen osaksi organisaatiostrategiaa on keskeinen osa kyberturvallisuuden kypsyyden kasvua.

Toisaalta haastatteluissa korostui, että pk-yrityksissä ei usein ole resursseja ylläpitää omaa tietoturvatiimiä. Näissä tapauksissa tietoturvavastuu jakautuu IT-tuen ja johdon kesken, mikä voi johtaa koordinaation puutteeseen ja epäselviin vastuunjakoihin. Tällöin tietoturva jää helposti yksittäisten henkilöiden varaan ja reagointi perustuu enemmän yksittäisiin tilanteisiin kuin ennakoivaan suunnitteluun.

6 Yhteenveto ja jatkoa tutkimukselle

Tässä pro gradu -tutkielmassa tutkittiin, miten pienet ja keskisuuret yritykset (pk-yritykset) arvioivat ja hallitsevat kyberhyökkäysten uhkia liiketoimintansa turvaamiseksi. Kyseessä on ajankohtainen ja monimutkainen ilmiö, jonka merkitys on kasvanut viime vuosien aikana erityisesti digitalisaation, etätyön yleistymisen ja globaalien kyberuhkien lisääntymisen myötä. Tutkimus yhdisti kirjallisuuskatsauksen ja empiirisen laadullisen aineiston, joka kerättiin puolistrukturoitujen asiantuntijahaastattelujen avulla. Aineiston analyysi toteutettiin aineistopohjaisesti, hyödyntäen laadullisen sisällönanalyysin menetelmiä. Analyysissa tunnistettiin toistuvia teemoja haastateltavien puheesta, ja näitä verrattiin kirjallisuudessa esitettyihin kyberuhkiin ja suojaustoimenpiteisiin, mikä mahdollisti käytäntöjen ja valmiuksien tarkastelun sekä teorian, että käytännön näkökulmasta.

6.1 Keskeiset löydökset: Mitä pk-yritykset tekevät ja mitä jää tekemättä

Tutkimuksen keskeinen löydös oli, että pk-yritykset kokevat kyberhyökkäysten arvioinnin tärkeänä mutta usein vaikeasti lähestyttävänä asiana. Vaikka organisaatiot ovat tietoisia kyberhyökkäysten kasvavasta uhkasta, ei niillä useinkaan ole selkeitä prosesseja arvioida hyökkäysten vaikutuksia järjestelmällisesti. Tämä ilmenee esimerkiksi siinä, että monet haastatellut yritykset arvioivat vaikutuksia vasta tapahtuneen hyökkäyksen jälkeen – retrospektiivisesti eikä proaktiivisesti. Tämä tukee Bendovschin (2015) ja Romanoskyn (2016) havaintoja siitä, että kyberriskien arviointi perustuu usein reaktiivisuuteen, ei ennakointiin.

Useat haastateltavat nostivat esiin, että arvioinnissa keskitytään ensisijaisesti välittömiin vaikutuksiin kuten järjestelmien käyttökatkoksiin, tulonmenetyksiin ja lunnasmaksuihin. Sen sijaan epäsuoria vaikutuksia – kuten maineen heikkenemistä, asiakassuhteiden murentumista tai työntekijöiden kuormittumista – arvioidaan harvemmin systemaattisesti. Tämä on ongelmallista, sillä juuri nämä epäsuorat seuraukset voivat pitkällä aikavälillä osoittautua kaikkein vakavimmiksi (Cavusoglu et al., 2004; Huang et al., 2018).

Vaikka useat pk-yritykset olivat tietoisia erilaisista viitekehyksistä, kuten NIST:n Cybersecurity Frameworkista (2018), vain harva hyödynsi niitä käytännössä. Esteiksi mainittiin resurssien puute, osaamisvaje ja se, ettei kehikon terminologia aina resonoi pk-yritysten arjessa. Tässä on selkeä kehitystarve: viitekehysten tulisi olla selkokielisempiä ja helpommin sovellettavissa erilaisiin organisaatiokonteksteihin. Tämä tukee havaintoa, jonka mukaan standardien soveltaminen jää usein suurten organisaatioiden varaan, vaikka ne olisivat arvokkaita myös pienemmille toimijoille (NIST, 2018; Collier & D'Anna, 2023).

