Verkkorikollisuuden kasvu ja sen vaikutus yksityisyyden suojaan

Ida-Nina Oinonen

Haaga-Helia ammattikorkeakoulu

Tradenomi

AMK-opinnäytetyö

2024

Tiivistelmä

Tekijä(t)
Ida-Nina Oinonen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Verkkorikollisuuden kasvu ja sen vaikutus yksityisyyden suojaan

Sivu- ja liitesivumäärä
29 + 7

Digitalisaation kehittyessä verkkorikollisuudesta on syntynyt yhä suurempaa huomiota ja toimenpiteitä vaativa uhka yksityisyyden suojalle. Verkkorikollisuudella on monia muotoja, tehden niiden torjumisesta haastavaa. Rikolliset voivat hyödyntää uusia haavoittuvuuksia yritysten verkkopalveluissa ja täten aiheuttaa yhteiskunnalle vahinkoa identiteettivarkauden, palvelunestohyökkäysten tai tietomurtojen muodossa.

Vaikka trendit ovat yleensä nopeasti muuttuvia, ovat Suomessa ne verkkorikollisuuden suhteen pysyneet vuodesta toiseen melko samanlaisina. Suomi hyödyntää viranomaisia kuten kyberturvallisuuskeskusta verkkorikollisuuden valvomiseen. Resursseja käytetään myös turvallisemman digiympäristön kehittämiseen esimerkiksi kyberturvallisuusstrategian avulla.

Tutkimuksen tarkoituksena on tutkia verkkorikollisuuden trendejä ja ilmenemisen muotoja, keskittyen Suomen lainsäädäntöön ja valtion käyttämiin säädöksiin. Tutkimuksessa pohditaan myös ilmiön vaikutusta ja haasteta tulevaisuuden näkökulmasta. Työ toteutettiin kirjallisuuskatsauksena, tutkimalla laajaa kirjoa erilaisia tieteellisiä artikkeleita, kirjallisuutta, raportteja sekä ajankohtaisia uutisia kuluvalta ja edellisiltä vuosilta.

Työn tavoitteena on herättää keskustelua verkkorikollisuuden kasvavasta ilmiöstä ja samalla antaa lukijalle kattava ymmärrys, miten verkkorikollisuus toimii uhkana yksityisyyden suojalle ilman aikaisempaa tuntemusta aiheesta. Työn avulla pyritään tutustuttaa lukija verkkorikollisuuden eri muotoihin ja esimerkkien avulla antaa realistinen käsitys, miten rikolliset toimivat verkossa. Työ keskittyy merkittävästi yritysten ja yksilöiden vastuuseen yksityisyyden suojan turvaamisessa.

Opinnäytetyön tutkimuksen tuloksena on havaittu, että vaikka yhteiskunta on kasvattanut tietoisuuttaan verkkorikollisuuden muodoista ja yksityisyyden suojan tärkeydestä, on vielä paljon tehtävää, jotta tulevaisuudessa voidaan rakentaa kehittynyttä ja yhä turvallista digiympäristöä. Vanheneva väestö ja resurssien puute on aiheuttanut hidastusta verkkorikollisuuden onnistuneessa torjunnassa, vaikka itse rikollisten toiminta ei ole hidastunut vaan päinvastoin monimutkaistunut sekä nopeutunut. Toisen ongelman verkkorikollisuuden ennaltaehkäisemiseksi on aiheuttanut tekoälyn kehittyminen. Tekoäly antaa verkkorikollisille hyvän alustan kehittää rikoksiaan ja toimia yhä enemmän järjestäytyneesti aiheuttaen suurempia vahinkoja.

Tulevaisuudessa tulisi keskittyä resurssien lisäämiseen ja yhteiskunnan kouluttamiseen ilmiöön liittyen. Paremmat mahdollisuudet tutustua verkkorikollisuuteen ja yritysten parempi panostus antavat heti suotavammat puitteet digiturvallisuuden parantamiseksi.

Asiasanat
Verkkorikollisuus, yksityisyyden suoja, digitalisaatio, teknologia, kyberturvallisuus

Sisällys

1 Johdanto

Verkkorikollisuus on kehittynyt huikean nopeasti viime vuosikymmeninä, ja se onkin yksi suurimmista uhista digitaalisessa ympäristössä. Yhteiskunnan digitalisaatio on antanut mahdollisuuksia niin innovaatiolle kuin myös rikolliselle toiminnalle, unohtamatta sen tuomia haasteita yksilölle ja yrityksille. Erilaiset verkkorikollisuuden muodot, kuten identiteettivarkaudet, tietomurrot ja palvelunestohyökkäykset ovat monimutkaistuneet ja yleistyneet, tehden niiden torjunnasta tai ennaltaehkäisemisestä vaikeampaa.

Ilmiön kasvu tuo mukanaan monenlaisia haasteita heikentäessä kansalaisten luottamusta yrityksiin ja niiden tarjoamiin digitaalisiin palveluihin. Yhteiskunnan hyödyntäessä suuresti verkkoympäristöä arkielämässään tuo tämä omat haasteensa palveluiden sujuvuuden ja tarjonnan jatkamiselle. Yksityisyyden suojan merkitys on myös kasvanut merkittävästi. Ihmiset ovat yhä tietoisempia sekä kiinnostuneempia omista oikeuksistaan ja omien henkilötietojen käsittely on herättänyt huolia. Yksityisyyden suojan ollessa yksi ihmisten perusoikeuksista, panostaa se yrityksiä yhä kasvavassa määrin keskittymään henkilötietojen turvalliseen ja vastuulliseen käsittelyyn.

Opinnäytetyön tarkoituksena on tutkia verkkorikollisuutta ja yksityisyyden suojaa omina kokonaisuuksinaan, sekä niiden vaikutuksista toisiinsa. Tavoitteena on nostaa lukijassa ajatuksia siitä, miten verkkorikollisuuden uhat ovat kasvaneet ja miten helppoa verkkorikollisuus on, ilman että tavallinen yksilö sitä huomaa. Verkkorikollisuuden uhriksi joutumisen riski on kasvanut yhä suuremmaksi ja opinnäytetyön toisena tarkoituksena onkin herättää lukijassa hieman huolta, mihin suuntaan verkkorikollisuus on menossa, ja nostaa jokaisen yksilön niin kuin myös yrityksen vastuuta henkilötietojen käsittelyssä yksityisyyden suojaan liittyen. Opinnäytetyön avulla halutaan myös herättää keskustelua verkkorikollisuuden ja yksityisyyden suojan välisestä suhteesta ja yleisesti luoda parempaa ymmärrystä siitä, kuinka kytköksissä yksityisyyden suojan turvaaminen on verkkorikollisuuteen.

Opinnäytetyön kohteena on verkkorikollisuus Suomen kannalta katsottaessa. Suomella valtiona on melko hyvät valmiudet verkkorikollisuuden torjuntaan ja siksi opinnäytetyö kohdistetaan yksilöille ja yrityksille. Viranomaisilla on Suomessa pystyssä omat strategiansa ja resurssinsa kyberturvallisuudesta huolehtimiselle, ja siksi tavoitteena on tutkia, miksi kohderyhmän kannalta verkkorikollisuus tuntuu olevan vain kasvusuuntainen ilmiö. Aihe on ajankohtainen jatkuvan uutisoinnin ansiosta, milloin uutisoidaan palvelunestohyökkäysten yrittämisestä ja milloin erilaisten huijausviestien kiertämisestä. Aihe on tärkeä, sillä se koskettaa jokaista ja on ensinnäkin vanhenevalle ja uudelle väestölle uusi konsepti digitalisaation jatkuvan kehityksen takia. Suomen kanta verkkorikollisuuteen kiinnostaa luonnollisesti enemmän, sillä Suomen tietoverkkoa ja digiympäristöä käyttäen uhat ovat erilaisia kuin ulkomailla. Suomen kantaa yhtyy myös

merkittävästi Pohjoismaiden ja jopa Euroopan kehitykseen ja tämän takia esimerkiksi Yhdysvaltojen ja Aasian rajaaminen pois tuntui luontevalta.

Opinnäytetyön johdantoa seuraa kappale, joka on katsaus verkkorikollisuuteen ja sen erilaisiin muotoihin. Osiossa tuodaan esiin erilaisia tilastoja ja tutkimustuloksia, jotka kuvaavat ilmiön laajuutta. Kappaleessa pohditaan myös hieman verkkorikollisuuden kasvun syytä ja katsotaan tarkemmin muutamaa Suomessa usein esiintyvää verkkorikollisuuden muotoa. Verkkorikollisuuden muodoista mainitaan muutamia yleisimpiä piirteitä sekä huomioita, miten varautua näihin.

Kolmannessa osiossa keskitytään yksinomaan yksityisyyden suojan käsitteeseen ja lainsäädäntöön, mukaan lukien esimerkiksi GDPR:n merkityksen ja sen soveltamisen Suomessa. Kappaleessa tarkastellaan Suomessa käytettävää lainsäädäntöä yksityisyyden suojaa ja henkilötietojen käsittelyä koskien. Osiossa käsitellään myös yksityisyyden suojan merkitystä sekä miten sen toteutuminen vaikuttaa yhteiskuntaan.

