Lunnashaittaohjelmien torjunta pk-yrityksissä: parhaat käytännöt ja haasteet

Juho Tuovinen

Haaga-Helia ammattikorkeakoulu
Tradenomi, tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
2025

Tiivistelmä

Tekijä(t)
Juho Tuovinen

Tutkinto
Tietojenkäsittelyn tradenomi

Raportin/Opinnäytetyön nimi
Lunnashaittaohjelmien torjunta pk-yrityksissä: Parhaat käytännöt ja haasteet

Sivu- ja liitesivumäärä
37 + 11

Tämän opinnäytetyön tarkoituksena oli selvittää pk-yritysten parhaita käytäntöjä lunnashaittaohjelmien torjunnassa sekä tunnistaa tähän liittyviä keskeisiä haasteita. Aihe on tärkeä ja ajankohtainen, sillä pk-yrityksillä on usein rajalliset resurssit ja tietoturvaosaaminen, mikä tekee niistä alttiita kyberhyökkäyksille ja erityisesti lunnashaittaohjelmille. Tutkimuksen tavoitteena oli tuottaa konkreettisia suosituksia pk-yrityksille tietoturvan parantamiseksi sekä lunnashaittaohjelmahyökkäyksien ennaltaehkäisemiseksi.

Tutkimuksessa käytettiin kvalitatiivista tutkimusmenetelmää, johon kuului kirjallisuuskatsaus sekä pk-yritysten edustajien haastattelut sekä kyselyt. Kirjallisuuskatsauksessa tarkasteltiin lunnashaittaohjelmien toimintaperiaatteita, niiden vaikutuksia pk-yrityksiin, torjuntastrategioita sekä minkälaisia haasteita ja parhaita käytäntöjä on aikaisempien tutkimuksien mukaan ollut. Haastattelujen ja kyselyiden avulla kerättiin käytännön kokemuksia ja näkemyksiä lunnashaittaohjelmien torjunnasta. Tarkoituksena oli vertailla pk-yritysten kokemuksia aikaisempiin tutkimuksiin ja teoriaan.

Tuloksista ilmeni, että pk-yritysten keskeisimpiä haasteita olivat resurssien niukkuus, tietämättömyys kyberuhista, riksien aliarviointi sekä jatkuvasti kehittyvät uhat. Parhaiksi käytännöiksi osoittautui säännöllinen tietojen varmuuskopiointi, henkilöstön kouluttaminen sekä järjestelmien aktiivinen päivittäminen. Työn tuloksien ja aikaisempien tutkimusten pohjalta laadittiin konkreettisia suosituksia pk-yritysten tietoturvan kehittämiseksi ja lunnashaittaohjelmilta suojautumiseksi.

Asiasanat
Lunnashaittaohjelmat, pk-yritykset, kyberturvallisuus, kyberresilienssi, tietoturva, tietoturvakäytännöt

Sisällys

1 Johdanto

Maailma digitalisoituu yhä nopeammin ja niin myös kyberhyökkäysten määrä kasvaa vuosi vuodelta. Suureksi kyberuhaksi yrityksille on koitunut lunnashaittaohjelmat. Thales Groupin mukaan lunnashaittaohjelmahyökkäysten määrä kasvoi vuonna 2024 merkittävästi, peräti 27 prosenttia edellisvuoteen 2023 verrattuna. (Thales Group 2024) Lisäksi lunnaiden suuruus on kasvanut huomattavasti viime vuosina: vuonna 2019 suurin yksittäinen lunnasvaatimus oli 13 miljoonaa euroa, kun taas vuonna 2021 se oli noussut 62 miljoonaan euroon. (Euroopan parlamentti 2022, 2)

Pk-yritykset ovat keskeisessä asemassa etenkin Suomen talouden kannalta, sillä ne tuovat merkittäviä verotuloja Suomelle ja työllistävät 1,45 miljoonaa ihmistä eli yli neljäsosan suomalaisista. (Yrittäjät s.a.) Pienemmillä pk-yrityksillä usein kuitenkin on rajalliset resurssit ja heikompi tietoturvaosaaminen, verrattuna suurempiin kansainvälisiin yrityksiin. Tämä tekee niistä erityisen haavoittuvaisia kyberhyökkäyksille, sillä usein rikollisten kohteiksi valikoituu yritykset, joilla on heikompi tietoturvataso. Rikollisten näkökulmasta pk-yritykset ovat houkuttelevia kohteita, koska niillä voi silti olla hallussaan yrityssalaisuuksia tai asiakasrekistereitä. Näitä tietoja vastaan yritys voi olla valmis maksamaan lunnaat, tai vaihtoehtoisesti tiedot voidaan myydä esimerkiksi rikollisille markkinoille. Tästä syystä opinnäytetyössäni keskitytään tutkimaan mitkä ovat pk-yritysten parhaat käytännöt lunnashaittaohjelmien torjuntaan sekä lunnashaittaohjelmien torjuntaan liittyvät haaste.

Onnistuneiden lunnashaittaohjelmahyökkäysten vaikutukset voivat olla pk-yritykselle todella haitallisia, ellei kohtalokkaita. Siitä voi seurata yritykselle taloudellisia tappioita, maineen ja asiakkaiden menetystä tai pahimmassa tapauksessa liiketoiminta joudutaan kokonaan lopettamaan. Tämän vuoksi aihetta on tärkeää tutkia ja tuottaa pk-yrityksille konkreettisia suosituksia lunnashaittaohjelman torjuntaan.

Opinnäytetyön tutkimus perustuu kirjallisuuskatsaukseen ja pk-yritysten edustajien haastatteluun. Kirjallisuuskatsauksen avulla pyritään kartoittamaan lunnashaittaohjelmien torjuntakeinoja sekä niihin liittyviä haasteita pk-yritysten näkökulmasta. Haastatteluiden ja kyselyiden avulla pyritään saamaan käytännönläheisiä kokemuksia ja näkemyksiä aiheesta.

Työssäni ensiksi tarkastellaan pk-yritysten tietoturvan taustatekijöitä ja lunnashaittaohjelmien toimintaperiaatteita. Kirjallisuuskatsauksessa käsitellään, kuinka lunnashaittaohjelmilta voidaan suojautua ja mitä haasteita pk-yritys voi kohdata tehokkaaseen torjuntaan liittyen. Haastattelussa ja kyselyssä saatuja vastauksia verrataan kirjallisuuskatsauksessa kerättyihin tietoihin, mikä mahdollistaa teorian ja käytännön välisen vertailun.

Lopuksi työssäni analysoidaan tulokset ja esitetään johtopäätökset sekä konkreettiset suositukset pk-yrityksille lunnashaittaohjelmien torjuntaan ja tietoturvan kehittämiseen yrityksessä. Yhdistelmä tietoa kirjallisuudesta ja haastatteluista sekä kyselyistä tarjoaa monipuolisen näkökulman tutkimusaiheeseen.

Tämän opinnäytetyön tavoitteena on ymmärtää lunnashaittaohjelmien riskit pk-yrityksille sekä ymmärtää tehokkaimmat toimintatavat lunnashaittaohjelmahyökkäysten torjumiseksi ja ennaltaehkäisemiseksi. Työn tavoitteena on tarjota pk-yrityksille konkreettisia vaihtoehtoja arkaluonteisten tietojen suojaamiseksi ja liiketoiminnan suojaamiseksi lunnashaittaohjelmilta.

Työssä keskitytään selvittämään, kuinka suomalaiset pk-yritykset voivat tehokkaimmin torjua lunnashaittaohjelmia sekä millaisia haasteita niiden torjuntaan liittyy. Työssä tarkastellaan lunnashaittaohjelmien vaikutusta pk-yritysten toimintaan, parhaita käytäntöjä ja torjuntakeinoja lunnashaittaohjelmien torjuntaan sekä pk-yritysten resurssien ja tietoturvataitojen rajallisuutta. Työssä ei käsitellä suuryrityksiä tai muita kyberuhkia.

Tutkimus perustuu pääasiassa kirjallisuuskatsaukseen sekä haastatteluihin tai kyselyihin, joissa selvitetään millaisia kokemuksia tai haasteita pk-yritykset voivat kohdata lunnashaittaohjelmien torjuntaan liittyen.

2 Pk-yritysten tietoturva

Tässä osiossa käsitellään opinnäytetyön keskeisiä teemoja ja käsitteitä, jotka liittyvät lunnashaittaohjelmien torjuntaan pk-yrityksissä. Tietoperustan avulla luodaan teoreettinen viitekehys, jonka avulla voidaan ymmärtää ja analysoida opinnäytetyön tutkimuksen tuloksia sekä lunnashaittaohjelmien torjuntaan liittyviä haasteita ja parhaita käytäntöjä pk-yrityksissä.

Euroopan komission määritelmän mukaan pk-yrityksiin lasketaan mikroyritykset sekä pienet ja keskisuuret yritykset, joissa työskentelee enintään 250 työntekijää ja vuoden liikevaihto on enintään 50 miljoonaa euroa, tai taseen loppusumma on enintään 43 miljoonaa euroa. (Euroopan komissio s.a. a, 3)

2.1 Tietoturva

Tietoturvalla tarkoitetaan arkaluonteisten tietojen saatavuuden, eheyden ja luottamuksellisuuden turvaamista, kuten esimerkiksi yksityishenkilön etninen alkuperä, terveystiedot tai biometriset tiedot, joita käytetään mm. tunnistautumisessa. (Euroopan komissio s.a. b) Yrityksen arkaluonteisia tietoja ovat esimerkiksi taloudelliset raportit, liiketoimintasuunnitelmat tai henkilöstön, asiakkaiden tai potilaiden henkilötiedot. (Stena Confidential 2024) Turvattava tieto voi olla joko fyysinen asiakirja tai digitaalinen tallenne. (Jyväskylän yliopisto s.a.)

Tiedon luottamuksellisuudella tarkoitetaan pyrkimystä pitää arka tieto salassa ja yksityisenä. Tätä varten tietojen saatavuutta on valvottava, jotta estetään tietojen luvaton jakaminen tahoille, joille se ei kuulu. Vastaavasti tehokas järjestelmä myös varmistaa sen, että niillä, joilla on oikeus tietoihin, on tarvittavat oikeudet. Esimerkiksi organisaation työntekijät voivat päästä käsiksi tiettyihin organisaation tietoihin, mutta muilta kuin työntekijöiltä pääsy on kielletty. (Fortinet s.a.)

Eheydellä tarkoitetaan, että tiedot ovat luotettavia ja täydellisiä, eikä luvaton käyttäjä ole muokannut tai muuttanut tietoja. Tietojen eheys voi vaarantua tahattomasti järjestelmän toimintahäiriön, tietojen syöttövirheen tai varmuuskopion unohtamisen vuoksi. Tietojen eheyden voivat vaarantaa myös uhkatoimijat, jotka yrittävät peukaloida tietoja. Esimerkiksi kalasteluyritys, jossa tarkoituksena on muuttaa pankkitilin reititysnumeroita palkkajärjestelmässämme, on uhka instituutionaalisten tietojemme eheydelle. (Washington University in St. Louis 2024) Tietoihin voi liittyä tarkistussummia tai jopa kryptografisia tarkistussummia eheyden varmistamiseksi. Lisäksi digitaalisia allekirjoituksia voidaan käyttää tehokkaisiin kiistämättömyystoimenpiteisiin, mikä tarkoittaa, että kirjautumista, lähetettyjä viestejä sekä sähköisten asiakirjojen katselua ja lähettämistä ei voida kiistää. (Chai, W. & Hashemi-Pour, C. 2023)

Vaikka tietojen luottamuksellisuus ja eheys säilyisi, ne ovat hyödyttömiä, elleivät ne ole organisaation tai henkilöiden saatavilla, kun niitä tarvitaan. Tämä tarkoittaa, että verkkojen, järjestelmien ja sovellusten on toimittava asianmukaisesti silloin kun niiden pitäisi. Henkilöiden, joilla on pääsy tietoihin, on myös voitava käyttää niitä tarvittaessa, eikä tietojen saaminen saisi viedä kohtuuttomasti aikaa. Tietojen saatavuus voi vaarantua, jos hyökkääjä tahallisesti aiheuttaa esimerkiksi organisaatioon kohdistuneen palvelunestohyökkäyksen (DoS) tai lunnashaittaohjelmahyökkäyksen vuoksi. (Fortinet s.a.)

Kyberresiliensillä tarkoitetaan kykyä suojata sähköisiä tietoja ja järjestelmiä kyberhyökkäyksiltä sekä kykyä palautua onnistuneista hyökkäyksistä. (Euroopan keskuspankki 2024) Kyberresilienssin rakentamiseen kuuluu riskipainotteisen turvallisuussuunnitelman laatiminen, jossa oletetaan, että yritys jossain vaiheessa tulee tietoturvaloukkauksen tai -hyökkäyksen kohteeksi. Yrityksen on siis tärkeä arvioida riskejä ja luoda prosesseja hyökkäysten varalle. Yrityksen on tärkeä palautua entiselleen mahdollisimman nopeasti, jotta vahinkoa syntyisi mahdollisimman vähän ja liiketoimintaa pystyttäisiin jatkamaan mahdollisimman nopeasti. (Cisco 2024)

2.2 Lunnashaittaohjelmat

Lunnashaittaohjelmat (ransomware) ovat digitaalisia haittaohjelmia, jotka estävät pääsyn tietokoneen tiedostoihin, järjestelmiin tai verkkoon ja vaativat lunnaiden maksamista niiden palauttamiseksi. Lunnashaittaohjelmahyökkäykset voivat aiheuttaa kalliita toimintahäiriöitä ja kriittisten tietojen ja datan menetyksen. (FBI s.a.)

Lunnashaittaohjelman voi tietämättään ladata tietokoneelle avaamalla sähköpostin liitetiedoston, painamalla mainosta avaamalla linkin tai vierailemalla verkkosivustolla, johon on upotettu haittaohjelma. Useimmiten tartunnan huomaa vasta kun haittaohjelma lukitsee tiedostot ja tietokoneen ruudulle ilmestyy viesti, jossa ilmoitetaan, että tiedostot on salattu ja salaus puretaan vasta kun lunnaat on maksettu. (FBI s.a.) Verkkorikolliset suosivat kryptovaluuttaa, kuten Bitcoinia, lunnaiden maksuun, sillä se tarjoaa rikollisille anonymiteetin ja vaikeasti jäljitettävän maksutavan. (FinCEN 2020, 5)

Kryptovaluutta on digitaalinen tai virtuaalinen valuutta, joka käyttää kryptografiaa turvaamaan transaktiot, eikä kryptovaluutta ole riippuvainen pankeista liiketoimien varmentamisessa. Kryptovaluutta talletetaan digitaaliselle lompakolle, ja valuutta perustuu hajautettuun lohkoketjuteknologiaan (blockchain), joka tallentaa kaikki tapahtumat julkiseen kirjanpitoon. Lohkoketju on rekisteri kaikista transaktioista. Tunnettuja kryptovaluuttoja ovat esimerkiksi Bitcoin, Ethereum, Cardano ja Monero. Ensimmäinen ja edelleen tunnetuin kryptovaluutta on Bitcoin, joka

perustettiin vuonna 2009. Bitcoinin on luonut nimimerkki ”Satoshi Nakamoto”, jonka henkilöllisyyttä ei tiedetä. (Kaspersky s.a. c) Kuitenkin nykyään verkkorikollisten suosikkina on kryptovaluutta Monero. Koska Bitcoin jättää jäljen transaktioista lohkoketjuun, on Monero saanut suosiota rikollismaailmassa. Monero on taas suunniteltu niin, että valuutan lähettäjä ja vastaanottaja sekä vaihdettu summa eivät paljastu. Tämän takia valuutta on suosittu juuri lunnashaittaohjelmajengeille. (Financial Times 2021)

3 Lunnashaittaohjelmien uhka pk-yrityksille ja suojautumiskeinot

Tässä luvussa käsitellään lunnashaittaohjelmien muodostamaa uhkaa erityisesti pk-yritysten näkökulmasta. Aluksi perehdytään siihen, miten lunnashaittaohjelmat ovat kehittyneet ajan mittaan sekä millaisia toimintaperiaatteita ja eri tyyppejä niihin liittyy. Tämän jälkeen tarkastellaan, millaisia vaikutuksia lunnashaittaohjelmahyökkäyksellä voi olla pk-yrityksille, kuten taloudellisia tappioita tai liiketoiminnan keskeytymisiä. Lisäksi luvussa esitellään tehokkaimpia torjuntastrategioita ja konkreettisia keinoja, joilla yritykset voivat suojautua yleisimmiltä hyökkäystavoilta. Koska täydellistä suojausta ei ole olemassa, luvussa käsitellään myös toimintamalleja siihen, kuinka pk-yrityksen tulisi toimia, jos lunnashaittaohjelmahyökkäys kuitenkin tapahtuu. Lopuksi luvussa nostetaan esille keskeiset haasteet, joita pk-yritykset kohtaavat torjuessaan lunnashaittaohjelmia ja parhaat käytännöt, joilla yritykset voivat tehokkaasti ennaltaehkäistä ja vähentää riskejä hyökkäykselle.