6.2 Phishing hyökkäysten erityinen uhka

Tutkimuksessa nousi erityisesti esiin phishing-hyökkäysten rooli. Ne nähtiin merkittävimpinä ja yleisimmin esiintyvinä hyökkäyksinä, jotka usein toimivat porttina vakavampiin kyberrikoksiin. Phishing-hyökkäykset perustuvat käyttäjien manipulointiin ja työntekijöiden inhimillisiin virheisiin, minkä vuoksi niiden torjuminen on erityisen haastavaa (ENISA, 2020; Jansson & von Solms, 2011). Haastatteluissa kävi ilmi, että phishing-hyökkäyksiltä suojautuminen riippuu pitkälti yksittäisten työntekijöiden tietoisuudesta ja koulutuksesta, eikä järjestelmällisiä testauksia tai simuloituja hyökkäysharjoituksia ollut juuri käytössä.

Phishing-hyökkäysten vaikutukset ovat paitsi teknisiä, myös psykologisia ja organisatorisia. Yrityksen työntekijät saattavat menettää itsevarmuutensa tai kokea syyllisyyttä, jos hyökkäys on onnistunut heidän kauttaan. Tämä voi johtaa organisaatiossa pelon kulttuuriin tai toisaalta välinpitämättömyyteen, jos aiheesta ei keskustella avoimesti. Hadlingtonin (2017) mukaan tietoturva on paitsi tekninen, myös käyttäytymistieteellinen haaste – ja tätä näkökulmaa tulisi vahvistaa pk-yritysten arviointikäytännöissä.

6.3 Kyberturvallisuus osana liiketoimintastrategiaa

Yksi tutkimuksen kriittisistä havainnoista oli, että kyberturvallisuutta ei useinkaan nähdä strategisena liiketoiminta-asiana, vaan teknisenä tai operatiivisena tukifunktiona. Tämä johtaa siihen, että turvallisuusbudjetit ovat pieniä, koulutus ad hoc -tyyppistä ja arviointi jää joko ulkoisten asiantuntijoiden tai IT-henkilöstön vastuulle. Armenia et al. (2021) ja Kapoor et al. (2022) ovat todenneet, että tämä näkemysero on yksi

suurimmista esteistä kyberturvallisuuden kehittämiselle pk-yrityksissä. Pk-yrityksissä tulisi ottaa käyttöön kyberresilienssiin perustuvia johtamismalleja, joissa turvallisuus on osa kilpailukykyä, ei sen este.

Tutkimuksessa korostui myös, että niillä yrityksillä, joilla oli aiempia kokemuksia kyberhyökkäyksistä, oli usein selkeämpi käsitys siitä, miten vaikutuksia arvioidaan. Tämä tukee ajatusta oppimisen merkityksestä: kun hyökkäys on jo tapahtunut, yritykset aktivoituvat arvioimaan ja kehittämään toimiaan. Ongelmana on kuitenkin se, että "oppiminen kantapään kautta" voi olla pienelle yritykselle kohtalokasta. Siksi ennakoiva ja simuloitu arviointi olisi tärkeää – mutta tällä hetkellä siihen ei juuri resursseja osoiteta.

6.4 Riskienhallinnan puutteet ja tarpeet

Tutkimuksessa havaittiin selkeästi, että riskienhallintaa ei useinkaan ole integroitu pk-yritysten arkeen. Useat haastateltavat kertoivat, että kyberriskit käsitellään lähinnä vakuutuksina tai virustorjuntaratkaisuina, mutta ei liiketoimintaprosesseihin upotettuina käytäntöinä. Tämä on ristiriidassa modernien riskienhallintateorioiden kanssa, joiden mukaan kyberriskien tulisi olla osa kokonaisvaltaista riskikartoitusta ja liiketoiminnan jatkuvuuden suunnittelua (Srinivas et al., 2019).