Neljännessä luvussa käsitellään verkkorikollisuuden vaikutuksia yksityisyyden suojaan; miten rikollisten toimet vaikuttavat yksilöiden kokemaan turvallisuuden tunteeseen ja digitaalisten palveluiden luottamiseen. Osiossa sivutaan myös identiteettivarkauksia, jotka kuuluvat verkkorikollisuuden muotoihin. Tarkemmin verkkoympäristöä hyödyntäviin rikoksiin, jotka rajautuvat opinnäytetyöstä pois. Verkkorikollisuuden yksi isoimpina haittavaikutuksina on ihmisten luottamuksen heikkeneminen niin viranomaisiin kuin digitaalisiin palveluihin, ja sen ehkäisemisen keinoja tutkitaan luvussa. Lukuun on myös haluttu nostaa esimerkki Vastaamon tapauksesta, jossa yksityisyyden suojaa rikottiin verkkorikollisuuden avulla, ja jonka seurauksista keskustellaan yhä tänä päivänä.

Verkkorikollisuuden ennaltaehkäisemiseksi ja vahinkojen lieventämiseksi on monia ratkaisuja ja niitä tutkitaan viidennessä luvussa. Teknologisten ratkaisujen kehittyminen ja lainsäädännön rooli ovat tärkeässä asemassa, kun halutaan rakentaa yhteiskunnasta digiturvallinen yhteisö. Organisaatioilla on myös suuri vastuu kyberturvallisuuden kehittämisestä ja parantamisesta, ja sen syvyyttä tutkitaan kappaleessa.

Kuudennessa luvussa tutkitaan verkkorikollisuuteen liittyviä kehityssuuntia ja miltä tulevaisuus näyttää edelleen digitalisoituvassa maailmassa. Osio keskittyy suuresti teknologian tuomiin uusiin haasteisiin kuten tekoälyyn, joka uusien tuulien puhaltaessa nostaa uusia haasteita ja ratkaisuja vanhoihin ongelmiin ja kysymyksiin.

Lopuksi kootaan yhteen tutkimuksen aikana selvinneet seikat verkkorikollisuuden merkitykseen Suomessa, ja minkälaisia vaikutuksia sillä on kehittyvässä yhteiskunnassamme niin yksilöiden kuin

yritysten kannalta. Luvussa pohditaan ratkaisuja ja keinoja, millä rakentaa huomisesta digiturvallisempi päivä yksityisyyden suojan kannalta.

2 Verkkorikollisuuden määritelmä ja kehitys

Verkkorikollisuus, usein käytetty myös termiä kyberrikollisuus, pääosin jaetaan kahteen kategoriaan. Tietoverkkosidonnaisiin rikoksiin, joita esiintyy ainoastaan tietojärjestelmissä tai tietoverkoissa, joissa rikos kohdistuu tietoverkkoon, -järjestelmään ja sieltä löytyvään dataan. Nämä rikokset suoritetaan tietokoneita tai tietoverkkoja käyttäen. Sekä rikoksiin, jotka tapahtuvat tietoverkkoavusteisesti, eli tietoverkkoympäristöä hyödyntäen, esimerkiksi petokset, rahapesu tai huumausainerikollisuus (Poliisi 2024). Verkkoalustat kuten Darknett ja Deepweb ovat rikollisten suosimia alustoja, joita käytetään pääosin rikollisuuden markkina- ja kohtauspaikkoina. Nykypäivänä yhä suurempi osa poliiseille ratkaistaviksi tulleista rikosilmoituksista onkin tehty tietoverkkoympäristössä tai sitä hyödyntäen. (Sisäministeriö 2017, 10-11)

Suomen laissa verkkorikollisuutta on avattu Rikoslain (39/1889) 38 luvun muutamassa pykälässä. Lain mukaan 5 pykälästä eteenpäin tuomittavia verkkorikollisuuden muotoja ovat esimerkiksi tietoliikenteen häirintä, törkeä ja lievä tietoliikenteen häirintä, tietojärjestelmän häirintä, törkeä tietojärjestelmän häirintä, tietomurto, törkeä tietomurto, tietosuojarikos, identiteettivarkaus sekä suojauksen purkujärjestelmärikos. (Rikoslaki 39/1889)

Nykypäivänä on jopa melkein todennäköisempää, että henkilö joutuu rikoksen uhriksi verkossa kuin reaalimaailmassa. Digitalisaation kehittymisen myötä, useammat laitteet ja lopulta koko yhteiskunta tulee olemaan riippuvainen verkkoympäristöstä. Verkkorikollisuus on kasvanut huimasti viimeisen kymmenen vuoden aikana eikä se terminä ole uusi. Verkkorikollisuus on ottanut muotoaan jo 1900-luvun lopussa. Vuosituhannen lopussa Internet alkoi yhdistämään ihmisiä eri viestintäverkkojen kautta maailmanlaajuisesti. Samaan aikaan kun tietoverkkoliikenne kehittyi, kehittyivät rikollisten keinot sekä tavoitteet. Teknologian alkuvaiheessa hyödynnettiin sen aikaisia heikkouksia, sekä turvallisuuden hallinnan puutetta – eihän siihen aikaan kyberturvallisuuskaan ollut mikään termi. Verkkorikollisuuden ensimmäiset rikokset tapahtuivat käyttäjien tunnistustietojen ja tietojenkalasteluhyökkäysten muodossa. Verkkorikollisuuden kasvava määrä osoitti rikollisten kehitystä ja mahdollisuutta päästä käsiksi järjestelmiin ja niiden manipulointiin. (Arctic Wolf 2024)

2.1 Verkkorikollisuuden eri muodot

Tietotekniikkarikoksia, eli rikoksia, jotka kohdistuvat tietotekniikkaan ja tietoverkkoihin on monia. Verkossa vietetyn ajan suuruus on kasvanut vuosien mittaa yhä suuremmaksi ja suuremmaksi, ja sen kautta nykypäivänä henkilö voi hoitaa melkein kaikki arkipäiväiset asiat verkossa. Tietomme voivat siis hyvinkin olla vain muutaman napautuksen päässä. Jos digitalisaatio kehittyy tätä tahtia, mikä estää verkkorikollisia kehittämästä omia strategioitaan? Verkkorikollisuudella ollen monia

muotoja, on välillä tavallisen henkilön vaikea pysyä perässä kaikesta siitä, mihin on varauduttava. Seuraavaksi kuvaillut muodot kuvaavat verkkorikollisuuden moninaisuutta ja sen jatkuvaa kehittymistä digitalisoituvassa maailmassa.

Tässä kappaleessa keskitytään pääosin tietoverkon kautta tapahtuviin rikoksiin. Verkkorikollisuutta, kuten nettikiusaamista ja verkkohäirintää, mobiilirikollisuutta tai taloudellisia verkkorikoksia kuten nettishoppailu huijauksia ei käsitellä. Nämä kaikki ovat verkkorikollisuuden muotoja, mutta opinnäytetyötä rajatessa keskitytään nyt ehkä siihen hieman vaikeampaan kokonaisuuteen, jossa ilmiselvät rikokset eivät ole esillä. Rajaukseen sisällytetään kuitenkin verkkorikollisuuden toiseen kategoriaan luokiteltavat identiteettivarkaudet, jotka ovat ajankohtainen aihe niiden suuren kasvun myötä.

2.1.1 Tietojenkalastelu

Tietojenkalastelu, englanniksi *phishing*, lukeutuu moniin huijauksiin, joita verkossa käytetään. Tietojenkalastelun tarkoituksena on henkilötietojen, kuten henkilö- ja pankkitunnusten varastaminen ja väärinkäyttäminen. Tietojenkalastelun voi myös jakaa eri osiin. Rikolliset yleensä lähettävät massaviestejä joko yksityishenkilöille tai organisaatioille. Sähköpostit räätälöidään kohderyhmälleen sopiviksi, jolloin huijausta on vaikeampi tunnistaa. Tekstiviestihuijaukset ovat varmasti monelle tuttu tietojenkalastelun muoto. Tekstiviestit voivat näyttää tulleen jokaiselle tunnetuista verkkopalveluista, hyödyntäen yritysten tietoja sekä viestien ulkoasua. Tekstiviestiketjuihin rikolliset pystyvät myös lisäämään omia haitallisia viestejä, jolloin huijauksen huomaaminen vaikeutuu entisestään. Viimeisenä muotona tietojenkalastelua voi esiintyä esimerkiksi huijauspuheluiden myötä. Puhelut noudattavat usein samaa kaavaa kuin tekstiviestit ja sähköpostit, jolloin rikolliset yrittävät uhria luovuttamaan mahdollisimman paljon tietoja, kuten eri tunnistautumistietoja. (F-Secure 2022a)

Huijausviesteiltä on vaikeaa täysin välttyä, joten on hyvä olla aina tarkkana viestejä tai puheluja vastaanottaessa, joissa pyydetään tunnistautumis- tai henkilötietoja. Harva organisaatio pyytää tunnuksia viestin välityksellä. Jos pankit tai viranomaisten pyytävät tietojasi viestin välityksellä, hälytyskellojen tulisi soida. Vaikka huijausviestit näyttävätkin usein todella aidoilta, on hyvä etsiä muutamia pieniä yksityiskohtia, joiden avulla selvittää onko viestit oikeasti huijausta vai ei. Usein huijausviesteissä pyydetään menemään linkin kautta täyttämään tietoja. Linkkejä ei tulisi ikinä avata, ja linkkien nimistä voi usein jo päätellä, että kyseessä saattaa olla huijaus. Linkit voivat olla kirjoitettu väärillä nimillä muistuttaen viranomaista, ja googlettamalla selviää hyvinkin nopeasti, että linkki ei välttämättä ole oikea ja sinne on esimerkiksi lisätty yksi piste tai ylimääräinen kirjain. Viestin lähettäjänä voi usein myös näyttää olevan ihan oikea viranomainen, mutta nimeen on voitu upottaa pieniä kirjoitusvirheitä. Tunnettu esimerkki tästä on Terveystalon nimellä tulleet

huijausviestit, jossa pieni L-kirjain olikin korvattu isolla i-kirjaimella. Tätä on miltei mahdotonta huomata, ellei ole jo tietoinen asiasta. Viesteissä kehotetaan myös usein toimimaan kiireellisesti ja se saattaakin sisältää hieman outoja lausahduksia, jos ajatellaan että kyseessä on kuitenkin jonkin tahon viranomainen. (Kuluttajaliitto 2024)