3.1 Lunnashaittaohjelmien kehitys

Vaikka lunnashaittaohjelmien esiintyvyys ja näkyvyys mediassa on kasvanut viime vuosina merkittävästi, eivät ne ole uusi ilmiö tietotekniikan maailmassa. Ensimmäiset lunnashaittaohjelmat, jotka salakirjoittivat uhrin tiedostot ja vaativat niiden avaamisesta lunnaita, on nähty jo 1980-luvun lopulla. (Baker, K. 2022) Digitaalisuuden kasvu sekä yritysten riippuvuus internetistä ja tietojärjestelmistä ovat tehneet niistä houkuttelevia kohteita verkkorikollisille. Nykyisin lunnashaittaohjelmat ovat monimutkaisempia, ja rikolliset käyttävät kryptovaluuttoja maksutapana jäljitettävyyden vaike.

AIDS-troijalainen (PC Cyborg) on ensimmäinen dokumentoitu lunnashaittaohjelma, jonka biologian tohtori Joseph Popp loi joulukuussa vuonna 1989. Popp lähetti yli 20 000 saastunutta levykettä postissa Maailman terveysjärjestö WHO:n AIDS-konferenssin osallistujille. Levyke sisälsi varoituksia ohjelmiston mahdollisista haitoista. Kun käyttäjä oli käynnistänyt tietokoneensa 90 kertaa, ohjelma laski käynnistykset ja sen jälkeen piilotti hakemistot ja salasi tiedostot. Käyttäjän oli maksettava 189 dollaria vuotuisesta lisenssistä tai 378 dollaria elinikäisestä lisenssistä tietojen palauttamiseksi. Rahat tuli lähettää PC Cyborg Corporationille Panamaan osoitettuun postilaatikkoon. (KnowBe4 s.a. b)

AIDS-troijalaisen jälkeen seurasi viidentoista vuoden hiljaisuus, kunnes, 2000-luvun alussa internetin ja sähköpostin yleistyessä lunnashaittaohjelmat alkoivat nostaa päätään. Yksi merkittävistä varhaisista lunnashaittaohjelmista oli vuonna 2004 ilmestynyt GPCode. Haittaohjelma levisi Windows-tietokoneille haitallisten verkkosivulinkkien ja kalastelusähköpostien kautta. PGCoden oli tarkoitus levitä mahdollisimman monelle käyttäjälle, ja siksi lunnaiden määrä oli vain

noin 20 dollaria. (Shea, S. 2025). Kuitenkaan haittaohjelman tiedostojen salaaminen ei ollut kovinkaan edistynyttä, joten tiedostot olivat helposti palautettavissa ja myöhemmät haittaohjelman variantit käyttivät symmetristä salausta, mikä teki avaimen palautuksesta helppoa. (KnowBe4 s.a. a)

Vuonna 2006 Archiveus Troijan oli ensimmäinen lunnashaittaohjelma, joka käytti kehittyneempää 1024-bittistä RSA-salausta. Tämä salaus oli vaikea purkaa, koska se edellytti alfanumeraalisen merkkijonon syöttämistä tiedostojen avaamiseksi. Poiketen tavallisimmista lunnashaittaohjelmista, Archiveus ei kuitenkaan vaatinut lunnaaksi rahaa, vaan pakotti uhrit ostamaan lääkkeitä venäläiseltä verkkosivustolta, jossa lääkkeet maksoivat vähintään 74 dollaria pullolta. Epäillään, että lunnashaittaohjelman kehittäjä on lääkkeitä myyvän verkkosivuston yhteistyökumppani, ja sai jokaisesta myydystä pullosta osuutensa. (Stewart, J. 2006)

Vuonna 2012 ilmestynyttä Revetonia pidetään yhtenä ensimmäisistä RaaS-operaationa. RaaS-malli mahdollistaa kokemattomienkin verkkorikollisten käynnistää tehokkaita haittaohjelmakampanjoita. Revetonilla oli omat kehittyneet jakelumenetelmät ja se julkaisi säännöllisesti uusia ominaisuuksia ja räätälöityjä versioita lunnasviesteistä. Se tarjosi haittaohjelmapakettejaan kolmansille osapuolille palveluna. Haittaohjelma oli myös yksi ensimmäisistä, joka vaati lunnaiden maksun Bitcoineina. (Reed, J. 2022) Vuonna 2015 ilmestynyttä Toxia pidetään ensimmäisenä RaaS-alustana, jonka käyttäjät pystyivät luomaan omia lunnashaittaohjelmavariaatioitaan ilman ohjelmointitaustaa. Tämä teki lunnashaittaohjelmien käytöstä entistä helpompaa, mikä lisäsi niiden käyttöä entisestään. (Holdsworth, J. & Kosinski, M. 2024)

CryptoLocker nousi esiin haittaohjelmakampanjan myötä vuonna 2013. CryptoLocker oli uusi haittaohjelmavariantti, joka rajoitti pääsyä saastuneelle tietokoneelle ja vaati maksua Bitcoineina tiedostojen purkamiseksi ja palauttamiseksi. Haittaohjelma levisi kalastelusähköpostien sekä väärennettyjen FedEx ja UPS-seurantailmoitusten kautta. Joissakin tapauksissa salauksen purkuavainta ei ole saatu, vaikka lunnaat olisikin maksettu. (CISA 2016)

Vuonna 2017 tunnetusta WannaCry- haittaohjelmahyökkäyksestä tuli maailmanlaajuinen epidemia. WannaCry-haittaohjelma on esimerkki tiedostot salaavasta crypto ransomwaresta, jota yleensä kyberrikolliset käyttävät rahan kiristämiseen verkossa. WannaCry salaa tiedostot Microsoft Windows-käyttöjärjestelmää käyttävät laitteet ja väittää poistavansa salauksen, kun lunnaat ovat maksettu Bitcoin-kryptovaluuttana. (Kaspersky s.a. b) WannaCry hyödynsi Windows-käyttöjärjestelmässä piilevää ”Eternal Blue”-haavoittuvuutta. Tämä haavoittuvuuden oli kehittänyt Yhdysvaltain kansallinen turvallisuusvirasto (NSA) omaan käyttöönsä, mutta Shadow Brokers-niminen hacktivistiryhmä sai sen varastettua, vuodettua julkisuuteen ja näin rikolliset pystyivät

hyödyntämään haavoittuvuutta haittaohjelmassa. WannaCry levisi nopeasti verkon kautta madon tavoin laitteesta toiselle, mutta leviäminen saatiin nopeasti pysäytettyä, kun englantilainen tietoturvatutkija Marcus Hutchins keksi lähdekoodia tutkiessaan tavan pysäyttää leviämisen. WannaCry oli merkittävä tapaus, sillä sen vaikutukset ulottuivat noin 150 maahan, lamautti noin 230 000 tietokonetta ja aiheutti arviolta noin 4 miljardin dollarin kustannukset maailmanlaajuisesti. Yhdysvallat ja Yhdistynyt kuningaskunta väittävät WannaCryn takana olevan Pohjois-Korean hallitus. (Cloudflare s.a. b)

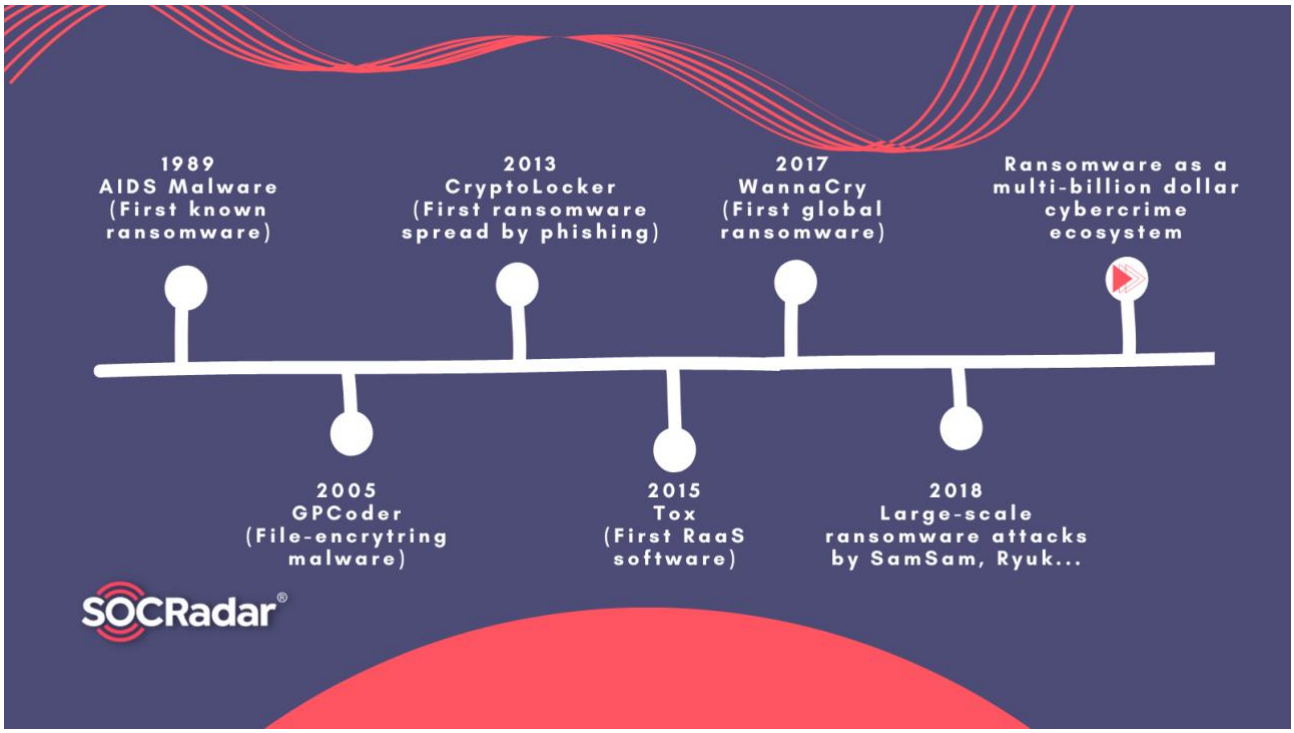
Samana vuonna myöhemmin kesäkuussa 2017 levisi myös toinen tuhoisa haittaohjelma NotPetya. Se oli muunnelma Petya-haittaohjelmasta, mutta paljon tuhoisampi. NotPetya-haittaohjelman päätoiminen tavoite ei ollut lunnaiden kerääminen, vaan aiheuttaa mahdollisimman paljon tuhoa salaamalla tietokoneiden Master Boot Record-tiedostot (MBR), jolloin tiedostoihin ei voinut enää päästä käsiksi (Cloudflare s.a. c). Haittaohjelma antoi mahdollisuuden maksaa 300 dollarin suuruiset lunnaat Bitcoineina, mutta vaikka maksu suoritettiin, ei avainta haittaohjelman purkamiseen luovutettu. (HYPR s.a.) Alun perin NotPetya-hyökkäys oli tarkoitus olla osittain poliittinen hyökkäys Ukrainaa vastaan kyberhyökkäyksessä. Ukraina kärsi suuria vahinkoja, ja haittaohjelma pääsi leviämään Ukrainasta maailmanlaajuisesti. Haittaohjelma käytti WannaCry:n hyödyntämää Eternal Blue-haavoittuvuutta sekä Windows-käyttöjärjestelmän Mimikatz-haavoittuvuutta levitäkseen tehokkaasti. (Greenberg, A. 2018) Hyökkäyksen takana eivät olleet tavalliset kyberrikolliset, vaan se nähtiin Venäjän hallituksen laajana kyberhyökkäyksenä Ukrainaa vastaan. NotPetya oli osa laajempaa kyberhyökkäysoperaatiota, jossa pyrittiin aiheuttamaan taloudellista ja infrastruktuurista häiriötä Ukrainassa. (HYPR s.a.)

Kohdennetut hyökkäykset alkoivat yleistyä vuonna 2018 Ryuk-lunnashaittaohjelman ilmestyttyä. Tätä erittäin tuottoisaa haittaohjelmaa käytetään yksittäisten kuluttajien sijaan erityisesti organisaatiota vastaan, jotka todennäköisesti maksavat korkeita lunnaita. Uhreilta on vaadittu huomattavasti suurempia summia kuin aikaisemmin lunnashaittaohjelmien historiassa. Keskimäärin lunnaat ovat olleet 15–50 bitcoinia, joka on vastannut noin 100 000–500 000 Yhdysvaltain dollaria. Salausta ei ole voinut purkaa ilman lunnaiden maksamista ja useissa tapauksissa purkutyökalu ei ole edes toiminut oikein. Haittaohjelma on liitetty venäjänkielisiin kyberrikollisryhmiin ja on vastuussa yli 61 miljoonan dollarin lunnaista. (Constantin, L. 2021; Brewster, T. 2019)

REvil (tiedetään myös nimellä Sodinokibi) on yksi tunnetummista lunnashaittaohjelmaryhmistä, joka operoi Ransomware-as-a-Service -mallia. Ryhmä on toiminut aktiivisena noin vuodesta 2019 vuoteen 2021 saakka ja on tunnettu hyökkäyksistään suuryrityksiin. McAfeen artikkelin mukaan REvilin taustalla on ryhmä huippuosaajia, joiden toiminta muistuttaa myyntitiimiä, jossa parhaat

tuottavat suurimman osan rikollisen verkoston tuloista. (Fokker, J. 2019) Ryhmä on yksi lunnashaittaohjelmaryhmistä, jotka käyttivät nykyaikaisempaa kaksinkertaista kiristystaktiikkaa, jossa kohteen tiedostot salataan sekä varastetaan ja uhataan julkaista yrityksen arkaluonteiset tiedot verkossa. Aktiivisista lunnashaittaohjelmaryhmistä, jotka käyttävät kaksinkertaista kiristystaktiikkaa on esimerkiksi Clop. (Trend Micro 2021)

Initial Access Brokers (IAB) ovat 2021 vuodesta lähtien nousseet merkittäväksi tekijäksi lunnashaittaohjelmien levittämisessä viime vuosina. IAB:t toimivat verkkorikollisuuden markkinoilla hankkimalla pääsyn haavoittuvien organisoiden verkkoihin ja myymällä tämän haavoittuvuuden hyväksikäytön muille toimijoille ja erityisesti lunnashaittaohjelmaryhmille. Tämä malli mahdollistaa lunnashaittaohjelmahyökkäysten nopeutumisen ja parantaa tehokkuutta, koska kohde ja heikkous on jo valmiiksi löydetty hyödynnettäväksi ja lunnashaittaohjelmaryhmät voivat keskittyä pelkästään hyökkäykseen. Monet nykyajan kyberrikollisorganisaatiot käyttäytyvät kuten tavalliset lailliset organisaatiot ja esimerkiksi Conti Ransomware-as-a-Service -ryhmä on hyödyntänyt IAB:ta tehokkuutensa lisäämiseksi palkkaamalla heidät tekemään alustavan työn. (ReliaQuest 2022; CISecurity s.a.)



Kuva 1. Lunnashaittaohjelmien kehitys (SOCRadar 2023)

3.2 Lunnashaittaohjelmien leviämien ja toimintaperiaatteet

Hyökkääjät käyttävät usein erilaisia keinoja lunnashaittaohjelmien levittämiseen, mutta yksi yleisimmistä keinoista on käyttää ”troijalaista” eli naamioidaan haittaohjelma luotettavan ja

harmittoman näköiseksi ohjelmaksi tai tiedostoksi. Useimmiten troijalainen aktivoituu vasta, kun käyttäjä ajaa ohjelman, mutta joissain tapauksissa pelkkä ohjelman lataaminenkin voi riittää.