Lisäksi havaittiin, että monet pk-yritykset eivät arvioineet riittävästi toipumiskyvykkyyttään. Kun hyökkäys on ohi, alkavat käytännön ongelmat: tiedon palautus, viestintä sidosryhmille, maineen palautus ja sisäisten prosessien uudelleenjärjestely. Näihin vaiheisiin ei kuitenkaan usein ole selkeitä toimintamalleja, mikä aiheuttaa lisäriskiä hyökkäyksen jälkeisessä palautumisvaiheessa. Tämä havainto tukee esimerkiksi ENISA:n (2021) ja Cloudfaren (2014) linjauksia, joiden mukaan toipumisen suunnittelu on yhtä tärkeää kuin ennaltaehkäisy.

6.5 Tutkimuksen rajoitukset ja kehittämisideoita

Tutkimuksen rajoituksiin kuuluu aineiston rajallisuus: vaikka haastattelut olivat laadukkaita ja eri toimialoilta, ei otos edusta kaikkia suomalaisia pk-yrityksiä. Lisäksi tutkimuksen laatu oli riippuvainen haastateltavien avoimuudesta ja kokemuksista.

Tutkimus ei myöskään kattanut kaikkia mahdollisia arviointimenetelmiä, kuten kybervakuutusten roolia, mikä voisi olla kiinnostava lisä jatkotutkimukseen.

Jatkossa olisi hyödyllistä:

1. Laajentaa tutkimusta määrällisesti, jotta voidaan vertailla eri toimialojen ja kokoluokkien toimintamalleja.
2. Tutkia kvantitatiivisesti vaikutusten arvioinnin ja kyberresilienssin välistä yhteyttä.
3. Syventyä siihen, miten pk-yritykset voisivat hyödyntää tekoälyyn perustuvia ennakointijärjestelmiä uhkien arvioinnissa.
4. Tarkastella, miten sääntely, kuten NIS2-direktiivi, vaikuttaa pk-yritysten arviointikäytäntöihin ja resilienssiin.

6.6 Johtopäätökset

Tutkimus osoittaa, että kyberhyökkäysten vaikutusten arviointi pk-yrityksissä on vielä kehittymässä oleva alue. Vaikka tietoisuus uhista on lisääntynyt, puuttuu monilta yrityksiltä järjestelmällisiä työkaluja ja osaamista arvioida riskejä ennakoivasti. Tulokset osoittavat myös, että strateginen ajattelu, turvallisuuskulttuurin kehittäminen ja viitekehysten käyttö ovat keskeisiä elementtejä, joiden avulla pk-yritykset voivat parantaa valmiuksiaan kohdata ja käsitellä kyberuhkia.

Erityisesti phishingin kaltaisten hyökkäysten kohdalla yritysten tulisi panostaa enemmän koulutukseen, tietoisuuden lisäämiseen ja jatkuvaan harjoitteluun. Myös johtamisessa tulisi huomioida, että kyberriskit eivät ole pelkkä IT-ongelma, vaan koko organisaation strateginen haaste.

Jatkossa tutkimusta tulisi suunnata siihen, miten pk-yrityksiä voidaan tukea vaikuttavien arviointimenetelmien ja ennakoivien toimenpiteiden käyttöönotossa. Tässä roolissa ovat niin valtiolliset viranomaiset, teknologiatoimittajat, elinkeinoelämän järjestöt kuin akateeminen tutkimus.
Vain yhteistyön ja ymmärryksen kautta voidaan rakentaa resilientimpiä pk-yrityksiä – ja turvata niiden elinvoima digitaalisessa maailmassa.

Lähteet

A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," in IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787.

Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. Journal of Sensor and Actuator Networks, 12(4), 51. https://doi.org/10.3390/jsan12040051.

Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/CyberSA49311.2020.9139638.

Alasmary, W., Alhaidari, F., & Alhaidari, A. (2021). A survey on access control models in cloud computing. Journal of Computer Networks and Communications, 2021, Article 5595071. https://doi.org/10.1155/2021/5595071.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196. https://doi.org/10.1016/j.cose.2017.04.006.