2.1.2 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat, tunnetaan englanniksi *Ransomware*, ovat haittaohjelmia, jotka salaavat käyttäjän tiedot. Rikolliset usein vaativat lunnaita uhreilta tietojen palauttamiseksi. Nämä tyypillisesti vaihtelevat 200 ja 500 euron välillä. Lunnaat tyypillisesti vaaditaan bitcoin kryptovaluuttana, jolloin rikollisten jäljittäminen on selkeästi vaikeampaa. Haittaohjelmat voidaan tietojenkalastelun tavoin jakaa kahteen osaan; kiristysohjelmiin, jotka lukitsevat laitteen, sekä kiristysohjelmiin, jotka salaavat laitteen tiedostoja tai tietoja. Kiristysohjelmat ladataan laitteelle yleensä uhrin toimesta vahingossa ja niiden levityskanavina käytetään usein haitallisia sivustoja tai mainoksia, suojaamattomia Wi-Fi-verkkoja sekä erilaisia sähköpostien liitteitä. (F-Secure 2022b)

Kiristyshaittaohjelman uhriksi joutumisen usein huomaa, kun joihinkin laitteessa oleviin tietoihin ei enää pääse. Haittaohjelma muuttaa myös tyypillisesti tiedostojen päätteet niille ominaiseen muotoon: .docx- ja .xlsx-päätteisten tiedostojen pääte muuttuu päätteeksi -.akira (Kyberturvallisuuskeskus 15.8.2024). Kiristyshaittaohjelmiin kuten muihinkin verkkorikollisuuden muotojen varautumiseen on hyvä aloittaa ajoissa. Varmuuskopiointi on yksi hyvä keino säilyttää itselle tärkeimmät tiedostot, oli ne sitten valokuvia lempireissusta tai sitten tärkeitä tiedostoja, vaikka töihin liittyen. Salasanojen vaihtaminen sekä ohjelmistojen päivittäminen ehkäisevät myös rikollista toimintaa sekä vähentävät riskiä joutua rikollisten kohteeksi.

2.1.3 Palvelunestohyökkäykset

Palvelunestohyökkäykset, Denial of Service DoS, ovat verkkojen kaatotarkoituksella tehtyjä hyökkäyksiä (F-Secure 2022c). Niiden tarkoituksena on estää verkkopalvelun tavallinen käyttö. Palvelunestohyökkäysten toimintamallina toimii liikenteen suurta kohdistamista johonkin tiettyyn verkkosivuun, jolla verkkosivun toimintaa pyritään häiritsemään (Poliisi 2024b). Tämän seurauksena verkkosivut toimivat hitaasti tai eivät toimi ollenkaan, ja pahimmassa tapauksessa se voi aiheuttaa vahinkoa palvelimiin ja niiden fyysisiin osiin. Palvelunestohyökkäyksissä lähteenä on yksi internettiin liitetty laite ja se voidaan suorittaa tarkoitukseen suunnitellulla ohjelmalla. Hajautettu palvelunestohyökkäys, Distributed Denial of Service DDoS, puolestaan tarkoittaa lukuisan laitteen osallistumista palvelunestohyökkäykseen, jolloin sitä on usein vaikeampi torjua tai jäljittää. (F-Secure 2022c)

Palvelunestohyökkäykset ovat kasvava uhka ja esimerkiksi Nordea on joutunut tämän vuoden aikana monien palvelunestohyökkäysten kohteeksi. Hyökkäysten aikana Nordean verkko- ja mobiilipankit sekä muut heidän tarjoamat palvelu eivät toimi tai ovat toimineet todella hitaasti. Palvelunestohyökkäykset eivät kuitenkaan tarkoita, että rikolliset olisivat päässeet käsiksi asiakkaiden pankkitietoihin vaan tavoitteena on yksinkertaisesti aiheuttaa haittaa. (Nordea 11.11.2024)

2.2 Kasvun syyt

Kuten aikaisemmin mainittu verkkorikollisuuden kasvu on monimutkainen ilmiö, johon vaikuttavat monet eri tekijät. Teknologian kehittyessä jatkuvasti ja digitaalisten palveluiden ja laitteiden yleistyminen on luonut myös uudet mahdollisuudet rikolliselle toiminnalle. Kehitys on muuttanut ihmisten tapaa työskennellä, kommunikoida ja asioida. Anonyymius on yksi merkittävimmistä syistä kasvulle. Verkkorikollisuus mahdollistaa rikollisen pysymisen anonyyminä, mikä siis madaltaa henkilön kynnystä rikolliselle toiminnalle. Tämä yhdistettynä taloudellisiin motiiveihin tekee verkkorikollisuudesta houkuttelevaa. (Sisäministeriö 2017)

Verkkorikollisia on usein vaikea saada kiinni, varsinkin kun kaikissa maissa sitä ei edes luokitella rikokseksi. Globalisaatio on myös tuonut omat haasteensa verkkorikollisten kiinni saamiselle. Rikolliset pystyvät hyödyntämään globaaleja verkkoja ja markkinoita, mikä tekee rikollisista toiminnoista entistä tuottavampia ja laajamittaisempia. Globalisaation ansiosta tietojärjestelmät ovat entistä enemmän yhteydessä toisiinsa, mikä lisää haavoittuvuuksia rikollisten hyökätessä useisiin eri järjestelmiin tai palveluihin yhdellä kertaa. (Cyber Security Intelligence 2021).

Sosiaalinen media antaa myös hyvän alustan verkkorikollisten toiminnalle. Sosiaalisen median eri alustoilla käyttäjät voivat jakaa huomaamattaan henkilökohtaisia tietojaan, kuten sähköpostiosoitteita tai sijaintietoja. Tämä tekee henkilöistä houkuttelevia kohteita rikollisille. Rikolliset voivat käyttää tietoja erilaisten petosten tekemiseen tai itse sosiaalista mediaa esimerkiksi huijausviestien lähettämiseen. Yksityisviestien avulla pyritään kalastelemaan rahansiirtoja tai henkilötietoja. Haitallisten liitteiden ja linkkien lähettäminen onnistuu myös sosiaalisessa mediassa helposti. Nykymaailman ollessa täynnä sisällön tekijöitä, voi huijausviestit näyttää myös houkuttavalta oman nimen kasvattamisen merkeissä tai esimerkiksi brändi diilien tekemisen kautta. (Kuluttajaliitto 2024)

Organisaatioiden voi myös olla vaikea pysyä kehityksessä mukana. Työntekijät eivät välttämättä panosta tarpeeksi tietoruvaan mikä tekee heistä helppoja uhreja. Monella saattaa olla ajatuksena, että koska itse ei ole ikinä joutunut uhriksi, ei todennäköisesti ikinä tule joutumaankaan. Tämä on ikävä yllätys sitten kun sen aika tulee. Organisaatioissa voidaan myös ajatella, että ei ole

yksittäisten työntekijöiden vastuu huolehtia tietoturvasta, vaan organisaatio itse hoitaa sen. Jokainen työntekijä voi kuitenkin tehdä osansa takakseen olevansa tietoruvan ajan tasalla. Koulutuksen puute on siis yksi organisaatioita ohjaavista heikkouksista. Työntekijät eivät välttämättä osaa arkistoida tietojaan oikein, jättävät sähköposteihin isot kasat vanhoja viestejä tai arkaluontoisia viestejä eivätkä täten ikinä käy niitä läpi. Sähköposteihin on onneksi asetettu monissa yrityksissä raja, jolloin sähköposti alkaakin herjaamaan tilan puutetta, jolloin työntekijän on pakko käydä tyhjentämässä sähköpostejaan. Toisena ongelmana voi olla myös se, etteivät työntekijät välttämättä ymmärrä, miten kaikki ohjelmistopäivitykset tukevat hyvän tietoturvan perustaa, jolloin ne ovat pakollisia hoitaa. Monien organisaatioiden käyttämissä ohjelmistoissa onkin onneksi mahdollista hylätä päivitykset vain muutamaan otteeseen, jonka jälkeen se alkaa päivittämään automaattisesti ilman käyttäjän hyväksyntää. Näin organisaatiot pyrkivät pienesti kuitenkin pysymään digiturvallisuuden turvaamisen tasalla. (Kyberturvallisuuskeskus 2023a)

Nämä tekijät ovat myötävaikuttaneet verkkorikollisuuden lisääntymiseen viime vuosina. Kasvun on ajateltu jatkavan kasvuaan ja sen kustannusten epäilty melkein tuplaantuvan vuoteen 2029 mennessä. Vuonna 2024 verkkorikollisuuden kustannukset ovat noin 9 miljoonassa USA:n dollarissa ja vuoteen 2029 mennessä kustannusten kasvun odotetaan saavuttavan jopa 15 miljoonaa dollaria. (Petrosyan, A. 2024)