Haittaohjelma voidaan naamioida esimerkiksi turvallisen näköiseksi liitetiedostoksi ja lähettää se sähköpostilla tuhansille käyttäjille samanaikaisesti. Sähköpostissa pyritään huijaamaan käyttäjää avaamaan tai suorittamaan tiedosto, ja näin saadaan tartutettua tietokone haittaohjelmalla. Tätä taktiikkaa kutsutaan sosiaaliseksi manipuloinniksi (social engineering). (Cloudflare s.a. d)

Microsoft Word tai Excel-tiedostoissa haittakoodi voi olla piilotettuina makroihin. Makrot automatisoivat toistuvia tehtäviä Wordissa, mikä sujuvoittaa käyttäjän toimimista ympäristössä. Käyttäjä voidaan saada huijaamalla suorittamaan makrot tai valitsemalla asetus, joka sallii makrojen suorittamisen automaattisesti. Tällä tavalla saadaan haittaohjelma leviämään.

Haittaohjelma voidaan myös toimittaa käyttäjän laitteelle exploit-kittien avulla. Exploit-kit on verkkorikollisten työkalupaketti, joka asetetaan verkkosivulle. Tämä työkalupaketti etsii jokaisen verkkosivulla käyneen kävijän laitteista haavoittuvuuksia ja jos haavoittuvuus löytyy, sitä hyödynnetään haittaohjelman asennuksessa. (Fsecure, 2024)

Haittaohjelma voi myös asentua Drive-by-latauksella (drive-by-download), jossa käyttäjän tarvitsee vain vierailla saastuneella, hyökkääjän hallitsemalla sivustolla ladatakseen haitallisen tiedoston. Hyökkääjä voi myös saastuttaa muita harmittomia sovelluksia tai luoda omia väärennettyjä sovelluksia, esimerkiksi pelien piraattiversiot, haittaohjelmien levittämiseen. Myös sovellusten ja järjestelmien haavoittuvuudet voivat tarjota aukon haittaohjelmien levittämiseen. Hyökkääjät voivat luoda matoja, jotka leviävät haavoittuvuuden kautta verkoissa, ilman, että käyttäjän tarvitsee tehdä mitään. (Cloudflare s.a. d)

Asennuksen jälkeen haittaohjelma voi pysyä piilossa odottaen aktivoimiskäskyä tai tiettyä tapahtumaa, esimerkiksi tietyn sovelluksen avaamista. (Avast 2020) Lunnashaittaohjelman aktivoituessa, se salaa järjestelmän tiedostot ja ruudulle ilmestyy viesti. Viestissä yleensä kerrotaan kuka tai mikä haittaohjelma on lukinnut tiedostot, ja annetaan ohjeet lunnaiden maksamiseksi kryptovaluutalla. Viestissä luvataan usein, että tiedostot palautetaan maksun jälkeen, mutta tämä ei välttämättä pidä aina paikkaansa. Uhria saatetaan myös kiristää uhkaamalla jättää tiedostot palauttamatta tai julkaisemalla arkaluonteista tietoa, jos lunnaita ei makseta tietyssä ajassa. (Cloudflare s.a. d) Kiristystä voi tapahtua useilla tasoilla: salattuja tietoja ei palauteta, varastetut tiedot julkaistaan tai myydään rikollisilla markkinoilla tai uhriin kohdistetaan vielä palvelunestohyökkäys, jos lunnaita ei makseta. (Tatar, S. 2025; Parvini, S. 2025)

3.3 Lunnashaittaohjelmatyypit

Lunnashaittaohjelmia voi olla erilaisia ja ne voivat vaihdella toimintatavoillaan ja tavoitteillaan. Kuitenkin hyvin yleinen piirre on, että käyttäjän tärkeisiin tietoihin pyritään päästä käsiksi ja kiristää rahaa niiden palauttamiseksi. Lunnashaittaohjelmat voidaan jakaa useisiin tyyppeihin, kuten crypto-ransomware, locker-ransomware, scareware ja dowxware, jotka kaikki hyödyntävät eri taktiikoita painostaakseen uhria maksamaan lunnaat.

Crypto-ransomware salaa mobiililaitteen tai tietokoneen tiedostoja kiristääkseen rahaa. Tiedoston sisältö sekoitetaan niin, että ne eivät ole enää luettavissa, ja normaalitilaan palautumiseen tarvitaan salausavain. Maksaessa lunnaat uhri saa salausavaimen. Tämä haittaohjelma käyttää pelottavia ja näyttäviä keinoja painostaakseen uhria maksamaan lunnaat. Jotkin crypto-ransomware-variantit eivät edes salaa tiedostoja ollenkaan, vaan uhkailevat sillä kiristääkseen uhrilta rahaa. Useimmiten uhkaus kuitenkin toteutetaan. Tunnetuimpia ovat CryptoLocker, TeslaCrypt ja Petya.

Haittaohjelma voi päätyä uhrin järjestelmälle esimerkiksi troijalaisia lataavien ohjelmistojen kautta tai exploit-kittien kautta, mutta yleisimmin sitä ilmenee sähköpostien tai pikaviestien kautta, jossa haittaohjelma saadaan näyttämään luotettavalta tiedostolta. Yleisimpiä tiedostotyyppejä, joiden mukana haittaohjelma voi tulla on Microsoft Word -dokumentit, Microsoft Excel-tiedostot, XML-dokumentit ja pakatut kansiot (esim. zip-tiedostot) joiden sisällä on haitallinen JavaScript-tiedosto, joka lataa haittaohjelman. Pelkkä sähköpostin saaminen ei itsessään aiheuta haittaohjelmatartuntaa, vaan haittaohjelma täytyy suorittaa laitteella. Hyökkääjä voi yrittää uhria sosiaalisella manipuloinnilla suorittamaan haitallisen ohjelman, joka lataa haittaohjelman järjestelmään. (Fsecure, 2024) Tämä haittaohjelmatyyppi voi olla erityisen vaarallinen yrityksille, jotka säilyttävät järjestelmissään arvokkaita tietoja. (Fsecure, 2024)

Kun crypto-ransomware salaa tiedostojen sisällön ja vaatii lunnaita niiden palauttamiseksi, locker-ransomware taas estää pääsyn laitteen tietoihin tai sovelluksiin. Jotta pääsy järjestelmään palautetaan, haittaohjelma vaatii lunnaita. Tämä haittaohjelma ei kuitenkaan vahingoita käyttäjän tietoja, toisin kuin crypto-ransomware, joka salaa tiedot. (Encyclopedia 2024) Käyttäjän laite voidaan lukita niin, että ohjelma simuloi lukitusnäyttöä käyttämällä koko näytön kokoista selainikkunaa ja poistamalla käytöstä tehtäväpalkin, kursorin ja pikanäppäimet. Haittaohjelma voi myöskin muuttaa laitteen salasanoja ja PIN-koodeja, mikä voi olla lamauttavaa, koska tietoja ei välttämättä saada silloin ollenkaan palautettua. Locker-ransomwaret esittävät usein itsensä viranomaista ja esittävät lunnaat ”pakollisena sakkona”, toisin kuin crypto-ransomwaret, jotka eivät peittele rikollista toimintaansa. Haittaohjelmaa voidaan levittää esimerkiksi roskapostina, piilottaa houkuttteleviin mainoksiin nettisivulla tai piilottaa sovelluksiin. (Check Point 2024) Tämä tyyppi on

puolestaan erityisen vaarallinen yrityksille, joiden toiminta on riippuvainen järjestelmien käytettävyydestä, kuten sairaaloissa.

Scareware puolestaan hyödyntää pelottelua ja sosiaalista manipulointia sadakseen uhrin paljastamaan esimerkiksi henkilötietojaan tai lataamaan haittaohjelman laitteelleen. Yleisin scarewaren muoto on verkkosivulla ilmestyvä ponnahdusikkuna, jossa varoitetaan esimerkiksi viruksesta uhrin laitteella. Viestissä saattaa lukea esimerkiksi: ”Laitteellasi on virus! Paina tästä laataksesi virustorjuntaohjelma ja poistaaksesi viruksen.” Oikeasti laitteella ei välttämättä ole virusta ollenkaan, mutta scareware väittää tarjoavansa ratkaisua tähän ongelmaan, mitä ei oikeasti ole. Ponnahdusikkuna saattaa käyttää tunnettujen yritysten logoja, jotta viesti näyttäisi legitiimiltä. Kun uhri uskoo viestin ja ohjelman, hän asentaakin tietämättään haittaohjelman, joka on naamioitu virustorjuntaohjelmaksi. (IBM s.a. a)

Arkaluonteisia tietoja säilyttävälle yrityksella vaarallinen lunnashaittaohjelma voi olla Doxware (tiedetään myös nimellä extortionware). Se on lunnashaittaohjelmatyyppi, joka ei ainoastaan lukitse uhrin tiedostoja, vaan myös uhkaa julkaista ne julkisesti. Tyypillisesti doxware pääsee uhrin järjestelmään tai verkkoon haitallisten ohjelmistojen asennuksen tai haitallisten liitteiden latausten kautta. Haittaohjelma salaa tiedostot ja uhkaa julkaista varastamansa tiedot julkisessa verkossa, mikäli lunnaita ei makseta. Tämä voi yritykselle tarkoittaa esimerkiksi luottamuksellisten asiakirjojen tai asiakasrekisterin paljastumista. (SecureMac 2020)

Yksi nykyaikaisemmista malleista on Ransomware-as-a-Service (RaaS) -malli, joka on niin sanotusti haitallinen versio Software-as-a-Service (SaaS) ohjelmistopalvelumallista. Se toimii liiketoimintamallina, jossa valmiiksi kehitettyjä lunnashaittaohjelmia myydään tai vuokrataan yhteistyökumppaneille. RaaS-mallin myötä hyökkääjän ei tarvitse olla kokenut ohjelmoija, sillä haittaohjelman käyttö on mahdollista kaikille riippumatta ohjelmointitaidoista. Monet RaaS-organisatiot kuitenkin tarkistavat mahdollisten yhteistyökumppaneidensa taustat ja digitaalisen jalanjäljen sekä mahdollisesti haastattelevat ennen pääsyn myöntämistä palveluihin. RaaS-malli tekee lunnaskampanjoista helppoa toteuttaa, sillä se tarjoaa hyökkääjille asiantuntijatason haittaohjelmiston sekä ympärivuorokautista teknisen tuen sen käyttöön. Tämä malli on rikollisille helppokäyttöinen ja tehokas malli, ja siksi se on nykyään merkittävä kyberturvallisuusuhka yrityksille. Varautuminen ja suojautuminen RaaS-hyökkäyksiä vastaan tulisi olla yrityksille siis erityisen tärkeää. (Palo Alto Networks s.a. b)

3.4 Lunnashaittaohjelmahyökkäyksen vaikutus Pk-yrityksille

Accenturen kyberrikollisuustutkimus paljastaa, että lähes 43 % kyberhyökkäyksistä kohdistuu pk-yrityksiin. (Palatty, N. 2025) Onnistuneilla lunnashaittaohjelmahyökkäyksillä voi olla kauaskantoisia

vaikutuksia pk-yrityksiin. Hyökkäykset voivat johtaa merkittäviin taloudellisiin tappioihin, jotka syntyvät vaadituista lunnaista sekä myös liiketoiminnan keskeytymisestä. SkyGroupin artikkelissa todetaan, että Britanniassa pk-yritysten kyberhyökkäyksistä aiheutuvat päivittäiset tappiot ovat noin 31 000 puntaa, mikä tarkoittaa yhteensä noin 900 000 euroa 24 päivän aikana. (SkyGroup 2024) Pk-yrityksille jopa yksi lunnashaittaohjelmahyökkäys voi olla kohtalokas, koska yrityksillä ei välttämättä ole varaa toipua iskusta. Pk-yritykset usein tarvitsevat lainarahoitusta toimiakseen, ja suurin osa pääomasta on sijoitettu liiketoimintaan, joten likvidejä varoja ei ole riittävästi saatavilla.

Toiminnalliset vaikutukset voivat olla myös huomattavia pk-yrityksille. Lunnashaittaohjelmahyökkäykset voivat estää pääsyn kriittisiin järjestelmiin ja tietoihin, mikä pysäyttää tai ainakin hidastaa yrityksen päivittäistä liiketoimintaa. Tällöin työntekijöiden tuottavuus laskee ja kyky palvella asiakkaita heikkenee. Keskimäärin lunnashaittaohjelmahyökkäyksestä toivuttiin 24 päivässä vuoden 2020 ja 2022 välillä Yhdysvalloissa. (Statista 2024)

Lunnashaittaohjelmahyökkäys voi vaikuttaa negatiivisesti asiakassuhteisiin sekä yhteystyökumppanuuksiin. Jos yrityksen maine kärsii tai luottamus heikkenee, seurauksena voi olla pitkäaikaisia ongelmia ja menetettyjä yhteistyömahdollisuuksia tulevaisuudessa. Esimerkiksi tietovuotojen paljastuminen voi vaarantaa myös yhteistyökumppanin brändin, jos kumppanin arkaluonteisia henkilötietoja pääsee vääriin käsiin.

3.5 Torjuntastrategiat ja parhaat käytännöt pk-yrityksessä

Kyberuhkien torjunta ja ennaltaehkäisy tulisi olla erityisen tärkeää pk-yrityksille, koska niiden resurssit ja kyky kestää kyberhyökkäyksistä aiheutuvia taloudellisia sekä maineeseen liittyviä vahinkoja, ovat rajalliset. Hyökkäykset, joilla voi olla vakavia seurauksia yrityksen toimintaan, vaativat tehokkaita torjuntastrategioita. Nämä strategiat eivät pelkästään rajoitu teknisiin ratkaisuihin, kute palomuureihin ja virustorjuntaan, vaan vaativat myös kokonaisvaltaista lähestymistapaa, joka sisältää henkilöstön koulutuksen ja jatkuvan tietoturvatietoisuuden ylläpitämisen.

Henkilöstön koulutus ja tietoisuuden lisääminen, pitäisi olla keskeisimpiä askelia, joita tulisi ottaa ensimmäisenä. Verizonin vuoden 2023 kyberturvallisuusraportti tuo esiin, kuinka inhimilliset tekijät, kuten työntekijöiden virheet ja tietämättömyys, ovat merkittävä syy kyberhyökkäyksen taustalla. Raportissa kerrotaan, että jopa 74 %:ssa kyberhyökkäyksistä hyödynnetään ihmisen tekemää virhettä. (Verizon 2023, 8) Tämä korostaa, kuinka suuri riski kouluttamattomilla työtekijöillä on yritykselle, ja kuinka tärkeää on investoida työntekijöiden koulutukseen kyberhyökkäysten ennaltaehkäisemiseksi. Yleisimmät tavat, joilla haittaohjelma päätyy yrityksen järjestelmiin tai

verkkoon ovat sähköpostien kautta. Tämän vuoksi henkilöstöä tulisi kouluttaa tunnistamaan ainakin esimerkiksi phishing- eli kalasteluviestit sekä muut epäilyttävät sähköpostit.

Säännöllinen varmuuskopioiden tekeminen on keskeinen osa varautumista haittaohjelmahyökkäyksiin. Yrityksen tulisi varmuuskopioida säännöllisesti sille keskeiset tiedot, kuten asiakastiedot. Mitä useammin tietoja varmuuskopioidaan, sitä vähemmän dataa menetetään, mikäli haittaohjelmahyökkäys onnistuu. Varmuuskopioita on suositeltavaa säilyttää erityisesti niille suunnitelluissa paikoissa, fyysisesti ja verkon ulkopuolella. Näin varmistetaan, että varmuuskopiot ovat suojassa, vaikka verkkoon kohdistuisi hyökkäys. Mikäli lunnashaittaohjelmahyökkäys tapahtuu, yritys voi palautua ennalleen käyttämällä varmuuskopioita, ilman että lunnaita tarvitsee maksaa.