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.

Alves, D., Apolinário, F., Pacheco, B., Escravana, N., & Grilo, A. (2023). Calculating Business Impact Assessment of Cyber-Threats. IEEE 9th World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/WF-IoT58464.2023.10539457.

Amin, Z. (2017). A practical road map for assessing cyber risk. Journal of Risk Research, 22(1), 32–43. https://doi.org/10.1080/13669877.2017.1351467.

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580. https://doi.org/10.1016/J.DSS.2021.113580.

Ayesha, A., Malik, H., Tanveer, H., & Shabir, H. (2020). ARDS—Anti-Ransomware Defense System Model—Based on the Systematic Review of Worldwide Ransomware Attacks. MDPI. https://doi.org/10.3390/su14010008.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531-540. https://doi.org/10.1016/j.bushor.2020.03.010.

Boletsis, C., Halvorsrud, R., Pickering, J., Phillips, S., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the human element into socio-technical cybersecurity risk assessment. Proceedings of the 16th International Conference on Availability, Reliability and Security. https://doi.org/10.5220/0010332902660274.

Burda, P., Altawekji, A. M., Allodi, L., & Zannone, N. (2023). The peculiar case of tailored phishing against SMEs: Detection and collective defense mechanisms at a

small IT company. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 1–12. https://doi.org/10.1109/EuroSPW59978.2023.00031.

Cabaj, K., Kotulski, Z., Księżopolski, B. et al. Cybersecurity: trends, issues, and challenges. EURASIP J. on Info. Security 2018, 10 (2018). https://doi.org/10.1186/s13635-018-0080-0.

Cao, C., Yuan, L.-P., Singhal, A., Liu, P., Sun, X., & Zhu, S. (2018). Assessing Attack Impact on Business Processes by Interconnecting Attack Graphs and Entity Dependency Graphs. https://doi.org/10.1007/978-3-319-95729-6_21.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104. https://doi.org/10.1080/10864415.2004.11044320.

Charitoudi, K., & Blyth, A. (2014). An agent-based socio-technical approach to impact assessment for cyber defense. Information Security Journal: A Global Perspective, 23(2), 125–136. https://doi.org/10.1080/19393555.2014.931492.

Chaudhary, S., Gkioulos, V., & Goodman, D. (2023). Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources. In S. Katsikas et al. (Eds.), Computer Security. ESORICS 2022 International Workshops. ESORICS 2022. Lecture Notes in Computer Science (Vol. 13785, pp. 91–104). Springer, Cham. https://doi.org/10.1007/978-3-031-25460-4_6.

Check Point Research. (2020). Ransomware Evolved: Double Extortion. CP<R>. https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/

Cimpanu, C. (2020). Cloud provider stopped ransomware attack but had to pay ransom demand anyway. ZDNet. https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/.

Cloudflare. (2014, January 13). Understanding and mitigating NTP-based DDoS attacks. Cloudflare Blog. Retrieved from https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/.

Collier, Z. A., & D'Anna, G. (2023). Cybersecurity for entrepreneurs. SAE International.

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2023). Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level. IEEE Transactions on Engineering Management, 70, 3745–3765. https://doi.org/10.1109/TEM.2021.3084687.

D'Adamo, I., González-Sánchez, R., & Medina-Salgado, M. S. (2021). Methodological perspective for assessing European consumers' awareness of cybersecurity and sustainability in e-commerce. Sustainability, 13(20), 11343. https://doi.org/10.3390/su132011343.

Daraghi, T., Dehghantanha, A., Nikkhah Bahrami, P., Conti, M., & Bianchi, G. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15(3), 277-305. https://doi.org/10.1007/s11416-019-00338-7.

Dhawan, S., Narwal, B. (2019). Unfolding the Mystery of Ransomware. In: Bhattacharyya, S., Hassanien, A., Gupta, D., Khanna, A., Pan, I. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 55. Springer, Singapore. https://doi.org/10.1007/978-981-13-2324-9_4.