2.3 Tilastot ja trendit

Vuosien mittaa verkkorikosten volyymi, intensiteetti sekä vahingon määrä on myös ollut kasvujohteista. Verkkorikollisten määrä on myös kasvanut vuosi vuodelta digitalisaation ansiosta. Tekoälyn kehitys on myös saanut verkkorikolliset kiinnostumaan sen antamista uusista mahdollisuuksista. Sen käyttö on jo nyt noussut esiin rikollisten käyttämissä työkaluissa. Huolestuttava trendi on myös verkkorikollisuuden kiinnostus nuorten keskuudessa. (Europol 2024, 6)

Vuonna 2023 palvelunestohyökkäykset, lasten seksuaalinen hyväksikäyttö sekä petokset olivat yleisimmät verkkorikollisuuden muodot EU:n sisällä (Europol 2024, 8). Suomessa syyskuussa on myös esiintynyt eniten palvelunestohyökkäyksiä sekä huijausviestejä (Kyberturvallisuuskeskus 10.10.2024, 6). Kyberturvallisuuskeskuksen tekemän kybersään mukaan kuluneen 12 kuukauden aikana selvästi eniten trendissä on ollut tietomurrot ja -vuodot, huijaukset sekä haittaohjelmat ja erilaiset haavoittuvuudet. Kesälomakuukausina huijausviesti olivat yksi eniten trendaavista verkkorikollisuuden muodoista. Omavero, Omakanta, suomi.fi ja PRH olivat yksiä suosituimmista huijausteemoina käytetyistä yrityksistä. (Kyberturvallisuuskeskus 10.10.2024) Rikolliset ovat toimineet niin yksin kuin ryhmässä niin Euroopan sisäpuolelta kuin ulkopuoleltakin.

Vuonna 2023 verkkorikollisuusfoorumit kuten Exploit, XSS ja BreachForum olivat rikollisten suosimia foorumeita. Sivustoilla verkkorikolliset jakavat neuvoja hakkerointiin liittyen, vaihtelevat varastettua dataa, hakkerointi työkaluja sekä erilaisia neuvoja aiheeseen liittyen. Verkkorikollisuuden pysäyttämiseksi luulisi, että verkkosivujen poistaminen tai alas ottaminen auttaisi. Toukokuussa 2023 yhden näistä verkkosivuista perustaja pidätettiin ja verkkosivusto onnistuttiin sulkemaan. Kuitenkin kolme kuukautta myöhemmin verkkosivusto nostettiin takaisin pystyyn hakkerointi ryhmän avulla. Lopulta sama sivusto kuitenkin otettiin alas internationaalissa LEA-operaatiossa. (Europol 2024, 15) Kaikilla foorumeilla voi löytää suuren kirjon erilaisia rikollisia. Foorumeja käytetään niin neuvojen jakamisen lisäksi markettipaikkoina esimerkiksi huumeiden myymisessä. Foorumeilla nähdään myös väärennettyjen henkilötodistusten myymistä, joilla voidaan avata erilaisia käyttötilejä tai taloudellisia palveluita verkossa. Foorumeilla on jo paljon palveluita, jotka auttavat rikollisia kehittämään kalastelu sähköposteja tai muita vastaavia viestejä. (Europol 2024)

Pienet ja keskikokoiset yritykset ovat jatkuvasti palvelunestohyökkäysten kohteena, niiden heikompien puolustuskeinojen takia. Pienemillä yrityksillä on vähemmän resursseja ja asiantuntevaa henkilöstöä kyberturvallisuuden hallintaan. (Kananoja, K. 2024)

Digi- ja väestöviraston toteuttaman Digiturvabarometrin tuloksien perusteella jopa joka viides suomalainen on joutunut verkkorikollisuuden kohteeksi. Valitettavasti vain puolet heistä on ilmoittanut rikoksesta poliisille. Tämä aiheuttaa selkeästi hieman hajontaa tilastoissa, sillä niissä ei voida ottaa huomioon ilmoittamatta jääneitä rikoksia. Rikosten ilmoittamisesta on myös trendi huomattavissa ehkä häpeän kautta. Moni suomalainen ei välttämättä usko itse joutuvansa verkkorikollisuuden uhriksi, ja kun se sitten käykin, voi henkilö tuntea jonkinlaista häpeää siitä, jonka seurauksena ei sitä välttämättä ilmoita poliisille. (Digi- ja väestötietovirasto 2023)

3 Yksityisyyden suoja

Yksityisyyden suoja on laaja käsite, joka pitää sisällään niin yksityisyyden suojan työelämässä kuin esimerkiksi viranomaistoiminnassa. Yksityisyyden suoja nähdään perusoikeutena ja se voidaan karkeasti määritellä henkilön oikeudella yksityiselämäänsä ja yksityisyyteensä erilaisessa tietojen käsittelyssä. Yksityisyyden suojaa käsitellään niin perustuslaissa kuin esimerkiksi EU:n perusoikeuskirjassa. Yksityisyyteen voidaan katsoa kuuluvan esimerkiksi yksilöivien tietojen suojan, kuten henkilötietojen tai paikkatietojen käsittelyn vain sallituissa tarkoituksissa, anonyymiyden sekä myös oikeuden toimia ilman julkisen vallan tuottamaa häiriötä. (Neuvonen 2014, 28-29)

Käsite yksityisyyden suojasta korostuu yhä enemmän digitalisoituneessa maailmassa, kun tietoja kerätään verkossa enemmän ja enemmän. Henkilötietojen suoja on osa yksityisyyden suojaa, ja kappaleessa keskitytäänkin sen näkökulmaan.

3.1 Lainsäädäntö ja säännökset

Suomen perustuslaissa (11.6.1999/731) yksityiselämän suoja on määrättynä yhtenä perusoikeutena. 10 pykälässä määrätään, miten jokaisen henkilön yksityiselämä, kotirauha ja kunnia on turvattu. Yksityiselämän suoja ei itse kerro mitään esimerkiksi henkilötietojen suojaamisesta, ja siitä määrätäänkin erikseen esimerkiksi tietosuojalaissa. (Perustuslaki 11.6.1999/731)

Suomessa oli pitkään voimassa henkilötietolaki (523/1999). Lain tarkoituksena oli toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia, kun kyseessä oli henkilötietojen käsitteleminen. Laki pyrki edistämään tietojenkäsittelytavan kehittämistä ja sen noudattamista. Laissa käsiteltiin henkilötietojen käsittelyä koskevia periaatteita, kuten huolellisuusvelvoitetta, henkilötietojen käsittelyn suunnittelua, arkaluontoisten tietojen käsittelykieltoja, henkilötunnusten käsittelyä aina vahingonkorvausvelvollisuuteen asti. (Henkilötietolaki 523/1999)

Henkilötietolaki kumottiin vuoden 2019 alussa voimaan tulleella tietosuojalailla (1050/2018). Tietosuojalailla täsmennetään ja täydennetään Euroopan parlamentin ja neuvoston yleistä tietosuoja-asetusta 2016/679 ja sen kansallista soveltamista. Tietosuojalaki siis määrittelee, miten henkilötietojen käsittelyä tulisi toteuttaa Suomessa. Tietosuojalaissa säädetään esimerkiksi henkilötunnusten käsittelemisestä, henkilötietojen käsittelemisestä akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoitusta varten, erityisten henkilötietoryhmien käsittelystä ja lapsiin

sovellettavasta ikärajasta tietoyhteiskunnan palveluita tarjottaessa (Tietosuojavaltuutetun toimisto s.a.).

Euroopan yleinen tietosuoja-asetus, GDPR, on hyväksytty vuonna 2016 ja sen sovellus tapahtui vuoden 2018 alkupuoliskolla. Asetuksen tarkoituksena on suojata yksityishenkilöitä, heidän tietojen ollessa käsittelyssä yksityisellä ja julkisella sektorilla. GDPR antaa vahvan suojan henkilötiedoille ja samalla asettaa tiukat vaatimukset niiden keräämiselle ja käsittelylle. Asetus myös auttaa yksilöitä hallitsemaan paremmin henkilötietojaan. Tämä halutaan toteuttaa helpommalla pääsyllä omiin tietoihin, uudella oikeudella siirtää tiedot järjestelmästä toiseen, selkeämmällä oikeudella tietojen poistamisesta sekä oikeudella saada tietoa henkilötietojen tietoturvaloukkauksesta. (Eur-Lex 2022)

Tietosuoja-asetuksessa pyritään myös tasapuoliseen toimintaedellytyksiin, joten asetukseen on myös listattu yrityksiä koskevia sääntöjä. Säännöillä halutaan pyrkiä innovaation edistämiseen useilla eri toimilla sekä sen avulla halutaan ottaa käyttöön teknologianeutraali lähestymistapa. Yrityksiä koskevissa säännöissä määrätään esimerkiksi tietosuojavastaavien nimeämisestä, yksityisyydensuojaa parantavista tekniikoista, tietojen kirjaamisesta sekä yritysten vastuusta tehdä tietosuojaa koskevia vaikutustenarviointeja. Määräysten avulla asetus haluaa vähentää yritysten byrokratiaa sekä halutaan yritysten hyötyvän kuluttajien suuremmasta luottamuksesta. (Eur-Lex 2022)

Suomessa on myös erikseen määrätty laki yksityisyyden suojasta työelämässä (18.8.2004/759). Lain tarkoituksena on siis yksityiselämän suojan ja sitä turvaavien perusoikeuden toteuttaminen työelämässä. Laissa määrätään esimerkiksi, miten työnantaja saa käsitellä vain työsuhteen kannalta tarpeellisia henkilötietoja, terveydentilaa koskevien tietojen käsittelystä, huumausaineiden käyttöä koskevien tietojen käsittelystä sekä esimerkiksi kameravalvontaa. (Laki yksityisyyden suojasta työelämässä 18.8.2004/759)