Tietoturvan ulkoistaminen on myös viime vuosina yleistynyt. Yritykset ovat alkaneet tiedostamaan IT-osaston osaamisvajeensa sekä budjettirajoitteet. Kaspersky Labin tutkimuksen mukaan noin 70 % yrityksistä aikoo siirtää tietoturvan hallinnoinnin ulkoisille palveluntarjoajille seuraavan 12 kuukauden aikana. Suurimpina syinä on se, että palveluntarjoajilta saa käyttöönsä uusia työkaluja sekä ajankohtaista ja ympärivuorokautista asiantuntijuutta. Ulkoisen palvelun käyttö on skaalautuvaa sekä joustavaa, ja yritys saa laskettua kokonaiskustannuksiaan. (Kass, D. 2021)

Tekniset ratkaisut, kuten palomuurit, vahvat salasanat ja virustorjuntaohjelmat ovat keskeisiä työkaluja yrityksen tietotuvassa. Palomuurit estävät haitallista liikennettä pääsemästä verkkoon ja suojavat järjestelmiä ulkopuolisilta hyökkäyksiltä. Vahvat salasanat, jotka sisältävät sekä isoja että pieni kirjaimia, numeroita ja erikoismerkkejä, vähentävät salasanojen murtamisen riskiä. Virustorjuntaohjelmat puolestaan tunnistavat haittaohjelmat, kuten virukset tai lunnashaittaohjelmat, ja pyrkivät estämään niiden suorittamisen ja leviämisen. (Kaspersky s.a. a) Nämä ratkaisut tulisi ottaa käyttöön, sillä ne ovat kustannustehokkaita ja helppokäyttöisiä keinoja ottaa käyttöön.

Monitasoinen puolustus (defence-in-depth) kyberturvassa on puolustautumisstrategia, jossa käytetään useita tietoturvajärjestelmiä ja -käytäntöjä organisaation verkon, verkko-ominaisuuksien ja resurssien suojaamiseen. Resursseja pyritään suojaamaan eri tasoissa kuten fyysisesti, teknisesti ja hallinnollisesti ja pyritään käyttämään erilaisia tietoturvaratkaisuja. Strategian pohjimmainen periaate on se, että yksi ainoa tietoturvaratkaisu ei voi torjua kaikkia hyökkäyksiä, jolloin jos hyökkääjä kaataa yhden puolustuslinjan sen jälkeen on useita muita järjestelmiä ja tekniikoita hankaloittaakseen hyökkäyksen etenemistä. (Cloudflare s.a. a)

Verkon segmentointi on strateginen tapa jakaa verkko pienempiin aliverkkoihin eli segmentteihin, joista kukin toimii omana pienenä verkkonaan. Segmentoinnin tavoitteena on vähentää

verkkoliikenteen ruuhkia, tehostaa verkon suorituskykyä sekä parantaa verkon valvontaa ja tietoturvaa. Segmentoimalla verkko, voidaan rajoittaa hyökkääjän liikkumista ja estää haittaohjelmatartunnan esimerkiksi sisäisiin resursseihin, jotka sijaitsevat eri verkossa. Verkko voidaan segmentoida fyysisesti tai loogisesti. Fyysisessä segmentoinnissa verkko jaetaan fyysisesti eri osiin, mutta vähemmän joustava ratkaisu. Loogisesti segmentoitu verkko toteutetaan virtuaalisen verkon (VLAN) tai verkko-osoitteiden avulla, mikä tarjoaa enemmän joustavuutta, kuin fyysiset ratkaisut. (Palo Alto Networks s.a. b)

Yleisimpiä ja yksinkertaisimpia ratkaisuja haittaohjelmahyökkäysten ennaltaehkäisemiseksi on yrityksessä käytettävien laitteiden ohjelmistojen ylläpito ja päivitys. Päivitykset usein sisältävät tärkeitä tietoturvapäivityksiä, jotka korjaavat haavoittuvuuksia, joita hakkerit voivat hyödyntää. Tämän takia päivitykset olisi hyvä asentaa välittömästi, kun ne ovat saatavilla. Vanhentunut ohjelmisto voi heikentää laitteiden yhteensopivuutta ja heikentää suorituskykyä. Vanhettuneiden ohjelmistoversioiden heikkouksia voi jokainen hakea internetistä, mikä helpottaa hyökkääjää, kun ohjelmiston heikot kohdat ovat jo tiedossa. Siksi esimerkiksi automatisoidut ja aikataulutetut päivitykset ovat tehokas ja yksinkertainen ratkaisu tietotuvan ylläpitämiseksi. (Device Autohority s.a.)

Yrityksen riskienhallinta ja varautumissuunnitelmat ovat keskeisiä käytäntöjä lunnashaittaohjelmahyökkäysten varalle. Master Cardin tutkimus tuo esiin, että 86 % vastanneista pk-yrityksistä on tehnyt kyberturvariskien arvioinnin ja laatinut suunnitelman kyberuhkien torjumiseksi. Kuitenkin vain 23 % tuntee olevansa täysin varma kyberuhkien tunnistamisessa. (Gerber, J & Prokop J. 2025) Pk-yrityksen on tärkeää luoda skenaarioita ja varautua uhkien varalle. Kuitenkin tutkimuksesta voidaan päätellä, että uhkien tunnistaminen ei kuitenkaan ole vielä riittävällä tasolla, mikä korostaa yritysten tarvetta syventää kyberriskien arviointia rikienhallinnassaan.

Muita yleisiä haittaohjelmien torjuntaratkaisuja voi olla esimerkiksi Endpoint Detection and Response (EDR) ja kybervakuutus. EDR on päätelaitteiden turvallisuusratkaisu, joka valvoo aktiivisesti käyttäjien laitteita havaitakseen ja torjuakseen kyberuhkia, kuten lunnashaittaohjelmia ja muita haittaohjelmia. EDR tallentaa päätelaitteiden käyttäytymistä, analysoi epäilyttäviä toimintoja ja estää haitallisia toimintoja. Se toimii reaaliajassa ja tarjoaa kattavan näkyvyyden päätelaitteiden tapahtumiin. EDR mahdollistaa kyberhyökkäyksen estämisen ja tutkinnan sekä analysoinnin pohjalta nopeatkin korjausliikkeet, mikäli päätelaite on altistunut hyökkäykselle. (Aarness, A. 2025.)

Kybervakuutuksella tarkoitetaan vakuutusyhtiön tarjoamaa vakuutusta, joka usein kattaa yhtiön taloudellisia menetyksiä, joita aiheutuu kyberhyökkäyksistä, kuten tietomurroista, lunnashaittaohjelmahyökkäyksistä ja muista tietoturvaloukkauksista. Vakuutus voi korvata

liiketoiminnan keskeytykset, oikeuskuluja, tietomurron selvittämiseen menneitä kuluja ja mainehaitan kuluja. Jotkin vakuutukset voivat kattaa jopa lunnaista aiheutuvia kuluja. Vakuutuksen kattavuus voi vaihdella yrityksen tarpeiden ja toimialan mukaan. Se ei välttämättä kata sitä, jos yhteistyökumppanilta vuodetaan tiedot, uhka tulee yhtiön sisältä tai valtiollisia hyökkäyksiä. Vaikka kysyntä kybervakuutukselle on lisääntynyt, on vakuutushinnatkin nousseet ja monet vakuutusyhtiöt asettavat tiukempia verkkoturvallisuusvaatimuksia vakuutettavalle yritykselle. (IBM s.a. b) Kybervakuutus ja EDR-ratkaisut ovat usein kuitenkin isommille yrityksille tavanomaisia ja voivat olla verraten kalliita pk-yrityksille, minkä takia pk-yritykset voivat mahdollisesti karisia näistä.

3.6 Mitä tulisi tehdä, jos hyökkäys on jo tapahtunut?

Lunnashaittaohjelmahyökkäyksen sattuessa ensimmäiseksi on tärkeää tunnistaa hyökkäys ja toimia nopeasti. Nopealla reagoinnilla voidaan estää haittaohjelman leviäminen ja lisävahinkojen syntyminen esimerkiksi eristämällä saastuneet laitteet verkosta. (Kyberturvallisuuskeskus 2024) Myös aikaisessa vaiheessa on tärkeää kääntyä tietoturva-asiantuntijan puoleen. Jos yrityksellä on haittaohjelmahyökkäyksiä kattava vakuutus, on hyvä sinne suuntaan olla yhteydessä, että saa neuvoja, kuinka tilanteessa tulisi toimia. On tärkeää edetä ennalta suunnitellun toimintasuunnitelman mukaan virheiden välttämiseksi. Jos yrityksellä ei ole lunnashaittaohjelmahyökkäyksen varalta vakuutusta, voi yritys kääntyä Viestintäviraston kyberturvallisuuskeskuksen puoleen. Tapahtuneesta kannattaa olla kaikille mahdollisimman läpinäkyvä ja ilmoittaa asiasta etenkin asiakkaille ja yhteistyökumppaneille sekä tietenkin tehdä rikosilmoitus. (Eisto, S. 2017) Tapahtuneen salailu paljastuessaan voi aiheuttaa epäluottamusta.

Henkilötietojen tarkkaan dokumentointiin on tärkeä keskittyä, kun yrityksessä on tapahtunut tietoturvaloukkaus. Yrityksen on tärkeää tunnistaa, mitä tietoja on mahdollisesti viety tai salattu. Suomessa tietosuojavaltuutetun toimisto valvoo henkilötietojen käsittelyä. Jos yrityksessä on tapahtunut tietoturvaloukkaus, on siitä GDPR:n mukaan ilmoitettava 72 tunnin kuluessa valvontaviranomaiselle. On myös syytä ilmoittaa viipymättä henkilötietojen tietoturvaloukkauksesta rekisteröidylle, mikäli tästä aiheutuu korkea riski henkilön oikeuksille ja vapauksille. (Tietosuojakeskus s.a.; GDPR Hub s.a.) Tietoturvaloukkauksen salailusta tai tietoturvan laiminlyönnistä vois saada rangaistuksia, jos yritys käsittelee henkilökohtaisia ja arkaluonteisia tietoja. Vuonna 2018 ja 2019 aikana tapahtuneet Vastaamon tietomurrot ovat hyvä esimerkki siitä, että tietoturvan laiminlyönnillä yrityksen johto voi joutua rikosoikeudellisikseen vastuuseen. (Mäntysalo, J. 2025)

Rikollisille ei kannata maksaa lunnaita, sillä se saattaa rohkaista rikollisia jatkamaan toimintaansa. Myöskään ei ole mitään takuuta tiedostojen palautumisesta, vaikka lunnaat maksettaisiin. (Kyberturvallisuuskeskus 2024) Suomessa lunnaiden maksaminen kryptovaluuttoina ei itsessään

ole laitonta, mutta se voi olla ristiriidassa esimerkiksi rahanpesulain tai muiden lakien kanssa. Rahanpesulaki säätelee rahanpesun estämistä ja voi myös näin ollen koskea tilannetta, jossa lunnaiden maksaminen rikollisille tapahtuu kryptovaluuttoina. Tämä voidaan katsoa rikolliseksi toiminnaksi rahoittamalla rikollista toimintaa kryptovaluutoilla, joita on vaikeampi jäljittää. (Finlex 2017)

Hyökkäyksen tapahduttua, hyviin käytäntöihin kuuluu myös koko prosessin tarkka dokumentointi. Tämä voi auttaa hyökkäystä tutkivaa tutkijaa ymmärtämään tapahtuman kulkua sekä yritystä ymmärtämään hyökkäyksen laajuutta ja kokonaisvaltaista vaikutusta yrityksen toimintaan. Dokumentointi helpottaa myös hyökkäyksen jälkeistä analyysia sekä auttaa yritystä varautumaan paremmin ja ennaltaehkäisemään tulevia hyökkäyksiä.

3.7 Haasteet

Pk-yritysten haasteet voivat olla monenlaisia kyberuhkien torjumiseen liittyen ja usein ne liittyvätkin resurssien, osaamisen ja tietoisuuden puutteeseen. Nämä haasteet tekevät pk-yrityksistä alttiita kasvaville kyberuhille. Pk-yrityksiin hyökätään enenevissä määrin ja BlackFogin vuonna 2024 julkaisemassa tutkimuksessa kerrotaan, että jopa 61 % Yhdysvaltojen ja Yhdistyneen kuningaskunnan pk-yrityksistä on joutunut onnistuneen kyberhyökkäyksen kohteeksi viimeisen vuoden aikana. (Robb, B. 2024)

Pk-yrityksillä on usein rajalliset taloudelliset ja henkilöstöresurssit yrityksen tietoturvan ylläpitämiskeksi sekä parantamiseksi. Yrityksillä ei ole omia IT-asiantuntijoita tai tietoturvan erikoistuneita osaajia. Pienemmillä yrityksellä on luonnollisesti pienemmät tulot, mikä tarkoittaa, että tietoturvaan panostettavat resurssit ovat vähäiset. Sen vuoksi käyttöön ei oteta kehittyneimpiä tietoturvateknologioita, ja käytössä olevat teknologiat ovat vanhoja, mikä suurentaa kyberhyökkäyksen riskiä. (Chidukwani, A. 2022; Tetteh, A. 2024) Tutkimuksien mukaan 35 % pk-yrityksistä Australiassa osoittaa erillisen budjetin tietoturvalle, kun taas 65 % ei täytä NIST CSF-viitekehyksen suositusta. (ScienceDirect 2024) NIST CSF on Yhdysvaltain kansallisen standardointiviraston (NIST) kehittämä ohjeistus kyberturvallisuuden ja riskien hallintaan. (IBM s.a. c)

Haasteita lunnashaittaohjelmia vastaan kohdataan erityisesti puutteellisen tietoturvatietämyksen ja koulutuksen vuoksi. Yhdysvalloissa ja Kanadassa tehdyssä tutkimuksessa, jossa on valittu 1200 pk-yritystä, 34 % vastanneista yrityksistä ei tarjonnut työntekijöilleen lainkaan koulutusta, jonka avulla työntekijät voisivat tunnistaa tavallisimpia kalastelusähköposteja. (Cleary, Q. 2023) Lisäksi tietoturvaosaajia ei ole markkinoilla tarpeeksi. Asiantuntijoista on pulaa esimerkiksi energiasektorilla maailmanlaajuisesti. (Uwasa 2023)

Australiassa lähes puolet pk-yrityksistä uskovat voivansa suojautua kyberrikollisuudelta rajoittamalla verkkonäkyvyyttään. Yhtiöt keskittyvät vähentämään näkyvyyttä verkkosivustoillaan, sosiaalisessa mediassa ja yhteystiedoissaan ja vain 15 % vastaajista tarjoaa verkkosivuston, jossa voi katsella tai ostaa tuotteita. Tehdystä kyselytystä voidaan päätellä, että yrityksillä ei ole ollut tarpeeksi tietämystä kyberriskeistä, sillä riskit eivät rajoitu pelkästään verkkosivustoihin tai sosiaaliseen mediaan, vaan myös kaikkiin yhtiön laitteisiin kuten esimerkiksi tietokoneisiin, puhelimiin ja muihin IoT-laitteisiin, jotka ovat verkossa. Myöskin 55 % vastanneista kertoi käyttävänsä sähköpostia yhtiön pääasiallisesti viestinnässä tietämättään altistuneensa kalastelu- tai lunnashaittaohjelmahyökkäyksille. (Chidukwani, A. 2022)

Yhdysvalloissa tehdyn tutkimuksen mukaan, pienyritykset eivät ymmärrä tarpeeksi hyvin alttiuttansa kyberhyökkäyksille. Yritykset eivät usko, että he tallentavat tarpeeksi arvokasta dataa, minkä takia kyselyn mukaan yli puolet eivät ole ottaneet tarvittavia toimenpiteitä tai investoineet kyberhyökkäyksiä vastaan. Todellisuudessa yritykset kuitenkin säilyttivät sähköpostiosoitteita, puhelinnumeroita, postiosoitteita, kotiosoitteita, sosiaalitunnuksia ja luottokorttitietoja. Nämä tiedot, joita yritykset pitivät arvottomina, ovat henkilökohtaisesti tunnistettavaa tietoa (PII), joka muodostaa perustan useimmille yksityisyydensuojalainsäädännöille useissa maissa. Artikkelissa Bhattacharya kertoo, että pienyritykset keskittyvät aina ensisijaisesti myyntiin ja tuloihin selvitäkseen ja pitääkseen liiketoimintaa yllä. Tietoturva jää usein vähemmälle huomiolle, koska niitä ei pidetä arvokkaina panoksina ydintoimintaan. Artikkelin ”Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity” mukaan aiempien tutkimuksien pohjalta on todettu, että pk-yritykset rahoittavat tietoturvatoimiansa vasta kyberhyökkäyksen tapahduttua. (Becker, J., Johnson, S. & Rombaldo Junior, C. 2023, 12)

Mastercardin tekemän kyselyn mukaan, johon osallistui 500 pk-yrityksen omistajaa neljältä eri mantereelta, kävi ilmi, että 46 % oli kokenut kyberhyökkäyksen. Lähes joka viides kohteeksi joutuneista on sen seurauksen hakeutunut konkurssiin tai lopettanut toimintansa. Lisäksi taloudellinen ja maineen palautuminen voi olla erittäin hidasta. Vastaajista 80 % kertoi joutuvansa käyttämään paljon aikaa asiakas- ja luottamussuhteiden palauttamiseen hyökkäyksen jälkeen. (Mastercard 2025)

4 Tutkimus

Tutkimuksen tavoitteena oli selvittää pk-yritysten edustajien näkemyksiä ja kokemuksia lunnashaittaohjelmien torjunnassa, siihen liittyvistä haasteista ja parhaista käytännöistä. Tutkimus toteutettiin laadullisena teemahaastattelulla, Google Forms -kyselyllä ja sähköpostitse kerätyillä vastauksilla. Tutkimukseen osallistujia henkilöitä oli viisi, ja he olivat yrityksen toimitusjohtajia tai yrityksen IT-vastaavia.