Elinkeinoelämän keskusliitto (EK) & Perheyritysten liitto. (2024). PK-sektorin yrittäjät ja omistajat peräänkuuluttavat EU:lta vahvempaa kasvun selkänojaa. https://ek.fi/ajankohtaista/tiedotteet/ek-ja-perheyritysten-liitto-pk-sektorin-yrittajat-ja-omistajat-peraankuuluttavat-eulta-vahvempaa-kasvun-selkanojaa/.

Emer, A., Unterhofer, M., & Rauch, E. (2021). A cybersecurity assessment model for small and medium-sized enterprises. IEEE Engineering Management Review, 49(2), 98-109. https://doi.org/10.1109/EMR.2021.3078077.

FarahaniNia, S., Dehghan, M., Sadeghiyan, B., & Niksefat, S. (2023). Impact Assessment for Cyber Security Situation Awareness. International Journal of Information and Communication Technology Research. https://doi.org/10.61186/itrc.15.3.21.

Feigenbaum, J., Johnson, A., Syverson, P. (2007). A Model of Onion Routing with Provable Anonymity. In: Dietrich, S., Dhamija, R. (eds) Financial Cryptography and Data Security. FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77366-5_9.

Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003.

Ghazali, K., & Hassan, R. (2011). Flooding distributed denial of service attacks: A review. Journal of Computer Science, 7(8), 1218–1223. https://doi.org/10.3844/jcssp.2011.1218.1223.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for economic analysis of information security investment. Communications of the ACM, 46(12), 78-84. https://doi.org/10.1145/953460.953461.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346.

Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioural analysis on Windows platforms. Journal of Information Security and Applications, 40, 44–51. https://doi.org/10.1016/j.jisa.2018.02.008.

Haque, M. A., Shetty, S., Kamhoua, C., & Gold, K. (2020). Integrating mission-centric impact assessment to operational resiliency in cyber-physical systems. 2020 IEEE Global Communications Conference, 1–7. https://doi.org/10.1109/GLOBECOM42002.2020.9322321.

Huang, K., Zhou, C., Tian, Y. C., Yang, S., & Qin, Y. (2018). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Transactions on Industrial Electronics, 65(9), 8153–8162. https://doi.org/10.1109/TIE.2018.2798605.

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. Deviant Behavior, 37(10), 1163–1178. https://doi.org/10.1080/01639625.2016.1169829.

IBM. (2023). Cost of a Data Breach Report. Saatavilla osoitteessa: https://www.ibm.com/security/data-breach.

ISO/IEC. (2013). ISO/IEC 27001:2013 Information security management systems — Requirements. International Organization for Standardization.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650.

Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2007). Detecting DNS amplification attacks. In Critical Information Infrastructures Security, Second International Workshop. https://doi.org/10.1007/978-3-540-77366-5.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2019). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics. http://dx.doi.org/10.2139/ssrn.313551.

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. Sustainability, 14(8). https://doi.org/10.3390/su14010008.

Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23 (pp. 369-384). Springer International Publishing.

Kumar, R., & Shukla, A. (2023). Deception in double extortion ransomware attacks: An analysis of criminal strategies and victim responses. Computers & Security, 126, 103670. https://doi.org/10.1016/j.cose.2023.103670.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework.

Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. Online Journal of Applied Knowledge Management. https://doi.org/10.36965/ojakm.2022.10(2)1-22.

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. *ICISSP*, 558-563.

Puusa, A., & Juuti, P. (2020). Laadullisen tutkimuksen näkökulmat ja menetelmät (3. painos). Gaudeamus.

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. Information Systems Research, 20(1), 121–139. https://doi.org/10.1287/isre.1080.0174.

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. M., & Assi, C. (2023). The age of ransomware: A survey on the evolution, taxonomy, and research directions. IEEE Access, 11, 40698-40714. https://doi.org/10.1109/ACCESS.2023.3268535.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001.

Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined cyber–physical system against DDoS and IoT-DDoS attacks. Computer Science Review, 40, 100371. https://doi.org/10.1016/j.cosrev.2021.100371.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cybersecurity: Framework, standards, and recommendations. Future Generation Computer Systems, 92, 178-188. https://doi.org/10.1016/j.future.2018.09.063.