Suomen rikoslaki (19.2.1889/39) sisältää rikosten määritelmiä sekä niistä seuraavia oikeussäännöksiä (Oikeusministeriö s.a). Rikoslain 24 luvussa määrätään yksityisyyden suojan rikkomisesta. Luvun ensimmäisissä pykälissä mainitaan kotirauhan, viestintärauhan sekä julkisrauhan rikkomisesta. Luvun viidennessä pykälässä mainitaan ensimmäistä kertaa teknisen laitteen käyttö. Pykälässä mainitaan salakuuntelusta, jota teknisen laitteen avulla tehdään. Kuudennessa pykälässä mainitaan puolestaan teknisten laitteiden välillä toteutettu salakatselu, josta siirrytäänkin sitten yksityiselämää loukkaavan tiedon levittämiseen. Kunnian loukkaamisen voi myös sivuuttaa verkkorikoksista puhuttaessa, sillä sen voi myös tehdä hyödyntäen tietoverkkoja sekä teknisiä laitteita. (Rikoslaki 19.2.1889/39)

Rikoslain 38 luvussa tieto- ja viestintärikoksista katetaan myös yksityisyyden suojan osia. Tämä kohdistuu salassapitorikkomuksiin, joilla on vaikutusta yksityisyyden suojaan ja luottamukseen. Näiden tieto- ja viestintärikosten voidaan siis katosvan loukkaavan huomattavasti yksityisyyden suojaa. Yksityisyyden suojaa rikottaessa rangaistukset ovat yleensä vain sakkoa. (Rikoslaki 19.2.1889/39)

3.2 Yksityisyyden suojan merkitys

Yksityisyyden suojan merkitys on yksi keskeisimpiä asioita digitaalisen turvallisuuden kannalta. Oikeus yksityisyyteen myös verkossa on jokaiselle henkilölle tärkeää. Minkä tahansa yksilöivän tiedon laittaminen verkkoon, voi johtaa jossain vaiheessa verkkorikollisuuden uhriksi joutumista. Yksityisyyden suojan tarkoituksena on auttaa suojaamaan yksilöiviä henkilötietoja, joilla on riski päätyä vääriin käsiin. Henkilökohtainen turvallisuus yksityisyyden suojan kanssa voi siis vähentää erilaisten riskien tapahtumista verkossa. Riskien kirjo on laaja, ja ne voivat vaihdella identiteettivarkauksista taloudellisiin menetyksiin, syrjintään sekä henkilökohtaisiin psyykkisiin ongelmiin. Yksityisyyden suojan riskien ennakointi myös säästää aikaa ja vahinkoja, tietojen ollessa alttiina monenlaisille uhille. (European Data Protection Board s.a.)

Yritykset ovat myös suuressa osassa yksityisyyden suojan merkityksessä keräämällä henkilöistä tietoa erilaisten tiedonkeruutoimien avulla. Näitä tietoja yritykset voivat käyttää mainonnan suuntaamisella tai jopa vaikuttamalla henkilöiden käyttäytymiseen. Ihmisillä saattaa olla huolestuttavan vähän vaikutusta loppupeleissä siihen, mitä tietoja heistä kerätään ja mihin niitä käytetään. (Veritas 2024) Siksi yksityisyyden suojan hyödyntäminen omassa tekemisessään on tärkeää. Turha tietojen luovuttaminen ei välttämättä ole hyväksi ja harvoin liika tiedon luovuttaminen on loppupeleissä oikeasti hyödyllistä.

Yksityisyyden suojan toteutumisen merkitys on suuri. Onnistuneiden kokemusten ansiosta luottamus kasvaa digitaalisiin palveluihin ja yrityksiin (European Data Protection Board s.a.). Kun henkilöitä informoidaan hyvin mihin heidän tietojaan käytetään ja vahvistetaan kuvaa yksityisyyden suojasta, kasvaa henkilöiden halukkuus yrityksiä kohtaan. Tämän positiivisen kehityksen myötä myös digitaalinen innovaatio voi ottaa omaa sijaansa, kun henkilöt ovat avoimimpia uusille asioille ja projekteille. Yksityisyyden suojalla on merkitystä sen vaikuttaessa yhteiskunnassamme luottamukseen, hyvinvointiin sekä turvallisuuteen.

Digitaalinen turvallisuus vaikuttaa yksilön elämän eri alueisiin. Yksityisyyden suoja auttaa suojaamaan henkilökohtaisia tietoja, kuten puhelinnumeroa, osoitetta sekä taloustietoja, joilla on suuri riski päätyä väärinkäytön kohteeksi. Henkilökohtainen turvallisuus yksityisyyden suojassa voi siis vähentää identiteettivarkauksien ja muiden verkkorikosten riskiä. Yksityisyyden suoja liittyy

vahvasti tietoturvaan. Hyvin toteutettu yksityisyyden suoja auttaa estämään tietomurtoja ja sekä muita rikollista toimintaa. Yksityisyyden suoja auttaa myös estämään verkkokäyttäytymisen seurantaa. Ilman riittävää yksityisyyden suojaa käyttäjien verkkokäyttäytymistä voidaan seurata ja analysoida esimerkiksi kohdennettuihin mainoksiin tai jopa manipuloivin käytäntöihin. Näin ollen jokaisella vierailemallasi verkkosivulla annat käyttöoikeudet evästeisiin, eli siihen mitä tietoja verkkosivu voi sinusta vierailun ajan kerätä. Moni henkilö ei edes vaivaudu lukemaan näitä, ja voi esimerkiksi huonolla verkkosivulla erehtyä antamaan verkkosivulle oikeuksia, mihin ei välttämättä halua. (Veritas 2024)

4 Verkkorikollisuuden vaikutukset yksityisyyden suojaan

Kyberturvallisuudesta on tullut entistä tärkeämpi prioriteetti yrityksille ja hallituksille ympäri maailmaa. Verkko tarjoaakin alustan useille infrastruktuurin kriittisille aloille, kuten terveydenhuollolle, tieto- ja viestintätekniikalle, hallinnolle ja monelle muulle. Verkkoympäristö onkin joutunut yhä uudestaan ja uudestaan kohteeksi erilaisten verkkorikollisuuden uhkien alla. Sähköistä dataa käsitellään suuret määrät, erilaisten palveluiden ja laitteiden kautta, joka suurentaa huomattavasti riskiä joutua verkkorikosten uhriksi. Vaikka verkkorikollisuus onkin suuri haaste yhteiskuntaan ja yrityksiin on se kuitenkin haasteena myös yksityisyyden suojalle. Useita haasteita verkkorikollisuudelle luo esimerkiksi sen nopean ja monimutkaistunut kehitys. Yritysten pyrkiessä uhkien jatkuvan muutoksen ohessa muuttumaan ja kehittymään, kerätty data ja tieto voi huomaamatta jäädä kyberuhille alttiiksi. (Office of the Privacy Commissioner of Canada 2014)

4.1 Tietomurrot ja niiden seuraukset

Suomen rikoslain (1889/39 38) luvun 8 pykälässä määritellään tietomurrot tietojärjestelmään tunkeutumista käyttämällä henkilölle kuulumatonta käyttäjätunnusta tai muita murtamiskeinoja. Tietojärjestelmät tässä tapauksessa käsittelevät järjestelmiä, joissa sähköisesti käsitellään, varastoidaan tai siirretään tietoja tai dataa. (Rikoslaki 1889/ 38 luku 8 §) Tietomurto on rankaistava teko ja rikollinen voidaan myös tuomita törkeästä tietomurrosta sen ollessa erityisen suunnitelmallinen tai järjestäytyneen rikollisryhmän toimintaa, josta erikseen mainitaan rikoslain 6 luvun 5 pykälän 2 momentissa.

Poliisin verkkosivuilla tietomurtoa kuvaillaan yksinkertaisemmin oikeudettomalla tunkeutumisella tietojärjestelmään. Tietomurrot ovat laajoja ja vakavia rikoksia ja yleisimmin ne tehdään varastamalla kirjautumistiedot käyttäjältä. Turvajärjestelmien ohi tunkeutuminen on toinen rikollisten käyttämä taktiikka, jolloin tarkoituksena on hyödyntää järjestelmistä löytyviä tietoja. Näitä tietoja kerätään joko niiden arkaluontoisuuden vuoksi, esimerkiksi erilaiset yrityssalaisuudet, tai petosten tekemistarkoituksena. (Poliisi 2024a)

Tietomurrot ovat monimutkaisia ongelmia ja ne voivat aiheuttaa aikaa vieviä ja pitkäkestoisia vahinkoja sen uhrille. Tietomurtoja voi tapahtua niin yksityishenkilöille kuin organisaatioille. Tietomurtojen seurauksena erilaiset henkilötiedot, kuten nimet, syntymäajat, puhelinnumerot sekä salasanat vuotavat rikollisten käyttöön ja niitä hyödyntäen voivat käyttää tietoja petoksiin, luottotietojen saamiseen sekä muihin taloudellisiin hyötyihin. Organisaatioihin kohdistuvat tietomurrot voivat vahingoittaa niiden mainetta. Organisaatiot voivat myös kokea negatiivista painetta esimerkiksi lakipalkkioiden tai liiketoiminnan menetysten ja sakkojen muodossa. Tietomurtojen seurauksena organisaatiot voivat kohdata oikeudellisia toimenpiteitä, kuten

vahingonkorvauksia, jos tietosuojalainsäädäntöä on rikottu. Liiketoiminnan menetys voi esiintyä palveluiden tuottavuutena ja saatavuutena asiakkaiden luottamuksen heikkenemisen myötä. Täten yrityksen voivat kärsiä erilaisia taloudellisia tappioita. (Microsoft 2024)

4.2 Identiteettivarkaudet

Suomen rikoslain mukaan identiteettivarkaus on tuomittava rikos. Rikoslain 38 luvun 9 § mukaan tuomittavalla identiteettivarkaudella tarkoitetaan tekoa, jolla rikollinen pyrkii oikeudettomasti erehdyttämään kolmatta osapuolta käyttämällä toisen henkilötietoja, tunnistautumistietoja tai muita yksilöivää tietoa ja täten aiheuttaa kyseiselle henkilölle, kenen tietoja käytetään, taloudellista tai muuta haittaa ja vahinkoa. Laki on tullut Suomessa voimaan vasta 2015 ja tuomioksi identiteettivarkaudesta voi saada vain sakkoa.