4.1 Tutkimuksen tavoitteet ja kohderyhmä

Tutkimuksen tavoitteena oli kartoittaa pk-yritysten edustajien näkemyksiä ja kokemuksia haittaohjelmien torjunnasta sekä siihen liittyvistä haasteista ja parhaista käytännöistä. Tutkimusta varten lähetin pk-yrityksille kyselyn tai haastattelin pk-yritysten toimitusjohtajia sekä IT-asiantuntijoita, jotka osallistuvat yrityksen tietoturvaratkaisuiden päätöksentekoon ja suunnitteluun. Haastattelujen ja kyselyiden avulla pyrittiin saamaan suuntaa antava kuva pk-yritysten valmiudesta lunnashaittaohjelmien torjunnassa sekä tunnistamaan konkreettisia ongelmia ja haasteita lunnashaittaohjelmien torjunnassa. Yritykset valittiin sattumanvaraisesti eri toimialoilta.

Tutkimukseen kutsuttiin osallistumaan 35 etukäteen valittua pk-yritystä, jotka edustivat eri toimialoja ja sijaitsivat eripuolella Suomea. Kaikkien yritysten henkilömäärä ja liikevaihto tarkistettiin etukäteen, ja vaikka yritysten koot vaihtelivat, ne kuitenkin täyttivät pk-yritysten määritelmän. Kutsutuista yrityksistä viisi osallistui varsinaiseen tutkimukseen.

4.2 Tutkimusmenetelmä ja toteutus

Tutkimus toteutettiin laadullisena eli kvalitatiivisena tutkimuksena, koska tarkoitus oli syventyä pk-yritysten edustajien kokemuksiin, näkemyksiin ja havaintoihin lunnashaittaohjelmien torjumisesta ja siihen liittyvistä haasteista. Tutkimuksessa käytettiin teemahaastattelumenetelmää, koska se mahdollistaa näkemysten ja kokemusten keräämisen lunnashaittaohjelmien torjunnasta ja siihen liittyvistä haasteista. Osa haastatteluista suoritettiin Teams -videoneuvottelun välityksellä etänä, osa Google Forms -kyselyillä ja osa sähköpostitse. Haastateltavat saivat itse päättää osallistumistavan.

4.3 Haastattelujen toteutus

Jokaiselle haastateltavalle lähetettiin sähköpostia, jossa kerrottiin mistä haastattelusta on kyse, miten haastattelu toteutetaan, kuinka kauan vastauksia säilytetään ja myös mainittiin, että kaikkiin kysymyksiin ei myöskään tarvitse vastata, jos ei halua. Lisäksi henkilöt, jotka osallistuivat Teams -haastatteluun, annettiin kysymykset luettavaksi etukäteen. Näin heille annettiin mahdollisuus

valmistautua haastatteluun etukäteen. Haastattelu eteni ennalta suunniteltujen kysymysten mukaan, mutta keskustelua ohjailtiin tarpeen mukaan, jotta haastateltavan kokemuksia ja näkemyksiä saatiin esille mahdollisimman kattavasti.

Haastattelut nauhoitettiin osallistujien suullisella suostumuksella, jotta vastauksia voitaisiin analysoida tarkasti. Haastattelut kestivät keskimäärin 20 minuuttia ja sisälsivät kysymyksiä lunnashaittaohjelmien torjumisesta, tietoturvahaasteista pk-yrityksissä ja yritysten valmiudesta torjua niitä.

4.4 Kyselylomakkeen käyttö ja sähköpostivastaukset

Henkilöille, jotka eivät halunneet osallistua haastatteluun kasvotusten, vastasivat kyselylomakkeella tai sähköpostitse samoihin kysymyksiin. Lomakkeeseen täyttäminen oli vaivattomin vaihtoehto, sillä suurin osa kysymyksistä oli monivalintatehtäviä. Avoimiin kysymyksiin vastaajat saivat vastata niin pitkästi kuin itse kokivat tarpeelliseksi. Lomake ja sähköpostivaihtoehdot kehitettiin helpottamaan osallistumista tutkimukseen ja madaltaakseen osallistumiskynnystä. (Liite 1: Google Forms- kysely) Sähköpostiin vastanneet saivat samat kysymykset kuin kyselyssä, mutta kysymyksiin täytyi vastata avoimesti, ilman monivalintavastauksia.

4.5 Aineiston kerääminen, käsittely ja analysointi

Aineisto kerättiin kolmella tavalla: Teams-palvelun kautta toteutetulla haastattelulla, Google Forms-kyselyllä sekä sähköpostitse saaduilla vastauksilla. Haastattelu nauhoitettiin osallistujan luvalla, jotta vastauksiin olisi helpompi palata vastausten dokumentointia ja analysointia varten. Sähköpostista sekä kyselyistä saadut vastukset tallennettiin PDF-muotoon tutkimuksen suorittajan henkilökohtaiselle tietokoneelle sekä pilvialustalle, joihin pääsy on ainoastaan vain tutkimuksen suorittajalla.

Kerätty aineisto litteroitiin eli kirjoitettiin tekstimuotoon helpottamaan analyysia. Litterointi toteutettiin tarkasti, jotta osallistujien vastaukset ja ilmaisut tulivat selkeästi esiin alkuperäisessä muodossaan. Monivalintakysymyksistä saadut kvalitatiiviset tulokset analysoitiin käyttäen yksinkertaisia tilastollisia menetelmiä, kuten prosenttijakaumia. Avoimista kysymyksistä kerätty laadullinen tieto puolestaan analysoitiin sisällönanalyysilla, jonka avulla tunnistettiin ja luokiteltiin aineistosta esiin nousevia havaintoja ja kokemuksia.

4.6 Eettiset kysymykset

Tutkimuksessa otettiin huomioon myös eettiset periaatteet, jotka ovat olennaisia laadullisessa tutkimuksessa sekä osallistujien oikeuksien ja yksityisyyden turvaamisessa. Kaikille osallistujille kerrottiin etukäteen tutkimuksen tavoitteet, toteutustapa sekä aineiston käsittelyyn liittyvät käytännöt. Osallistujille kerrottiin, että osallistuminen on vapaaehtoista ja osallistumisen voi peruuttaa missä tahansa vaiheessa ennen opinnäytetyön julkaisua. Kaikkia osallistujia kohdeltiin tasavertaisesti ja kunnioittavasti. Heille annettiin mahdollisuus päättää mihin kysymyksiin he haluavat vastata ja kuinka pitkästi.

Osallistujille kerrottiin, että osallistumalla he antavat luvan vastausten hyödyntämiseen tutkimuksessani. Haastateltavilta varmistettiin suullinen lupa nauhoittamiseen. Näin varmistettiin, että haastateltavat ovat tietoisia tutkimuksen luonteesta ja aineiston käytöstä.

Kerätty aineisto kerättiin turvallisesti, sitä säilytetään suojatusti ja pääsy siihen on vain tutkimuksen tekijällä. Kaikki aiheeseen liittyvä kerätty aineisto ja nauhoitusmateriaalit tuhotaan turvallisesti, kun tutkimus on saatu päätökseen. Näin varmistetaan yritysten yksityisyys ja ennalta ehkäistään aineiston leviäminen.

5 Tulokset ja pohdinta

Haastattelujen ja kyselyiden perusteella ilmeni, että 80 %:lle eli suurimmalle osalle tutkimukseen osallistuneista yrityksistä lunnashaittaohjelmat ovat käsitteenä tuttuja tai he ovat vähintään kuulleet aiheesta aikaisemmin. Tutkimuksessa oli mukana yrityksiä eri aloilta, kuten finanssi-, teknologia- ja energia-aloilta sekä yrityspalveluja tarjoavilta sektorilta, mikä antoi mahdollisuuden vertailla tietoturvakäytäntöjen ja uhkakuvien tunnistamisen eroja myös toimialojen välillä. Yksikään tutkimukseen osallistuneista yrityksistä ei ollut tähän mennessä kokenut lunnashaittaohjelmahyökkäystä, mutta yritykset tunnistivat ne yleisesti vakavana ja mahdollisena uhkana liiketoiminnalleen. Toimenpiteet lunnashaittaohjelmien torjumiseksi vaihtelivat merkittävästi yritysten resurssien ja toimialan mukaan, mutta valtaosalla oli kuitenkin jo jonkinlaisia konkreettisia toimia tai varautumissuunnitelmia kyberuhkien varalta.

Tutkimukseen osallistuneista yrityksistä yli puolet koki lunnashaittaohjelmat konkreettisena uhkana omalla toimialallaan. Finanssialan yritys nosti esiin, että finanssi- ja pörssiyhtiöt kiinnostavat kyberrikollisia, koska niillä on usein hallussaan arvokasta ja luottamuksellista dataa. Energia-alan yritys ei kokenut puolestaan olevan kyberrikollisten potentiaalinen kohde, koska yritys on suhteellisen pieni, eikä siksi välttämättä herätä rikollisten kiinnostusta.

Yritysten kyky selviytyä mahdollisesta lunnashaittaohjelmahyökkäyksestä vaihteli. Yrityksistä kaksi viidestä koki selviytyvänsä hyökkäyksestä, kun taas yksi yritys oli hieman epäröivä, mutta arvioi kykenevänsä mahdollisesti selviämään. Loput kaksi yritystä eivät osanneet arvioida kykyään selvitä iskusta. Tämä voi kertoa siitä, ettei useimmilla yrityksillä kuitenkaan ole tarkkaa käsitystä omista valmiuksistaan tai toimintatavoistaan kriisitilanteissa. Ainostaan yksi yrityksistä pystyi itsevarmasti kertomaan, että heillä on olemassa järjestelmät ja toimintatavat, joilla pystyvät varmistamaan nopean palautumisen normaaliin tilaan liiketoiminnan katkoksista.

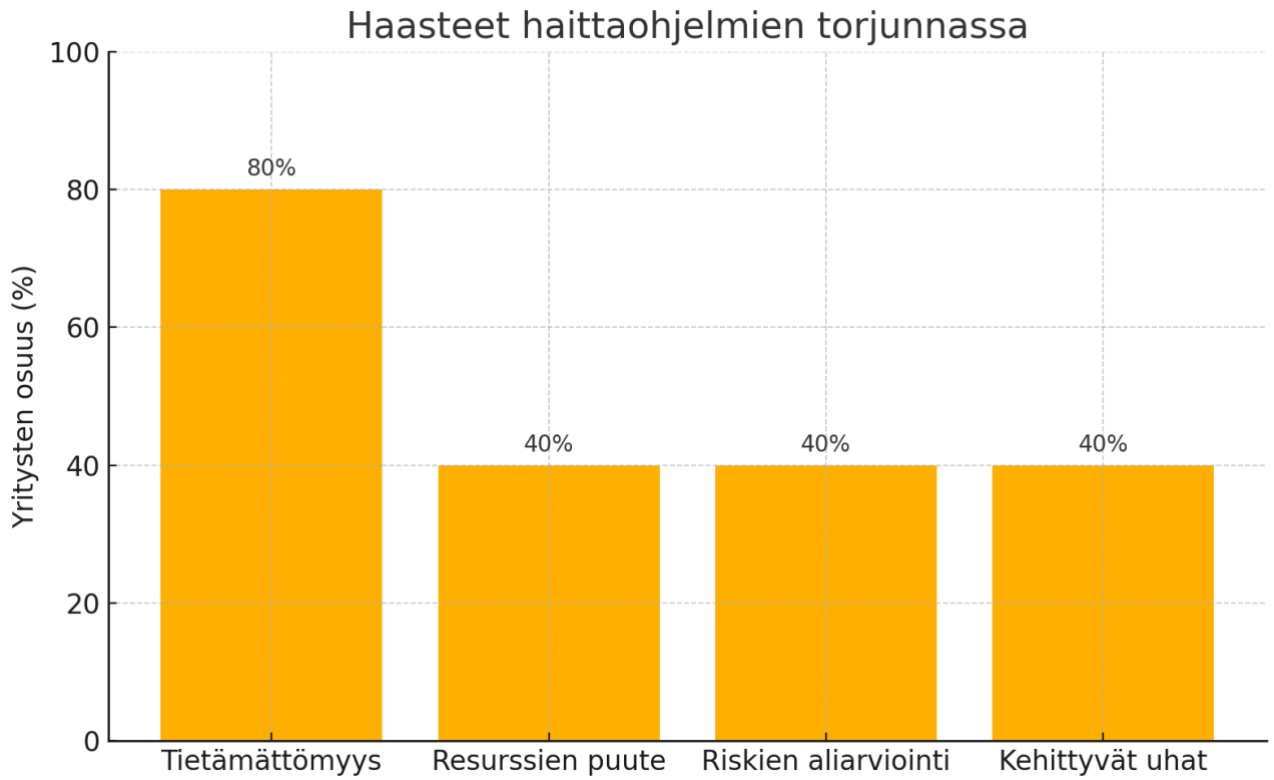
Yli puolet yrityksistä kertoivat tietoturvansa olevan joko kokonaan tai ainakin osittain ulkoistettu ammattilaisille. Tämä kertoo siitä, että pk-yritykset ovat tunnistaneet oman osaamisensa ja resurssien rajallisuuden tietoturvassa, jolloin ulkopuolisen ammattilaisen hyödyntäminen nähdään turvallisena ja kustannustehokkaana ratkaisuna. Kaksi viidestä kuitenkin koki pystyvänsä huolehtimaan tietoturvastaan yrityksessä ilman ulkoisten palveluiden apua.

Kuitenkin yli puolet vastanneista yrityksistä koki, että heidän tämänhetkiset resurssinsa lunnashaittaohjelmien torjumiseksi olivat riittävän hyvät. Yksi yritys tunnisti resurssiensa riittämättömyyden, ja yksi yritys ei ottanut kantaa asiaan. Vastaukset voivat viitata siihen, että yritykset ovat pääosin tietoisia riskeistä ja uhista sekä uskovat hallitsevansa nykyistä tilannetta

tämänhetkisillä resursseilla. Toisaalta on myös mahdollista, että ajatellaan ylioptimistisesti omia valmiuksia, sillä todellista lunnashaittaohjelmahyökkäystä ei olla vielä koettu.