Ståhlberg, M. (2007, September). The trojan money spinner. In Virus bulletin conference (Vol. 4).

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. IEEE Access, 11, 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670.

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. Int. J. Netw. Secur., 15(5), 390-396.

van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M. J. S., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. Applied Sciences. https://doi.org/10.3390/app11156909.

Wang, Z., Liu, C., Qiu, J., Tian, Z., Cui, X., & Shen, S. (2018). Automatically Trace-back RDP-Based Targeted Ransomware Attacks. Wireless Communications & Mobile Computing (Online), 2018, 13. https://doi.org/10.1155/2018/7943586.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. Journal of Computer Information Systems, 63(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791.

Y. -F. Liu, L. -W. Zhang, J. Liang, S. Qu and Z. -Q. Ni, "Detecting Trojan horses based on system behavior using machine learning method," 2010 International Conference on Machine Learning and Cybernetics, Qingdao, China, 2010, pp. 855-860, doi: 10.1109/ICMLC.2010.5580591.

Yigit Ozkan, B., & Spruit, M. (2022). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. Journal of Computer Information Systems, 63(4), 965–987. https://doi.org/10.1080/08874417.2022.2119442.

Zhu, Q., Qin, Y., Zhou, C., & Fei, L. (2019). Hierarchical Flow Model-Based Impact Assessment of Cyberattacks for Critical Infrastructures. IEEE Systems Journal, 13, 3944-3955. https://doi.org/10.1109/JSYST.2019.2912626.

Liitteet

Liite 1. Haastattelurunko

Haastattelurunko

Tutkimusaihe: Kyberhyökkäysten vaikutusten arviointi pk-yrityksissä

Haastattelun tyyppi: Puolistrukturoitu

Kohderyhmä: Pk-yritysten työntekijät/asiantuntijat

1. Taustatiedot

Voitko kertoa lyhyesti työtehtävistäsi ja roolistasi yrityksessä?

Kuinka pitkään olet työskennellyt tässä yrityksessä?

Oletko saanut koulutusta kyberturvallisuuteen liittyen työssäsi?

2. Kyberuhkien ymmärrys ja kokemukset

Mitä kyberuhkia pidät merkittävimpinä työtehtäviesi näkökulmasta?

Oletko itse kohdannut tai havainnut työpaikallasi kyberuhkiin liittyviä tilanteita?

Jos kyllä niin missä muodossa hyökkäys on tapahtunut?

Jos olet, niin miten tilanne havaittiin ja miten siihen reagoitiin?

Onko pandemian jälkeisessä yleistyneessä etätyöskentelyssä ollut riskejä kyberturvallisuuden kanssa?

3. Kyberhyökkäysten vaikutusten arviointi

Miten yrityksessäsi arvioidaan kyberhyökkäysten vaikutuksia liiketoimintaan?

Onko yrityksessä käytössä jotakin tapoja tai järjestelmiä, joilla seurataan kyberhyökkäysten vaikutuksia?

Miten kyberhyökkäysten mahdollisia vaikutuksia on käsitelty organisaation sisällä? (Esim. keskustelut, koulutukset, raportit)

Koetko, että kyberhyökkäykset vaikuttaisivat merkittävästi yrityksen päivittäiseen toimintaan, jos sellainen tapahtuisi? Miksi/miksi ei?

4. Yrityksen valmiudet ja toimenpiteet

Miten yrityksessäsi varaudutaan mahdollisiin kyberhyökkäyksiin?

Oletko saanut ohjeistusta siitä, miten toimia kyberhyökkäyksen tai epäilyttävän tapahtuman yhteydessä?

Miten koet yrityksesi valmiuden käsitellä kyberuhkia työntekijän näkökulmasta?

Miten yrityksessäsi suhtaudutaan kyberturvallisuuden parantamiseen? (Esim. onko tehty konkreettisia muutoksia tai investointeja viime aikoina?)