Identiteettivarkaudet ovat yksi eniten kasvavista verkkorikollisuuden muodoista, mikä voi johtua sen helposta suorittamisesta nykypäivänä. Identiteettivarkaudet tapahtuvat yleensä esimerkiksi tietomurron yhteydessä, varastetusta tai kadonneesta henkilöllisyystodistuksesta. Sosiaalinen media on myös antanut yhden alustan lisää kalastella erilaisia yksilöiviä tietoja. Henkilötietoja sekä tunnistautumistietoja on myös todella helppo haavia esimerkiksi sähköpostien tai viestien välityksellä. Näiden huijausviestien kaava on usein sama, ja niissä pyydetään nopeaa toimintaa ja tiedot pitääkin mennä erillisen linkin kautta antamaan. Identiteettivarkauksilla usein tavoitellaan jonkinlaista taloudellista hyötyä, kuten asioiden ostamista tai rahan siirtoa ja nostoa. Rikolliset saattavat myös esiintyä verkossa väärällä identiteetillä ja aiheuttaen uhrille maineellista haittaa. (MySafety s.a.)

Suomessa yleisimpiä digiuhkia ovat erilaiset huijausviestit ja tietojenkalastelu. Digi- ja väestöviraston Digiturvabarometrin tutkimukseen vastanneiden mukaan suomalaisista miltei 80 prosenttia on saanut sähköpostitse erilaisia huijaus- tai kalasteluviestejä ja reilu 60 prosenttia tekstiviestitse (Digi- ja väestötietovirasto 2023). Digiturvabarometri kertoo siis, miten suomalaiset kokevat digitaalisen toimintaympäristön ja digitaalisen turvallisuuden tilan (Digi- ja väestövirasto s.a). Identiteettivarkaudet eivät ole kohdistuneet vain yksityishenkilöihin, mutta myös organisaatioihin. Rikolliset voivat yhtä lailla esiintyä myös organisaationa sosiaalisessa mediassa, aiheuttaen maineellista haittaa myös organisaatioille tavoitellessaan omia tavoitteitaan. Organisaatioiden identiteettivarkauksissa tavoitteena on usein pääsy yrityksen rahastoihin tai yritystietoihin, joita voi käyttää myöhemmin muiden rikosten tekemiseen (MySafety 2024)

Vaikka identiteettivarkauksista ilmoittaneiden määrä on kasvussa, on se edelleen huolestuttavan pieni. Digiturvabarometrin mukaan 60 prosenttia suomalaisista ei ilmoita viranomaisille huomattuaan identiteettivarkauden. Identiteettivarkaudet eivät välttämättä ole taloudellisesti

haitallisia, olisi niistä erittäin tärkeää ilmoittaa viranomaisille, jotta kehitystyötä voidaan tehdä niin rikollisten jäljittämisessä kuin identiteettivarkauden ennaltaehkäisemisessä. Suomalaiset ovat tällä hetkellä kuitenkin suhteellisen hyvällä mallilla identiteettivarkauden tiedotuksen kanssa, sillä vain kahdeksan prosenttia rikoksen ilmoittaneista eivät tiedä mistä identiteettivarkaudet ovat saaneet alkunsa. Vaikka tämä luku onkin hyvä ja suomalaiset näyttävät olevan jo hyvin informoituneita identiteettivarkauden keinojen suhteen, olisi tänä päivänä entistä tärkeämpää tiedottaa rikosilmoituksen tekemisen tärkeydestä. Tilastot eivät myöskään tämän takia anna sitä oikeaa kuvaa pienistä positiivisistakin luvuista kuten tietämättömyydestä. (MySafety 2022, 14-17)

Suojautuminen identiteettivarkauksilta onkin hyvä aloittaa jo varhaisessa vaiheessa. Internet on täynnä erilaisia neuvoja siitä, miten olisi hyvä suojautua ja mitä toimia tehdä. Näitä pieniä ja nopeita kikkoja noudattaessa ottaa jo hyvän askeleen oman identiteettinsä turvaamiseksi. Esimerkiksi F-Secure on julkaissut nettisivuillaan artikkelin *5 nopeaa ja helppoa tapaa välttää identiteettivarkaus* (engl. 5 quick and easy ways to avoid identity theft). Artikkelin ensimmäisenä ohjeena on asettaa sähköposti tietomurtoseurantaan, jolloin käyttäjä saa ilmoituksen, jos sähköposti on murrettu. Ilmoitus auttaa käyttäjää toimimaan nopeasti ja täten salasanan vaihto voi pysäyttää rikolliset jo alkuvaiheessa. Toista neuvoa, salasanan vaikeutta, ei voi olla kuulematta tai näkemättä, kun salasanoista puhutaan. Salasanat ovat siis helppo alku identiteettivarkauden torjumiseen. Monet haluavat päästä helpolla ja laittaa salasanaksi jotakin helposti muistettavaa ja itselleen tärkeää, tajuamatta kuinka helposti nämä salasanat voidaan murtaa. On siis erityisen tärkeää ottaa neuvosta vaari ja tehdä salasanasta erittäin uniikki. Salasanojen ajoittainen vaihtaminen on myös hyvä ehkäisykeino, mikäli käytössä ei ole tietomurtoseurantaa. Erilaisia neuvoja on kymmeniä alkaen salasanojen vaihtamisesta, linkkien spekulointiin aina VPN:n käyttöön julkisilla paikoilla asti. (F-Secure 14.12.2023)

4.3 Luottamuksen heikkeneminen

Luottamuksen heikkenemisellä viitataan asetteluun, jossa yksityishenkilöiden tai organisaatioiden usko toistensa kykyyn toimia vastuullisesti ja rehellisesti heikkenee (Mielenterveystalo.fi s.a.). Luottamus on erittäin tärkeä säilyttää, sillä loppupeleissä se voi vaikuttaa jopa taloudellisin haitoin. Luottamuksen heikkenemiseen vaikuttavat kaikki verkkorikollisuuden muodot. Tietomurrot sekä identiteettivarkaudet aiheuttavat turhaa pelkoa sekä epäluottamusta erilaisiin digitaalisiin palveluihin. Julkisuuteen tulleet tietovuodot, kuten seuraavassa kappaleessa käsiteltävä Vastaamon tapaus, aiheuttava suurta epäluottamusta organisaatioita kohtaa. Epäluottamusta voivat lisätä myös epäselvä tiedon käyttö, jolloin organisaatiot eivät välttämättä ole niin läpinäkyviä tietojen keräämiseen ja käyttöön liittyen.

Luottamuksen heikkeneminen vaikuttaa yksityishenkilön ja organisaation väliseen asiakassuhteeseen, joka voi johtaa esimerkiksi asiakkaiden menettämiseen. Asiakkaat voivat kuvitella toisen yrityksen hoitavan turvallisuuden toimenpiteet paremmin ja näin siirtyä kilpailijalle. Organisaation mainehaitta on toinen suuri negatiivinen vaikutus. Ääripäissä se voi johtaa jopa konkurssiin (Yle 2021). Myös sosiaalisen median suuren vaikutuksen ansiosta, sana leviää todella nopeaa ja yhtäkkiä negatiivista mainetta voi tulla monesta suunnasta, vaikka asia olisikin lähtenyt vain yhden asiakkaan tapauksesta. Luottamuksen heikkeneminen voi mainehaittojen lisäksi näkyä liikevaihdon pienenemisenä tai muina taloudellisina vahinkoina. Mainehaittoja on todella vaikea lähteä parantamaan, sillä mahdollisilla asiakkailla voi olla jo kuva organisaatiosta negatiivisella puolella. Tämä vaikuttaa myös asiakkaiden käyttäytymiseen. Asiakkaat voivat lopettaa palvelun käyttämisen kokonaan tai rajoittaa toimintaansa. Tämän tuloksena organisaatioiden toiminta rajoittuu asiakassuhteen käsittelyssä. (SIA Innovations s.a.)