Suurimmiksi haasteiksi yritykset mainitsivat yleisen tietämättömyyden mahdollisista riskeistä, riksien aliarvioinnin, kehittyvät uhat, työntekijöiden inhimilliset virheet sekä resurssien puutteen. Yrityksistä neljä viidestä mainitsivat, että tietäjättömyys mahdollisista tietoturvauhista ja riskeistä sekä työntekijöiden inhimillisten virheet niiden torjunnassa ovat keskeisiä haasteita. Yritystä perustettaessa ei usein selvitetä riittävästi mahdollisia tietoturvaan liittyviä uhkia, eikä niihin osata varautua tarpeeksi hyvin. Teknologiayritys X, kertoi, että monesti startupia perustettaessa ei laiteta perusasioita kuntoon ja tietoturva jää huomioimatta. Nuorella yrityksellä voi myöskin olla paljon kuluja, mutta vähän tuloja. Siksi yritykset ovatkin maininneet, myös resurssien puutteen yhdeksi suurimmista haasteista. Yrityksen on tärkeä saada yritys pidettyä hengissä ja kasvaa. Siksi voi olla, että panostus tietoturvaan jää vähäisemmäksi. Voi siis myös olla, että mahdolliset riskit tiedostetaan, mutta e aliarvioidaan js niitä ei pidetä itselleen tarpeeksi todennäköisinä. Resurssien puute voi myös olla henkisten resurssien puute, eli ei ole varaa palkata yritykseen alusta lähtien tietoturva-asiantuntijaa, jolloin tietoturvan tietämys yrityksessä voi jäädä heikoksi. Yrityksistä 40 % mainitsi haasteeksi myös lunnashaittaohjelmien ja muiden tietoturvauhkien jatkuvan kehittymisen. Jotta yritys pysyisi verkkorikollisten edellä ja pystyisi asianmukaisesti puolustautumaan hyökkäyksiltä, tulisi yrityksien investoida tietoturvaan jatkuvasti, mikä tietenkin maksaa yritykselle, ja silloin raha voi olla pois jostain muusta tärkeästä investoinnista.

Jatkuva tietoturvan päivittäminen vaatii paljon resursseja. Teknologia yritys X mainitsi myös, että kasvavilla yrityksillä ei ole usein riittävästi resursseja tietoturvan kehittämiseen ja että rikejä ei aina ymmärretä kunnolla. Teknologiayritys Y kertoo, että on vaikeaa pitää työntekijöiden kiinnostusta tietoturvasta yllä, jos ei ennestään ole aiheesta kiinnostunut.



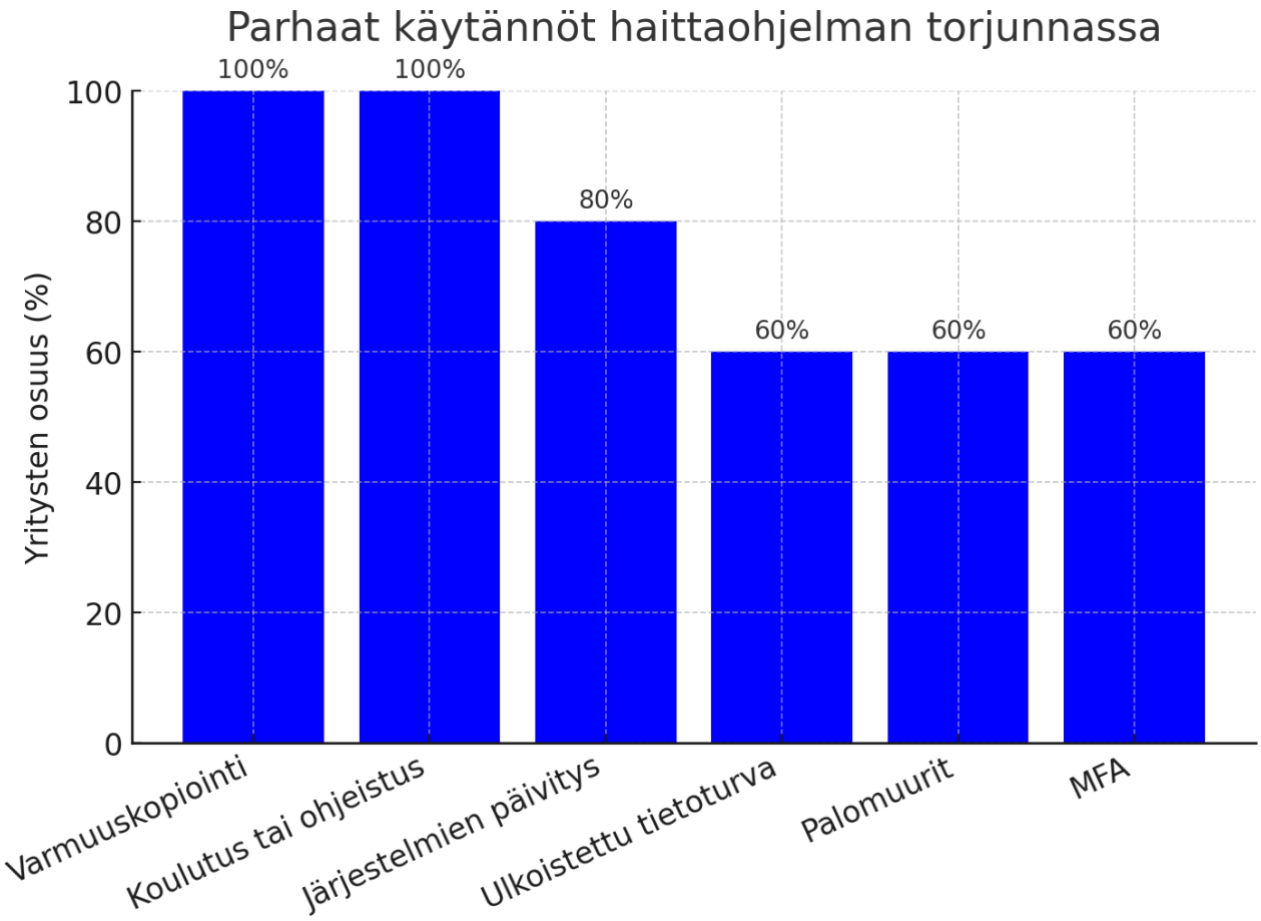
Kuvio 1. Haasteet lunnashaittaohjelmien torjunnassa haastattelun ja kyselyn pohjalta.

Parhaiksi käytännöiksi lunnashaittaohjelmien sekä muiden tietoturvauhkien torjuntaan osoittautui tietojen varmuuskopiointi, työntekijöiden tietoturvakoulutus tai -ohjeistus, laitteiden päivitysten ylläpito, ulkoistettu tietoturva, palomuurit sekä monivaiheinen tunnistautuminen (MFA). Kaikki haastateltavista yrityksistä varmuuskopioi tietonsa saannollisesti ja tämä osoittautuikin suosituimmaksi tavaksi varautua mahdollisia hyökkäyksiä ja tietojenmenetystä vastaan. Riippuen datasta, yritykset kertoivat varmuuskopioivansa tärkeimpiä tietoja päivittäin ja vähemmän tärkeämpiä tietoja esimerkiksi viikon välein. Yksi yrityksistä kertoi käyttävänsä kaksinkertaista varmuuskopiointia, eli datasta luotiin kerran vuodessa myös fyysinen kopio.

Suurimmalla osalla yrityksistä oli myös tietoturva kokonaan tai osittain ulkoistettu, eli yrityksen tietoturvaa hoitaa ulkoinen tietoturvaan erikoistunut yritys tai palvelu. Tämä on yleinen ratkaisu yrityksien keskuudessa, jotka tiedostavat, että heillä ei ole tarpeeksi resursseja huolehtia tietoturvasta täysin itse. Yritykset pitivät myös hyödyllisenä työntekijöidensä kouluttamista tai ohjeistamista tietoturvaan sekä laitteiden päivitysten ylläpitämistä. Kaikki vastanneista yrityksistä ohjeistaa tai kouluttaa työntekijöitään jollain tasolla tietoturvaan liittyen.

Yli puolet vastanneista yrityksistä mainitsivat palomuurit sekä monivaiheisen tunnistamisen (MFA) hyödylliseksi tietoturvauhkia torjuttaessa. Muita vähemmän mainittuja parhaita käytäntöjä oli esimerkiksi muiden spesifien tietoturva- tai torjuntaohjelmien käyttö, verkkosuojaukset, ulkoisten

asiantuntijoiden konsultaatiot, uhkasimulaatiot, verkon segmentointi, sähköpostien suodattimet, Zero Trust- malli sekä salasanojen hallinta Ledgerissä.



Kuvio 2. Parhaat käytännöt lunnashaittaohjelmien torjuntaan haastattelun ja kyselyn pohjalta.

Vaikka usealla yrityksellä oli tietoturva ulkoistettuna, eivät he kuitenkaan tee juurikaan yhteistyötä muiden toimijoiden kanssa. Yrityksistä vain finanssialan yritys toimi viranomaisten kanssa aktiivisesti. Yrityksistä 60 %:lla ei ollut tai eivät osanneet sanoa onko yrityksellä vakuutus, joka kattaisi lunnashaittaohjelmat. Kahdella yrityksellä oli vakuutukset, jotka kattavat lunnashaittaohjelman aiheuttamat haitat tai siitä aiheutuvat liiketoiminnan katkokset.

Asteikolla arvosanalla 1–5, jossa 1 on heikko ja 5 on erittäin tärkeä, yritykset antoivat tietoturvan tärkeydeksi yrityksessä keskiarvolta arvosanan 4,4. Tästä voidaan päätellä, että vastanneet yritykset pitävät tietoturvaa yrityksessään tärkeänä. Kuitenkaan yrityksen toimialalla ei ollut hirveästi vaikutusta siihen pitikö yritys tietoturvaa yrityksessään tärkeänä. Teknologiayritys X antoi arvosanaksi 5, kun taas teknologiayritys Y antoi arvosanaksi 3. Y perusteli arvosanaansa sillä, että tärkeintä on pyrkiä tekemään kustannustehokkaimmat toimenpiteet.

5.1 Johtopäätökset ja suositukset

Tutkimuksen ja aiempien tutkimuksien perusteella voidaan päätellä, että pk-yritykset ovat enenevissä määrin kyberuhkien, kuten lunnashaittaohjelmien kohteena. Vaikka useimmat yritykset tunnistivat lunnashaittaohjelmat todellisena uhkana liiketoiminnalleen, valmiuksissa torjua ja selviytyä hyökkäyksestä on huomattavia eroja. p tämän opinnäytetyön tuloksia aiempiin pk-yrityksiä käsitteleviin tutkimuksiin haasteista ja parhaista käytännöistä, törmää laajasti samoihin havantoihin. Resurssien niukkuus, puutteellinen tietoisuus ja osaaminen olivat merkittävimmät haasteet pk-yrityksille lunnashaittaohjelmien torjunnassa. Lisäksi aiempien tutkimusten perusteella havaittiin, että yritysten käsitys omista kyvyistään suojautua lunnashaittaohjelmia vastaan tai selviytyä niistä voivat olla optimistisia, mikä voi johtaa kyberuhkien aliarviointiin.

Useimmissa keskeisissä raporteissa (Verizon 2023; Clearly, Q. 2023) koulutusta pidetään lähtökohtana hyökkäyksien ennaltaehkäisemiseksi ja myös opinnäytetyön tutkimuksessakin tuli esille erityisesti henkilöstön koulutus. Tutkimuksessa selvisi, ettei pk-yrityksillä välttämättä ole tarpeeksi tietämystä kyberuhista ja siksi tietoisuuden lisääminen ja tietoruvan kiinnostuksen lisääminen tulisi olla ensimmäisenä listassa, kun parannetaan pk-yrityksen tietoturvaa. Inhimillisten virheiden merkitys kasvaa digitalisoituvassa maailmassa, kun järjestelmien yleinen tietoturvan taso nousee, mutta ihmisten tekemät virheet eivät vähene ilman koulutusta. Tutkimuksessa tuli esille, että tietämättömyys on suurimpia haasteita tietoturvan ylläpitämisessä, ja siksi aktiivinen koulutus ja selkeät ohjeet uhkien ja kalastelusähköpostien tunnistamiseen ovat välttämättömiä. Laitteiden tekninen suojaaminen, kuten päätelaitteiden suojaus, palomuurit, virustorjunta ja monivaiheinen tunnistautuminen tulisi nähdä perustason vaatimuksina, sillä ne ovat suhteellisen helppoja ja edullisia ratkaisuja, ja pienentävät huomattavasti kyberhyökkäysten riskiä.

Suositeltavaa on tehdä säännöllinen tietojen varmuuskopiointi (Device Authority s.a.; Science Direct 2024). Tutkimuksen vastauksien perusteella myös haastateltavat on yleisesti nähneet tämän käytännöllisenä ja tehokkaana keinona minimoida vahinkoja lunnashaittaohjelmahyökkäyksen sattuessa tai muissa tapauksissa, jossa yrityksen tärkeä data voidaan ulkoisen tapahtuman seurauksena menettää. Varmuuskopioiden olisi hyvä olla erillään yrityksen pääverkosta, jotta tiedot saadaan palautettua hyökkäyksen sattuessa. Hyviin käytäntöihin kuuluisi, että kopiot olisivat tallennettuna myös irrallaan verkosta tai fyysisenä, jolloin hyökkääjä ei pääse käsiksi varmuuskopioihin verkon kautta

Myöskin järjestelmien jatkuva ja aktiivinen päivittäminen nähtiin hyödyllisenä. Teknologia vanhentuu nopeasti ja vanhentunut ohjelmisto avaa rikollisille aukkoja tunkeutua järjestelmään. Säännöllisellä päivitysprosessilla varmistetaan, että uusimmat tietoturvakorjaukset tulevat nopeasti käyttöön, jolloin haavoittuvuudet suljetaan, ennen kuin niitä ehditään hyödyntämään.

Automatisoidut päivitykset tehostavat päivitysten seurantaa ja vähentävät inhimillisiä unohduksia ja virheitä.

Monet ulkomaalaiset pk-yritykset ovat siirtäneet tietoturvansa ulkopuoliselle toimijalle. (Kass, D. 2021) Yhtäläisyyttä ilmeni myös tutkimuksessa. Silloin kun yrityksen päättäjät ovat ymmärtäneet, että yrityksellä ei ole tarpeeksi tietämystä tai resursseja pitää omia tietoturva-asiantuntijoita, on päädytty käyttämään ulkoisia asiantuntijoita. Ulkoistettu tietoturva on osoittautunut realistiseksi ratkaisuksi pk-yrityksille, jotka eivät pysty ylläpitämään omaa tietoturvatiimiään. Tietoturvapalveluiden käyttö mahdollista asiantuntijoiden hyödyntämisen tehokkaasti, silloin kun on tarvetta. Kun yrityksen tietoturvan voi luovuttaa ulkoisen osapuolen hoidettavaksi, pienempi henkilökunta voi keskittyä yrityksen juoksevien asioiden hoitamiseen sekä tuloksen tekemiseen, eikä tietoturvasta tarvitse murehtia.

Pk-yritysten tulisi ymmärtää kyberturvallisuus jatkuvana prosessina. Kyberrikolliset kehittävät jatkuvasti uusia keinoja hyökätä yrityksiin ja siksi on tärkeää pysyä hyökkääjien edellä. Tietoturvan ylläpitäminen vaatii säännöllisiä investointeja, tietoturvakäytäntöjen päivittämistä ja henkilöstön motivaation ylläpitämistä tietoturvaa kohtaan. Yrityksen johdolla tulisi olla aktiivinen rooli tietoturvan korkean tason ylläpitämisessä, sillä tietoturva on myös yrityksen liiketoiminnan kannalta oleellinen aihe. Hyökkäyksestä palautuminen voi käydä kalliiksi, ja siksi yritykselle halvempi ratkaisu olisi ylläpitää yrityksensä tietoturvaa.

Vaikka tulokset tukivat pitkälti aikaisempia tutkimuksiin ja teorioita, on opinnäytetyössä tehdyn tutkimuksen otanta suhteellisen pieni. Tämä on tärkeä huomioida, sillä pienempi otanta rajoittaa tulosten yleistettävyyttä ja niiden luotettavuutta. Tästä syystä tutkimukseni löydöksiä on syytä tarkastella opinnäytetyön kontekstissa, eikä niitä voida välttämättä soveltaa suoraan vastaaviin tilanteisiin.

5.2 Pohdinta

Tämän opinnäytetyön tarkoituksena oli selvittää pk-yritysten parhaita käytäntöjä lunnashaittaohjelmien torjunnassa sekä tunnistaa tähän liittyviä keskeisiä haasteita. Tutkimuksessa perehdyttiin kirjallisuuskatsauksen avulla siihen, miten lunnashaittaohjelmat toimivat, kuinka niitä voi torjua, mitkä ovat aiemmin todettuja parhaita käytäntöjä sekä mitä haasteita pk-yritykset voivat kohdata lunnashaittaohjelmien torjunnassa. Lisäksi aineistoa kerättiin haastattelemalla pk-yritysten edustajia ja toteuttamalla kyselytutkimus, jotta teoreettinen tieto voitiin yhdistää yritysten käytännön kokemuksiin ja näkemyksiin.