5. Parannusehdotukset ja työntekijöiden näkemykset

Mitä keinoja ehdottaisit yrityksellesi kyberturvallisuuden parantamiseksi?

Miten mielestäsi työntekijöitä voisi paremmin valmistaa mahdollisiin kyberuhkiin?

Onko sinulla muuta lisättävää tai huomioitavaa kyberuhkiin ja niiden vaikutusten arviointiin

Liite 2. Opiskelijan aineistonhallintasuunnitelma

1. Tutkimusaineisto

Aineistotyyppi	Sisältää henkilötietoja*	Tuotan aineiston itse	Joku muu on tuottanut aineiston	Muuta huomioitavaa
Aineistotyyppi 1: *Haastattelut*	x	x	x	

* Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Esimerkkejä henkilötiedoksi katsotuista tiedoista löydät Tietosuojavaltuutetun toimiston sivuilta

2. Henkilötietojen käsittely tutkimuksessa

Laadin tutkittavilleni tietosuojailmoituksen** ja toimitan sen heille ennen aineiston keruuta ☒

Henkilötietojen osalta rekisterinpitäjänä** toimii opiskelija ☒ yliopisto ☐

Aineistoni ei sisällä henkilötietoja ☐

3. Aineiston käyttöön liittyvät luvat ja oikeudet

Selvitä mitä lupia ja oikeuksia aineistojen käyttöön liittyy. Ole tarvittaessa yhteydessä opinnäytteesi ohjaajaan. Kuvaile jokaisen aineistotyypin osalta niiden käyttöön liittyvät luvat ja oikeudet, voit tarvittaessa lisätä aineistotyyppejä listaukseen.

3.2 Jonkun muun tuottama aineisto

Aineistoon liittyvät oikeudet ja lisenssit

Aineistotyyppi 1: Kuva 1, NIST viitekehys

4. Aineiston säilyttäminen tutkimuksen aikana

Yliopiston verkkokansiossa ☒
Yliopiston tarjoamassa Seafile-pilvipalvelussa ☐
Jossakin muualla, missä? ☒

Olen pitänyt huolta, että minulla löytyy aina varmuuskopio niin olen tallentanut yliopiston onedriveen sekä omalle koneelle niin ei käyt vahingossakaan tiedoston korruptuneisuutta tmv.

5. Aineiston dokumentointi ja metadata

5.1 Aineiston dokumentointi

Käytän aineiston dokumentointiin omaa kansiota tietokoneella. Täällä olen säilyttänyt kaikki mahdolliset eri versiot tutkielmasta ml. tutkimussuunnitelma mikä esitin MENY2-kurssilla.

tutkimuspäiväkirjaa ☐
erillistä dokumenttia, johon kirjaan aineiston pääasiat, kuten tehdyt muutokset, analyysin vaiheet sekä esim. muuttujien merkitykset ☒
aineiston mukana kulkevaa readme-tiedostoa, jossa kuvataan aineiston pääasiat ☒
jotain muuta, mitä? ☐

5.2 Aineiston järjestys ja eheys

Säilytän alkuperäisen aineiston erillään tutkimuksenteon aikana käyttämästäni aineistosta, jotta voin palata alkuperäiseen, jos tarvetta ilmenee. ☒

Versionhallinta: mietin jo ennen tutkimuksenteon alkua, miten tulen nimeämään eri aineistoversiot ja noudan sitä systemaattisesti ☒

Tiedostan jo tutkimuksen alussa aineistoni elinkaaren, ja varaudun tilanteisiin, joissa data saattaa huomaamatta muuttua, kuten esim. nauhoitus, litterointi, konversio toiseen tiedostomuotoon, tallentaminen jne. ☒

5.3 Metadata

En tallenna aineistoani julkiseen arkistoon, enkä tarvitse metadataa. ☒

6. Aineisto tutkimuksen valmistuttua

Tuhoan koko datan heti tutkielman valmistuttua, koska sitä ei tarvita tutkielmassa olevan analyysin jälkeen ja näin olen myös viestinyt asiat haastateltavilta.