Suomessa verkkorikollisuus on oletettavasti laskenut luottamusta, mutta suurin osa kuitenkin kokee osaavansa käyttää digilaitteita ja palveluita turvallisesti. Digiturvabarometrin mukaan 36 prosenttia tutkimukseen vastanneista kokee, että luottamus on heikentynyt. Luottamus on kuitenkin kokonaisuutena säilynyt hyvin, jos huomioidaan kuinka paljon esimerkiksi huijausyrityksiä suomalaiset ovat saaneet. Tutkimukseen vastanneista jopa 10 prosenttia toisessa kädessä arvioi luottamuksen parantuneen. Parantumisen syinä vastanneet ovat selittäneet tiedon runsauden ja riskien paremman tunnistamisen. Sosiaalinen media on myös osaltaan auttanut tiedon jakamisen kanssa ja täten auttanut uhkien tunnistamisen ajoissa. Suomalaisten osaamisen on myös arvioitu kasvaneen, jolloin he osaavat jo tunnistaa itse uhkat. Osaltaan on myös uuden teknologian kehitys saanut kehuja, uusien tunnistautumistapojen ja henkilötietojen käsittelyn tehostumisen myötä. (Digi- ja väestötietovirasto 2024)

Digiturvabarometriin vastanneiden kesken luottamuksen heikentymisen syinä pidetään erilaisia uhkia, kuten tietomurtoja ja huijauksia. Näiden lisääntyminen on aiheuttanut selitettävästi epävarmuutta ja niiden kehittyessä on niistä tullut vaikeampia tunnistaa sekä estää. Vaikka sosiaalinen media onkin lisännyt joillakin suomalaisilla luottamusta, on se antanut toiselle osalle käänteisen puolen. Uutisoinnin lisääntyessä ja luettaessa erilaisista tietomurroista, on turvallisuuden tunne heikentynyt osalla suomalaisista. Maailman tilanne sekä epäilyt Venäjän kyberhyökkäyksistä heikentävät myös luottamusta. Vastaajien kesken huolta on myös nostattanut epävarmuus siitä, miten organisaatiot käyttävät heidän tietojaan ja miten niitä käsitellään. (Digi- ja väestötietovirasto 2024)

Kyseinen ilmiö on vakava ongelma, ja se vaatiikin huomiota sekä yksilöiltä että organisaatioilta. Organisaatiot voivat osakseen parantaa asiakkaiden välistä luottamusta koskien esimerkiksi

heidän käyttämiään digipalveluita. Organisaatiot hyötyvät suuresti läpinäkyvästä toiminnastaan ollessa avoimia käytännöistään sekä tiedon käytöstään. Tätä arvostetaan suuresti asiakkaiden toimesta, varsinkin heidän kasvavan halun olla yhä tietoisempia tietojen käyttämisen prosesseista. Asiakkaiden arvostaessa yhä enemmän turvallisuutta, organisaatioiden olisi hyvä investoida tietoturvaan. Suojaamalla asiakkaiden tiedot, auttaa se parantamaan luottamusta. Monilla pienillä tai keskikokoisilla ei välttämättä ole resursseja tai asiantuntijuutta nostaa tietoturvan suojaamista ensimmäisiksi prioriteeteiksi, mutta siihen olisi syytä tehdä muutos.

4.4 Tapaus Vastaamo

Suomea tähän mennessä ehkä eniten kuohauttanut ja laajimmin uutisoitu verkkorikollisuuteen liittyvä tapaus – Psykoterapiakeskus Vastaamon tietomurto. Vuoden 2018 lopulta vuoden 2019 maaliskuun välillä tapahtunut tietomurto vaikutti yli 30 000 tuhannen ihmisen tietoihin (Rimpiläinen, T. 26.10.2020). Tapaus saavutti myös huomiota maailmanlaajuisesti uutisartikkeleiden muodossa esimerkiksi yhdysvaltalaisen tietokonekulttuuria käsittelevässä Wired -aikakausilehdessä sekä Britannian yleisradioyhtiön nettisivuilla BBC:llä. Tapaus on ollut niin laaja, että jopa Valtiokonttori, joka myöntää rikoksen uhreille korvauksia rikosvahinkolain mukaan, on tehnyt verkkosivuilleen oman välilehden otsikolla *Vastaamon uhrit* (Valtiokonttori 2024). Tapauksesta poikkeuksellisen teki myös se, ettei aikaisemmin ole yksityishenkilöiden terveystiedot olleet ensimmäisenä kohteena verkkorikollisille, vaan ensisijaisesti on pyritty vaikuttamaan verkkopankkien tai maksujärjestelmien toimintaan ja tietoihin (Valtanen, T. & Harjumaa, M. 24.10.2020).

Psykoterapiakeskuksen tietomurrossa tunkeuduttiin organisaation sisäisiin järjestelmiin ja sen työntekijöiden ja potilaiden tietoja varastettiin. Tietoja, mitä tietomurrossa varastettiin, oli muun muassa osoitteita, yhteystietoja, henkilötunnuksia, potilastietoja, sekä muita potilaita yksilöiviä tietoja. Varastetut tiedot sisälsivät harmillisesti myös terapiamuistiinpanoja sekä erilaisia diagnooseja. Vastaamon tapauksessa tietoihin päästiin käsiksi organisaation IT-järjestelmissä olleen tietoturvavirheen kautta. Rikoksen tekijän tarkoituksena oli alun perin kiristää Vastaamolta lunnaiden muodossa, ja myöhemmin lunnaiden kiristäminen keskittyikin potilainen kohdistamiseen. Jos lunnaiden maksamista ei tapahtunut, oli kiristäjä päättänyt vuotaa potilastietoja julkisuuteen. (Ralston, W. 9.12.2020)

Vastaamon tietomurto tuli julki vasta vuoden 2020 lopusta, mikä on ollut organisaation puolelta huolestuttava seikka. Asiakkaita, eikä viranomaisia ei oltu tiedotettu tarpeeksi ajoissa, eikä vahinkojen minimoimiseen voitu panostaa. Vastaamon entinen toimitusjohtaja tuomittiinkin tietosuojarikoksesta viimevuoden huhtikuussa kolmen kuukauden ehdolliseen vankeusrangaistukseen. Toimitusjohtaja ei toteuttanut yleisen tietosuoja-asetuksen määrittelemiä toimenpiteitä uhrien henkilötietojen salauksesta tai niiden pseudonymisoinnista, eli henkilötietojen

käsittelemistä ilman että niitä voi yhdistää tiettyyn henkilöön ilman lisätietoja. (Salumäki, T. 19.5.2020)

Tapauksen ainoana ongelmakohtana ei ollut organisaation toimitusjohtajan toiminta, mutta myös Psykoterapiakeskuksen it-järjestelmistä vastanneet työntekijät. Kolme Vastaamolla työskennellyttä henkilöä olivat olleet aikaisemmin pidätettynä epäiltynä törkeästä petoksesta ja viestintäsalaisuuden loukkauksesta. Kyseessä oli vuonna 2015 tapahtunut Tekesin tietomurto. Vastaamon tapauksessa miehet olivat työskennelleet järjestelmäarkkitehteinä ja tietomurron tapahtuessa salanneet asian toimitusjohtajan pyynnöstä. (Kärkkäinen, H. 6.5.2021)

Tapauksesta tuomittu Aleksanteri Kivimäki saatiin kiinni Ranskassa helmikuussa 2023 ja luovutettiin nopeasti takaisin Suomeen (Mannermaa, J. & Salumäki, T. 2.8.2023). Käräjäoikeuden mukaan Kivimäki syyllistyi törkeään tietomurtoon, törkeään kiristykseen ja sen yritykseen sekä törkeään yksityiselämää loukkaavan tiedon levittämiseen. Kivimäki sai käräjäoikeuden puolesta kuuden vuoden ja kolmen kuukauden vankeusrangaistuksen. Tuomio oli lievempi, mitä syyttäjä vaati, seitsemän vuoden rangaistusta, mutta Kivimäen tekoja pidettiin kuitenkin vakavina ja hänen suhtautumistaan asiaan piittaamattomana. Lievenemisen yhtenä syynä katsottiin olevan Kivimäen sopimista ehdollisiin sovintoihin korvausvaatimuksia esittäneiden asianomistajien kanssa. (Lapinkangas, J. 30.4.2024)

Tapaus on harmillisesti erinomainen esimerkki siitä, miten organisaation ei tule toimia tietomurron tapahtuessa tai sitä epäiltäessä. Tapaus on aiheuttanut uhreille niin taloudellista kuin henkistä haittaa. Vastaamo kärsi tapauksessa huomattavasti niin asiakkaiden luottamuksesta kuin taloudellisesti. Psykoterapiakeskus asetettiinkin vuonna 2021 konkurssiin (Yle 2021). Vastaamon tietomurto on ollut Suomen rikoshistorian suurin uhrimäärän vaatinut tapaus (Rautio, M. & Paukkeri, M. 26.4.2023).