Tutkimuksen tulosten perusteella merkittävimpiä haasteita pk-yrityksille ovat rajalliset resurssit, tietämättömyys kyberuhista sekä nopeasti muuttuvat kyberuhat. Parhaiksi käytännöiksi

lunnashaittaohjelmien torjunnassa osoittautui säännöllinen tietojen varmuuskopiointi, henkilöstön koulutus sekä järjestelmien aktiivinen päivittäminen. Työssä esitettiin konkreettisia suosituksia, joiden avulla pk-yritykset voivat parantaa tietoturvaansa ja vähentää riskiä joutua lunnashaittaohjelmahyökkäysten kohteeksi.

Opinnäytetyö tarjoaa hyödyllistä tietoa erityisesti startupin tai pk-yrityksen tietoturvasta vastaaville henkilöille. Aihe on ajankohtainen, sillä pk-yrityksiin kohdistuvien kyberhyökkäysten määrä on kasvussa, ja onnistuneen hyökkäyksen seuraukset voivat olla yritykselle vakavia. Työ luo myös hyvän pohjan jatkotutkimuksille, kuten henkilöstön koulutuksen vaikuttavuuden tarkempaan selvittämiseen.

Jatkotutkimuksena voisi selvittää tarkemmin, kuinka henkilöstön koulutus vaikuttaa pk-yritysten valmiuteen torjua lunnashaittaohjelmia ja miten työntekijöiden tehokkuutta haittaohjelmien ehkäisyssä voisi parantaa. Henkilöstön koulutuksen merkitys pk-yritysten tietoturvakäyttäytymisessä on keskeinen jatkotutkimuksen kohde, sillä suuri osa onnistuneista haittaohjelmahyökkäyksistä johtuu ihmisten tekemistä virheistä. Usein juuri työntekijän huolimattomuus, esimerkiksi kalasteluviestien avaaminen tai haitallisten linkkien klikkaaminen mahdollistaa haittaohjelman pääsyn yrityksen järjestelmiin. Tämä korostaa ihmisen roolia osana yrityksen tietoturvan heikointa lenkkiä. Virheiden vähentämiseksi koulutuksen tulisi olla käytännönläheistä ja säännöllistä. Esimerkiksi realististen tapausesimerkkien läpikäynti ja simulaatioharjoitukset voivat parantaa työntekijöiden valmiuksia. Lisäksi on tärkeää pyrkiä nostamaan työntekijöiden motivaatiota ja kiinnostusta tietoturvaa kohtaan. Jatkotutkimuksessa voitaisiin kartoittaa tarkemmin, mitkä koulutusmenetelmät vaikuttavat kustannustehokkaimmin työntekijöiden tietoturvakäyttäytymiseen ja vähentämään inhimillisiä virheitä.

Opinnäytetyön toteutukseen liittyi joitakin rajoitteita ja haasteita, jotka voivat vaikuttaa tulosten tulkintaan ja luotettavuuteen. Keskeisenä haasteena oli haastateltavien saaminen tutkimukseen mukaan. Tämä johtui todennäköisesti siitä, että tietoturva koetaan monissa yrityksissä arkaluonteiseksi ja luottamukselliseksi aiheeksi, miksi epäröivät kertoa siitä avoimesti ulkopuolisille tahoille. Lisäksi osa vastaajista saattoi epäillä yhteydenottoa tietojenkalasteluksi, mikä vähensi halukkuutta osallistua tutkimukseen. Kyselyyn vastaamisen aikataulutus oli monelle vaikeaa, yritysten rajallisista ajallisista resursseista johtuen. Vaikka kyselylomakkeella onnistuttiin tavoittamaan suurempi joukko vastaajia, niiden kautta saatavan tiedon syvyys jäi hieman pintapuolisemmaksi kuin henkilökohtaisissa haastatteluissa. Kyselyissä saattoi myös esiintyä väärinymmärryksiä, jos vastaajat eivät ymmärtäneet kysymyksiä tai niihin liittyviä käsitteitä. Haastattelujen vähäinen osallistujamäärä voi heikentää tulosten yleistettävyyttä, ja suurempi haastattelujen määrä olisi mahdollistanut yksityiskohtaisemman analyysin sekä vahvistanut

tutkimustulosten luotettavuutta. Myöskin ajallinen rajallisuus tutkimuksen tekemisessä madalsi osallistujien määrää, sillä enempää aikaa ei potentiaalisine osallistujien etsimiseen riittänyt.

Opinnäytetyöprosessi auttoi minua syventämään ymmärrystäni tietoturvasta ja erityisesti, miten pk-yritykset ovat alttiita kyberhyökkäyksille. Opin tunnistamaan millaisia haasteita yritykset kohtaavat lunnashaittaohjelmien torjunnassa sekä hyviä käytäntöjä niiden torjumiseksi. Haastatteluiden ja kyselyiden suunnittelu sekä niiden toteuttaminen kehittivät taitojani laadullisen tutkimuksen tekemisessä sekä erityisesti tiedon keräämisessä ja analysoinnissa.

Prosessin aikana kohtasin myös haasteita, kuten laajan lähdeaineiston hallintaa, pk-yritysten heikkoa halukkuutta osallistua haastatteluun ja kyselyihin sekä tutkimustulosten analysointi. Ajoittain koettu epävarmuus opinnäytetyön suunnasta auttoi ymmärtämään suunnitelmallisuuden ja aikataulutuksen tärkeyden sekä kyvyn toimia ajallisen paineen alla. Kirjallisuuskatsauksen laatiminen paransi kriittistä lukutaitoani ja kykyä tunnistaa relevanttia tietoa sekä analysoida ja yhdistellä eri lähteiden tarjoamia näkemyksiä.

Kokonaisuutena opinnäytetyöprosessi oli palkitseva ja opettavainen kokemus, joka vahvisti osaamistani ja valmiuksiani uraa varten tietoturva-alalla.

Lähteet

Aarness, A. 2025. What is endpoint detection and response (EDR). Crowdstrike. Luettavissa: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/. Luettu: 2.5.2025.

Avast. 2020. s.a. What is CryptoLocker ransomware and where does it come from? Luettavissa: https://www.avast.com/c-cryptolocker. Luettu: 13.5.2025.

Baker, K. 9.10.2022. History of ransomware. Crowdstrike. Luettavissa: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/history-of-ransomware/. Luettu: 19.1.2025.

Becker, J., Johnson, S. & Rombaldo Junior, C. 2023. University College of London. Luettavissa: https://arxiv.org/pdf/2309.17186. Luettu 2.4.2025.

Bitdefender. What is Ransomware? Prevention & Data Recovery. Luettavissa: https://www.bitdefender.com/consumer/support/answer/24260/. Luettu 13.5.2025.

Brewster, T. 2019. Mistaken for North Koreans. The 'Ryuk' ransomware Hackers Are Making Millions. Forbes. Luettavissa: https://www.forbes.com/sites/thomasbrewster/2019/02/20/mistaken-for-north-koreans-the-ryuk-ransomware-hackers-are-making-millions/. Luettu: 9.5.2025.

Chai, W. & Hashemi-Pour, C. 2023. What is the CIA triad (confidentiality, integrity and availability)? TechTarget. Luettavissa: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. Luettu: 2.10.2024.

Check Point. s.a. What is Locker Ransomware. Luettavissa: https://www.checkpoint.com/cyber-hub/ransomware/what-is-locker-ransomware/. Luettu 18.2.2025.

Chidukwani, A., Koutsakis, P. & Zander, S. 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access. Luettavissa: https://www.researchgate.net/publication/362628150_A_Survey_on_the_Cyber_Security_of_Small-to-Medium_Businesses_Challenges_Research_Focus_and_Recommendations. Luettu: 6.5.2025.

Chidukwani, A. 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommedations. IEEE Access. Luettavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9853515. Luettu: 2.4.2025.

Chidukwani, A., Koutsakis, P. & Zander, S. 2024. Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. Science Direct. Luettavissa: https://www.sciencedirect.com/science/article/pii/S0167404824003316?ref=pdf_download&fr=RR-2&rr=93b8beeb5b0d8d66. Luettu: 6.5.2025.

CIS Center. s.a. Initial Access Brokers How They're Changing Cybercrime. Luettavissa: https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime. Luettu: 4.3.2025.

CISA. 2016. CryptoLocker Ransomware Infections. Luettavissa: https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections. Luettu: 2.3.2025.

Cisco. s.a. What is cyber resilience? Luettavissa: https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html. Luettu: 5.1.2025.

Cleary, Q. 2023. The Devastating Impact of Ransomware Attacks on Small Businesses. University of Maryland. Luettavissa: https://www.law.umaryland.edu/content/articles/name-659577-en.html. Luettu: 14.5.2025.

Cloudflare. s.a. a. What is defense in depth | Layered security. Luettavissa: https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/. Luettu: 5.3.2025.

Cloudflare. s.a. b. What was the WannaCry ransomware attack? Luettavissa: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Luettu 18.2.2025.

Cloudflare. s.a. c. What are Petya and NotPetya? Luettavissa: https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/. Luettu: 18.2.2025.

Cloudflare. s.a. d. What is ransomware? | Ransomware meaning. Luettavissa: https://www.cloudflare.com/learning/security/ransomware/what-is-ransomware/. Luettu 19.2.2025.

Constantin, L. 2021. Ryuk explained: Targeted, devastatingly effective ransomware. CSO Online. Luettavissa: https://www.csoonline.com/article/569343/ryuk-explained-targeted-devastatingly-effective-ransomware.html. Luettu: 9.5.2025.

CWSI. s.a. The History of Ransomware. Luettavissa: https://cwsisecurity.com/history-of-ransomeware/. Luettu: 19.1.2025.

Device Authority. s.a. How Secure Software Updates Can Prevent Cyber Attacks on Connected Devices. Luettavissa: https://deviceauthority.com/9614-2/. Luettu: 2.5.2025.

Eisto, S. 2017. Kyberhyökkäys iskee yritykseen – näin tunnistat hyökkäyksen ja toimit oikein. OP Media. Luettavissa: https://www.op-media.fi/yrittajyys/kyberhyokkays-iskee-yritykseen--nain-tunnistat-hyokkayksen-ja-toimit-oikein. Luettu: 8.5.2025.

Encyclopedia. s.a. Locker Ransomware. Luettavissa: https://encyclopedia.kaspersky.com/glossary/blocker/. Luettu 18.2.2025.

Euroopan keskuspankki. s.a. What is cyber resilience? Luettavissa: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.fi.html. Luettu: 5.1.2025.

Euroopan komissio. s.a. a.Käyttöopas: Pk-yrityksen määritelmä. Luettavissa: https://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0007.01/DOC_1. Luettu 2.1.2025.

Euroopan komissio. s.a. b. Mitkä henkilötiedot katsotaan arkaluonteisiksi? Luettavissa: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_fi. Luettu: 2.10.2024.

Euroopan parlamentti. 20.4.2023. Kyberturvallisuus: nykyiset ja tulevat uhat – Yleisimmät kyberuhat vuonna 2022, kaikkien altteimmat sektorit ja Ukrainan sodan vaikutukset. Luettavissa: https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_fi.pdf?utm_source=chatgpt.com. Luettu: 8.1.2025.

FBI. s.a. Ransomware. Luettavissa: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware. Luettu: 5.1.2025.

FinCEN. 1.10.2020. Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. Luettavissa: https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Luettu: 5.1.2025.

Financial Times. 2021. Monero emerges as crypto of choice for cybercriminals. Luettavissa: https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6. Luettu: 2.1.2025.

Finlex. 2017. Laki rahapesun ja terrorismin rahoittamisen estämisestä. Luettavissa: https://www.finlex.fi/fi/lainsaadanto/2017/444. Luettu: 8.5. 2025.

Fokker, J. 2019. McAfee ATR Aalyzes Sodinokibi aka REvil Ransomware-as-a-Service – The All-stars. McAfee. Luettavissa: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-the-all-stars/. Luettu: 10.5.2025.

Fortinet. s.a. What Is The CIA Triad? Luettavissa: https://www.fortinet.com/resources/cyberglossary/cia-triad. Luettu: 2.10.2024.

F-Secure. s.a. Crypto-Ransomware. Luettavissa: https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml. Luettu: 18.2.2025.

GDPR Hub. s.a. KHO – KHO: 2024:115. Luettavissa: https://gdprhub.eu/index.php?title=KHO_-_KHO%3A2024%3A115. Luettu: 13.5.2025.

Gerber, J & Prokop J. 2025. Too small to be ignored? Not anymore. Why shoring up cyber defenses is crucial for small businesses. Luettavissa: https://www.mastercard.com/news/perspectives/2025/cybersecurity-for-small-business/. Luettu: 6.5.2025.

Greenberg, A. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. WIRED. Luettavissa: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Luettu: 18.2.2025.

HYPR. s.a. NotPetya. Luettavissa: https://www.hypr.com/security-encyclopedia/notpetya. Luettu: 18.2.2025.

Holdsworth, J. & Kosinski, M. 2024. What is ransomware as a service (RaaS)? IBM. Luettavissa: https://www.ibm.com/think/topics/ransomware-as-a-service. Luettu: 2.3.2025.

IBM. 2023a. What is scareware? Luettavissa: https://www.ibm.com/topics/scareware. Luettu: 17.2.2025.

IBM. s.a. b. What is cyber insurance? Luettavissa: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/. Luettu 2.5.2025.

IBM. s.a. c. What is the NIST Cybersecurity Framework? Luettavissa: https://www.ibm.com/think/topics/nist. Luettu: 14.5.2025.

Jyväskylän yliopisto. s.a Mitä on tietoturva? Luettavissa: https://www.jyu.fi/fi/yliopistopalvelut/digipalvelut/palvelut/tietoturva/mita-on-tietoturva. Luettu: 2.10.2024.

Kaspersky. s.a. a. Cybersecurity Tips for Small Businesses. Luettavissa: https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security. Luettu: 14.5.2025.

Kaspersky. s.a. b. Mikä on WannaCry-kiristysohjelma? Luettavissa: https://www.kaspersky.fi/resource-center/threats/ransomware-wannacry. Luettu: 18.2.2025.

Kaspersky. s.a. c. What is Cryptocurrency and how does it work? Luettavissa: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency. Luettu: 2.1.2025.

Kass, D. 2021. 70% of Organizations Will Use MSSPs for Outsourced Security in Next 12 Months, Study Finds. MSSP Alert. Luettavissa: https://www.msspalert.com/news/70-of-organizations-will-use-mssps-for-outsourced-security-in-next-12-months-study-finds. Luettu: 14.5.2025.

KnowBe4. s.a. a. AIDS Trojan or PC Cyborg Ransomware. Luettavissa: https://www.knowbe4.com/aids-trojan. Luettu 20.2.2025.

KnowBe4. s.a. b. GPcode Ransomware. Luettavissa: https://www.knowbe4.com/gpcode. Luettu: 20.2.2025.

Kyberturvallisuuskeskus. 2024. Mikä ihmeen kiristyshaittaohjelma? Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma. Luettu: 8.5.2025.

Malwarebytes. s.a. WannaCry. Luettavissa: https://www.malwarebytes.com/wannacry. Luettu: 18.2.2025.

Mastercard. 2025. Too small to be ignored? Not anymore. Why shoring up cyber defenses is crucial for small businesses. Luettavissa: https://www.mastercard.com/news/perspectives/2025/cybersecurity-for-small-business. Luettu: 6.5.2025.

Microsoft. s.a. Mitä on tietoturva? Luettavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-data-security. Luettu: 8.1.2025.

Mäntysalo, J. 2025. Työntekijöiden virhe mahdollisti Vastaamon tietomurron, sanoo Ville Tapion puolustus – syyttäjä vaatii kovempaa tuomiota. Yle. Luettavissa: https://yle.fi/a/74-20159716. Luettu: 8.5.2025.

NIST. s.a. Integrity. Luettavissa: https://csrc.nist.gov/glossary/term/integrity. Luettu: 2.10.2024.

National Cyber Security Centre. 2021. Mitigating malware and ransomware attacks. Luettavissa: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. Luettu: 14.5.2025.

Palatty, N. 2025. 51Small Business Cyber Attacks Statistics 2025 (And What You Can Do About Them). Astra Security. Luettavissa: https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/. Luettu: 17.2.2025.

Palo Alto Networks. s.a. a. What Is Network Segmentation. Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation. Luettu: 5.3.2025.

Palo Alto Networks. s.a. b. What is Rasomware as a Service (RaaS)? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service. Luettu 2.3.2025.

Parvini, S. 2025. Cybersecurity officials warn against potentially costly Medusa ransomware attacks. AP News. Luettavissa: https://apnews.com/article/fbi-cisa-gmail-outlook-cyber-security-email-6ed749556967654ff41a629a230973e6. Luettu: 13.5.2025.

Pure Storage. s.a. Life Cycle of a Ransomware Attack. Luettavissa: https://www.purestorage.com/knowledge/life-cycle-of-a-ransomware-attack.html. Luettu: 17.2.2025.

Reed, J. 2022. How Reveton Ransomware-as-a-Service changed cybersecurity. Security Intelligence. Luettavissa: https://securityintelligence.com/articles/how-reveton-raas-changed-cybersecurity. Luettu: 2.3.2025.

ReliaQuest. 2022. Initial Access Brokers in 2021: An Ever Expanding Threat. Luettavissa: https://reliaquest.com/blog/initial-access-brokers-in-2021-an-ever-expanding-threat/. Luettu: 4.3.2025.

Robb, B. 2024. New BlackFob research: 61% of SMBs were victims of a cyberattack in the last year. BlackFog. Luettavissa: https://www.blackfog.com/smbs-were-victims-cyberattack/. Luettu: 3.5.2025.

SOCRadar Research. 2023. Evolution of Ransomware: So Far and Hereafter. Luettavissa: https://socradar.io/evolution-of-ransomware-so-far-and-hereafter/. Luettu: 7.5.2025.

SecureMac. 2020. What is Doxware? Luettavissa: https://www.securemac.com/blog/what-is-doxware. Luettu: 17.2.2025.

Shea, S. 2025. The history and evolution of ransomware attacks. TechTarget. Luettavissa https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware. Luettu: 20.2.2025.

Sky Business. 2024. SMEs miscalculate the cost of cyber attacks on their business. Luettavissa: https://www.skygroup.sky/article/SMEs-miscalculate-the-cost-of-cyber-attacks-on-their-business. Luettu: 17.2.2025.

Statista. s.a. Average duration of downtime after a ransomware attack at organizations in the United States from 1st quarter 2020 to 2nd quarter 2022. Luettavissa: https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-us/. Luettu: 17.2.2025.

Stena Confidential. s.a. Mitä arkaluonteiset tiedot ovat? Luettavissa: https://www.stenaconfidential.com/fi/uutiset-tietoa-kierratyksesta/tietoa-kierratyksesta/oppaat-ja-artikkelit/mita-arkaluonteiset-tiedot-ovat/. Luettu: 2.10.2024.

Stewart, J. 2006. Arhiveus Ransomware Trojan Analysis. Secureworks. Luettavissa: https://www.secureworks.com/research/arhiveus. Luettu: 20.2.2025.

Suomi.fi. s.a. Tietoturva. Luettavissa: https://www.suomi.fi/kansalaiselle/oikeudet-ja-velvollisuudet/turvallisuus-ja-jarjestys/opas/tietoturva. Luettu: 8.1.2025.

Tatar, S. 2025. The Dangers of Double and Triple Extortion in Ransomware Attacks. Arctic Wolf. Luettavissa: https://arcticwolf.com/resources/blog/dangers-of-double-and-triple-extortion/. Luettu: 13.5.2025.

Tetteh, A. 2024. Cybersecurity needs for SMEs. Issues in Information Systems. Luettavissa: https://iacis.org/iis/2024/1_iis_2024_235-246.pdf. Luettu: 2.4.2025.

Thales Group. 20.3.2024. 2024 Thales Data Threat Report Reveals Rise in Ransomware Attacks, as Compliance Failings Leave Businesses Vulnerable to Breaches. Luettavissa: https://www.thalesgroup.com/en/worldwide/security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware-attacks. Luettu: 8.1.2025.

Tietosuoja. s.a. Tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietoturvaloukkaukse. Luettu: 8.5.2025.

Tietosuojakeskus. s.a. Miten toimitaan kyberhyökkäyksen sattuessa? Luettavissa: https://tietosuojakeskus.fi/tietoturva-loukkaus-toimintasuunnitelman-laatiminen. Luettu: 8.5.2025.

Trend Micro. 2021. Ransomware Double Extortion and Beyond: REvil, Clop and Conti. Luettavissa: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti. Luettu: 10.5.2025.

Vaasan yliopisto. 2023. Kyberturvallisuuden osaajapula haaste yrityksille – yliopistot lisäävät kyberturvallisuuden koulutustarjontaa. Luettavissa: https://www.uwasa.fi/fi/uutishuone/uutiset/kyberturvallisuuden-osaajapula-haaste-yrityksille-yliopistot-lisaavat. Luettu: 14.5.2025.

Verizon. 2023. DBIR – 2023 Data Breach Investigations Report. Luettavissa: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf. Luettu: 14.5.2025.

Washington University in St. Louis. s.a. Integrity. Luettavissa: https://informationsecurity.wustl.edu/items/integrity/. Luettu: 2.10.2024.

WatchGuard. s.a. Ransomware – AIDS Trojan. Luettavissa: https://www.watchguard.com/wgrd-ransomware/aids-trojan. Luettu: 20.2.2025.

Yrittäjät. s.a. Yrittäjyys Suomessa. Luettavissa https://www.yrittajat.fi/tietoa-meista/tietoa-yrittajajarjestosta/yrittajyys-suomessa/. Luettu: 8.1.2025.

Liitteet

Liite 1. Google Forms- kysely

Opinnäytetyö: Haastattelu pk-yritysten tietoturvasta (lunnashaittaohjelmat)

Tervetuloa vastaamaan kyselyyn! Tämä kysely on osa opinnäytetyötäni, jonka aiheena on **lunnashaittaohjelmien torjunta pk-yrityksissä: parhaat käytännöt ja haasteet**.

Vastauksesi ovat erittäin arvokkaita ja auttavat tuomaan esiin pk-yritysten kohtaamia haasteita ja kehittämään käytännön ratkaisuja. Tavoitteeni on kartoittaa pk-yritysten haasteita ja parhaita käytäntöjä lunnashaittaohjelmien torjunnassa, jotta startupit ja muut pk-yritykset voivat hyödyntää kerättyä dataa vahvistaakseen kyberresilienssiään ja parantaakseen tietoturvakäytäntöjään. Kysymykset ovat jaoteltu kahteen osioon: jos yrityksessä on tapahtunut lunnashaittaohjelmahyökkäys ja jos ei ole. Mikäli et halua ottaa kantaa onko yrityksessänne kyseinen hyökkäys tapahtunut, voit vastata kaikkiin haluamaasi kysymyksiin. Yleiskysymyksiin voi vasta siitä huolimatta, onko yrityksenne koskaan kokenut lunnashaittaohjelmahyökkäystä vai ei. Kaikkiin kysymyksiin ei ole pakko vastata, jos ette halua. Opinnäytetyöni kannalta arvokkainta olisi, jos voisitte vastata kysymyksiin, jotka käsittelevät yrityksenne kohtaamia haasteita lunnashaittaohjelmien (tai muiden kyberuhkien) torjunnassa. Lisäksi olisi erittäin hyödyllistä kuulla, mitkä toimintatavat olette kokeneet tehokkaiksi niiden torjunnassa.

Kyselyyn vastaaminen kestää noin 5-10 minuuttia, ja kaikki vastaukset käsitellään luottamuksellisesti. Kerätty data hävitetään välittömästi opinnäytetyön valmistuttua.

Jos sinulla on kysyttävää, haluat lisätietoja tutkimuksesta tai peruuttaa osallistumisesi kyselyyn, voit ottaa yhteyttä minuun sähköpostitse: **juho.tuovinen@hotmail.fi**.

Kiitos ajastasi ja arvokkaasta panoksestasi tutkimukseen!

- Juho Tuovinen

1. Kerro lyhyesti minkä alan yritystä edustat ja mikä on roolisi yrityksessä.

2. Onko lunnashaittaohjelmat ilmiönä sinulle tuttu?

   Merkitse vain yksi soikio.

   - ◯ Kyllä
   - ◯ Ei

Tässä on lyhyt kuvaus lunnashaittaohjelmasta, jos aihe ei ole sinulle ennestään tuttu:

Lunnashaittaohjelma (ransomware) on tietokoneeseen tai verkkoon leviävä haittaohjelma, joka lukitsee tiedostoja tai estää laitteen käytön. Hyökkääjä vaatii rahaa, yleensä kryptovaluutassa, jotta tiedostot vapautetaan tai laite avataan. Eli kyseessä on eräänlainen digitaalinen kiristys.

3. Oletteko kohdanneet lunnashaittaohjelmahyökkkäyksen?

   Merkitse vain yksi soikio.

   - ◯ Kyllä
   - ◯ En
   - ◯ En kommentoi

Mikäli vastasit edelliseen kysymykseen "En", vastaa seuraavaksi kysymyksiin 1 ja 2.

Jos vastasit edelliseen kysymykseen "Kyllä" , vastaa kysymyksiin 3-13.

Mikäli et halua kommentoida, onko yrityksenne kokenut lunnashaittaohjelmahyökkäystä, voit vapaasti vastata niihin kysymyksiin, jotka koet itsellesi sopiviksi.

Lopussa on yleiskysymykset 14–30, joihin voi vastata riippumatta siitä, onko yritykseenne koskaan kohdistunut lunnashaittaohjelmahyökkäystä vai ei.

4. 1. Miksi luulette, että yrityksenne ei ole kokenut lunnashaittaohjelmahyökkäystä?

5. 2. Uskotteko, että yrityksenne voisi selvitä lunnashaittaohjelmahyökkäyksestä?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

Vastaa kysymyksiin 3–13, mikäli yrityksenne on kohdannut lunnashaittaohjelmahyökkäyksen.
Jos olet kohdannut lunnashaittaohjelmahyökkäyksen edellisessä työpaikassasi, mutta et nykyisessä, mainitse ensimmäisessä esittelyosiossa nykyisen työpaikan sijaan entisen työpaikkasi toimiala sekä roolisi.

6. 3. Miten hyökkäys havaittiin ja miten siihen reagoitiin?

_____

_____

_____

_____

_____

7. 4. Mitkä olivat hyökkäyksen tapahtumat? Miten se aloitettiin ja mikä oli sen laajuus?

_____

_____

_____

_____

_____

8. 5. Mikä oli hyökkäyksen kohteena (esim. tietokannat, asiakastiedot, järjestelmät)?

9. 6. Mitä toimia teitte heti hyökkäyksen jälkeen?

10. 7. Mitä vaikutuksia hyökkäyksellä oli yrityksen toimintaan (esim. taloudelliset tappiot, maine)?

11. 8. Kuinka suuri oli lunnasvaatimus?

12. 9. Kuinka pitkään yrityksenne toipui hyökkäyksestä?

13. 10. Mitä opitte hyökkäyksestä ja miten se vaikutti tietoturvakäytäntöihin?

14. 11. Oletteko tehneet muutoksia tai parannuksia tietoturvatoimiinne hyökkäyksen jälkeen?

15. 12. Oliko teillä yhteistyötä viranomaisten tai asiantuntijoiden kanssa hyökkäyksen jälkeen?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

16. 13. Oletteko laatineet uuden varautumissuunnitelman tulevia hyökkäyksiä varten?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

YLEISKYSYMYKSET 14-30

Seuraavaksi alla esitetään yleiskysymyksiä. Kysymyksiin voi vastata riippumatta siitä, onko yritykseenne kohdistunut lunnashaittaohjelmahyökkäystä vai ei.

17. 14. Näettekö lunnashaittaohjelmat uhkana toimialallenne yleisesti? Miksi tai miksi ei?

18. 15. Onko yrityksenne tietoturva ulkoistettu?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

19. 16. Oletteko laatineet varautumissuunnitelman lunnashaittaohjelmien varalta? Mitä se sisältää?

20. 17. Onko teillä käytössä järjestelmiä tai työkaluja uhkien valvomiseksi?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

21. 18. Kuinka usein tarkastatte ja päivitätte tietoturvakäytäntöjänne?

Valitse kaikki sopivat vaihtoehdot.

- ☐ Harvemmin kuin kerran 10 vuodessa
- ☐ Vähintään kerran 10 vuodessa
- ☐ Vähintään kerran 5 vuodessa
- ☐ Vähintään kerran vuodessa
- ☐ Puolivuosittain (6kk välein)
- ☐ Useamman kerran vuoden aikana
- ☐ Ei päivitetä ollenkaan
- ☐ Jokaisen merkittävän muutoksen jälkeen (esim. kun otetaan käyttöön uusi järjestelmä)
- ☐ Tietoturvapoikkeamien jälkeen
- ☐ Muu: _____

22. 19. Oletteko tehneet riskiarviointeja?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

23. 20. Mitä toimenpiteitä olette toteuttaneet lunnashaittaohjelmien torjumiseksi?

Valitse kaikki sopivat vaihtoehdot.

- [ ] Tietoturvakoulutus
- [ ] Tietojen varmuuskopiointi
- [ ] Haittaohjelmien torjuntaohjelmat
- [ ] Palomuurien käyttö
- [ ] Verkkosuojauksen käyttö
- [ ] Järjestelmien päivittäminen
- [ ] Monivaiheinen tunnistautuminen
- [ ] Käyttöoikeuksien rajoittaminen
- [ ] Ulkoisten asiantuntujoiden konsultaatiot
- [ ] Tietoturvan ulkoistaminen
- [ ] Uhkasimulaatiot tai -harjoitukset
- [ ] Verkon segmentointi
- [ ] Tiedostojen salaaminen
- [ ] Sähköpostin suodattimet
- [ ] Zero Trust -malli
- [ ] Muu: _____

24. 21. Saavatko työntekijänne koulutusta lunnashaittaohjelmista tai tietoturvasta?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

25. 22. Onko yrityksellänne käytössä erityisiä turvatoimenpiteitä lunnashaittaohjelmien varalta? Jos on, mitä ne ovat?

26. 23. Mitkä ovat mielestänne suurimmat haasteet lunnashaittaohjelmien (tai muiden kyberuhkien) torjunnassa?

27. 24. Koetteko, että yrityksellänne on riittävästi resursseja suojautua lunnashaittaohjelmilta? Jos ei, mitä resursseja voisi mielestänne lisätä?

28. 25. Mitä parhaita käytäntöjä olette omaksuneet lunnashaittaohjelmien (tai mahdollisesti muiden kyberuhkien) torjumiseksi?

29. 26. Onko teillä käytössä varmuuskopiointijärjestelmä? Kuinka usein varmuuskopiot tehdään?

_____

30. 27. Teettekö yhteistyötä muiden yritysten tai viranomaisten kanssa tietoturvatoimien parantamiseksi?

Merkitse vain yksi soikio.

- ◯ Kyllä
- ◯ En osaa sanoa
- ◯ Ei
- ◯ Muu: _____

31. 28. Mitä teknologisia ratkaisuja tai työkaluja käytätte lunnashaittaohjelmien torjumiseksi?

_____

_____

_____

_____

_____

32. 29. Onko yrityksellänne kybervakuutusta ja kattaako se lunnashaittaohjelmat?

Merkitse vain yksi soikio.

- ◯ On vakuutus ja kattaa lunnashaittaohjelmat
- ◯ On vakuutus, mutta ei kata lunnashaittaohjelmia
- ◯ On vakuutus, mutta en osaa sanoa kattaako se lunnashaittaohjelmat
- ◯ En osaa sanoa
- ◯ Ei ole kybervakuutusta
- ◯ Muu: _____

33. 30. Kuinka tärkeänä pidätte tietoturvaa yrityksessänne asteikolla 1–5? (1 = ei kovin tärkeä, 5 = erittäin tärkeä)

Merkitse vain yksi soikio.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ Muu: _____