Rikosilmoituksen tekemisen tärkeys korostuu myös tässä tapauksessa. Tietomurron uhrien määrä on noin 33 000 henkilöä ja heistä noin 24 000 on tehnyt asiasta rikosilmoituksen. Valtionkonttorin lisäksi uhreille apua ja neuvoja voi saada myös Rikosuhripäivystyksestä. (Rautio, M. & Paukkeri, M. 26.4.2023)

5 Välineet ja käytännöt yksityisyyden suojaamiseksi

Suomella on verkkorikollisuuden torjumiseksi kehitettynä kyberturvallisuusstrategia. Valtioneuvoston kanslia on julkaissut lokakuussa strategian, joka ulottuu tästä vuodesta vuoteen 2035 asti. Kyberturvallisuusstrategian tarkoituksena on vastata teknologiseen kehitykseen ja muuttuneeseen geopoliittiseen tilanteeseen. Kyberturvallisuusstrategiassa käsitellään kyberturvallisuutta erityisesti kansalliselta puolelta. Tämä puoli kattaa toimia, joiden avulla yhteiskunta pystyy tunnistamaan, varautumaan, torjumaan sekä kestämään verkkorikollisuuden uhkia sekä niiden vaikutuksia yhteiskunnan elintärkeisiin toimintoihin ja palveluihin. Vaikka strategia ulottuukin kymmenen vuoden päähän, on sitä digitalisaation kehittyessä myös tarvittaessa kehitettävä sekä pidettävänä ajantasaisena. (Valtioneuvoston kanslia 2024)

Vaikka kyberturvallisuusstrategian mukaan Suomeen kohdistuva vihamielinen kybertoiminnan lisääntyminen on todennäköistä, on Suomi kuitenkin saavuttanut International Telecommunication Unionin (ITU) kyberturvallisuusindeksissä 100 pistettä, mikä on korkein mahdollinen määrä. Vertailussa sata pistettä sijoittuu ensimmäiselle tasolle, joka on varattu kaikille esikuvana toimiville maille (Europol 2024). Tämä pitää sisällään maiden osoittamaa vahvaa sitoutumista kaikkiin indeksissä verrattuihin kyberturvallisuuden viiteen osa-alueeseen. Osa-alueet ovat kuvaavat maiden sitoutumista kyberturvallisuuteen oikeudellisesta, organisatorisesta, teknisestä, valmiuksien kehittämisestä ja yhteistyöllisestä kulmasta. Suomen lisäksi Euroopan maista 19 muuta on myös sijoitettu ensimmäiselle tasolle. Kokonaisuutena Eurooppa on siis pärjännyt hyvin indeksin mittauksissa. (Kyberturvallisuuskeskus 20.9.2024)

Suomessa Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palvelujen toimintavarmuutta ja turvallisuutta. Kyberturvallisuuskeskus muodostaa kyberturvallisuustilannekuvan ja kokoaa riskianalyysejä eri hallinnonalojen ja toimijoiden kanssa. Kyberturvallisuuskeskuksen tavoitteena on yhteistyön tehostaminen ja osaamisen kehittämisen tukeminen esimerkiksi kyberhäiriötilanteiden hallinnassa. (Kyberturvallisuuskeskus 2024)

5.1 Teknologiset ratkaisut

Vaikka verkkorikollisuus kehittyykin jatkuvasti ja välillä tuntuukin, ettei mikään voi rikollisia pysäyttää, on kuitenkin joitakin teknologisia ratkaisuja verkkorikollisuuden torjumiseen. Erilaisilla teknologisia ratkaisuja voi hyödyntää oman yksityisyyden suojan takaamiseksi ja itseen kohdistuvan verkkorikollisuuden ennaltaehkäisemiseksi. Jos verkkorikolliset käyttävät verkkoympäristöä hyväkseen, miksi emme myös hyödyntäisi alustaa rikollisuuden ennaltaehkäisemiseen.

Ensimmäinen ja ehkä helpoin tapa aloittaa omien tietojen suojaaminen on ottamalla käyttöön salasanan hallintaohjelma. Sovelluksen avulla voit säilyttää salasanat, joita käytät erilaisissa palveluissa, yhdessä paikassa. Salasanojen tärkeys on korostunut päivä päivältä yhä enemmän ja siksi olisikin tärkeää, ettei samoja salasanoja käyttäisi monessa paikassa. Tällöin murtautuminen käyttäjätileihin tulee entistä helpommaksi. Useita ja monimutkaisia salasanoja on varmasti vaikea muistaa, ja siksi salasananhallintaohjelmat ovatkin hyvä ja nopea apu. Esimerkiksi Applella on mobiilipuhelimissaan käytössä ”salasana” -palvelu, jonne voit melkein huoletta tallentaa kaikki käyttäjien salasanat. Palvelu myös auttaa vaikeasti murrettavien salasanojen keksimisessä. Salasanaohjelmissa on myös yksi erittäin hyvä apu. Ne voivat auttaa tunnistamaan erilaisia kalasteluyrityksiä. Yleensä sovellukset ehdottavat verkkosivulla tallennettua salasanaa, ja jos vaikka meneekin sähköpostiin tulleen linkin kautta verkkosivulle. Kun verkkosivulle yrittääkin kirjautua ja sovellus ei ehdota tallennettua salasanaa voi kyseessä olla huijaus sivusto ja tietojen kalasteluyritys. (Kyberturvallisuuskeskus 30.7.2020)

Vahva salasana voi tuoda lisää turvaa, ei se aina ole ehto sille, ettei joudu verkkorikollisten uhriksi. Kaksivaiheinen tunnistautuminen suojaa vielä enemmän käyttäjätilejäsi, tekemällä sinne murtautumisesta vielä vaikeampaa. Kaksivaiheinen tunnistautuminen vaatii salasanan ja käyttäjätunnuksen lisäksi jotakin muuta vaihtoehtoista tunnistautumista. Tämä voidaan tehdä esimerkiksi tekstiviestillä lähetettävän koodin tai turvakysymyksen avulla. Monet yritykset ovatkin ottaneet jo verkkopalveluissaan käyttöön kaksivaiheisen tunnistautumisen ja olisikin hyvä, että käyttäjät ottaisivat ne käyttöön. Kaksivaiheisen tunnistautumisen avulla käyttäjille murtautuminen vaikenee ja tunnistautuminen suojaa käyttäjien yksityisyyttä. (F-Secure 28.10.2023)

Organisaatiot voivat puolestaan ottaa käyttöönsä Traficomin kautta haettavaa SMS Sender ID-tunnusta. Tämän avulla yritys voi varmistua siitä, ettei kukaan muu käytä samaa lähettäjä tunnistetta tekstiviestejä lähettäessä. Traficomin sivuilta voi myös löytää tällä hetkellä rekisteröidyt SMS Sender ID -tunnukset, joita kuka tahansa voi mennä katsomaan. Tämä auttaa yksityishenkilöitä epäillessä huijausviestiyrityksiä. Kaikkia mutkia ei kuitenkaan lista suorista, sillä toisessa luvussa mainittu Terveystalon tapaus on esimerkki. Terveystalohan löytyy siis itse tältä SMS Sender ID -tunnus listalta, mutta verkkorikolliset ovat kuitenkin keksineet keinot tämän kiertämiseksi. (Traficom 2024)

5.2 Lainsäädännön rooli

Lainsäädännöllä on tärkeä rooli yksityisyyden suojaamisessa sekä verkkorikollisuuden torjunnassa. Koska verkkorikollisuus on ollut pinnalla niin Suomessa kuin muuallakin Eurooppaa on kyberturvallisuusvelvoitteiden tiukentaminen ollut ajankohtainen aihe Euroopan parlamentissa. Euroopan parlamentti hyväksyi uuden kyberturvallisuusdirektiivin NIS2-direktiivin kaksi vuotta

sitten 2022. Tämä korvasi edellisen verkko- ja tietoturvadirektiivin NIS1-direktiivin, joka hyväksyttiin 2016. (Valtioneuvosto 2024a) NIS2-direktiivin merkittävämpänä tavoitteena on Euroopan parlamentin mukaan varmistaa yhteinen kyberturvallisuuden taso läpi Euroopan Unionin. NIS-direktiivi säätää erilaisista tietoturvavelvollisuuksista ja häiriöraportoinnista. NIS2-direktiivi asettaa toimijoille riskienhallinnan toimenpiteet, joilla ehkäistään kyberturvallisuutta. (Kyberturvallisuuskeskus s.a. a)

NIS2-direktiicillä tavoitellaan oikeudellisen kehityksen nykyaikaistamista, jotta digitalisaation turvallista kehittymistä voidaan jatkaa. Kyberturvallisuussääntöjen soveltamisalaa laajennettiin uusiin aloihin ja toimijoihin tavoitteena parantaa yksityisten ja julkisten tahojen, toimivaltaisten viranomaisten sekä koko Euroopan Unionin reagointivalmiuksia ja häiriönsietokykyä. Direktiivi edellyttää, että jokaisella jäsenvaltiolla on asianmukaiset varusteet kyberturvallisuuden varmistamiseksi. Direktiivi myös edellyttää jäsenvaltioiden välistä yhteistyötä, tukemalla ja helpottamalla tietojenvaihtoa. (Euroopan komissio 2023)

Hanke NIS2-direktiivin saattamisesta osaksi kansallista lainsäädäntöä astui voimaan Suomessa lokakuussa 2024. Hankkeella tavoiteltiin NIS2-direktiivin vähimmäistason mukaisia kyberturvallisuuden riskienhallinta- ja raportointivaatimusten toteutumista soveltamisalan kuuluville toimijoille. Esityksellä halutaan Suomessa parantaa samalla tavalla kyberturvallisuuden tasoa. (Valtioneuvoston kanslia 2024)

Aikaisempi NIS1-laki ei ole parantanut riittävästi kyberturvallisuutta, joten aikaisempaa tiukempi NIS2-laki tarvittiin käyttöön. Tiukempi laki pakottaa sakon uhalla jäsenmaita parantamaan kyberturvallisuuden tasoja esimerkiksi ottamalla käyttöön kyberturvaan liittyviä suojamuureja. Euroopan Unioni on kokenut, ettei aikaisempi laki ole antanut jäsenmaille tarpeeksi ”potkua” kyberturvallisuuden parantamiseksi, ja täten tiukempi laki on oltu miltei pakko ottaa käyttöön, jotta verkkorikollisuudelta voidaan välttyä jossakin määrin. (LähiTapiola 2024)

5.3 Organisaatioiden vastuullisuus

Kuten tähän mennessä on painotettu, organisaatioiden vastuu verkkorikollisuuteen liittyvissä toimissa jatkaa kasvuaan. Verkkorikollisuuden kasvu ja etenkin viime vuosien huomiota herättäneet tapahtumat, kuten juurikin Vastaamon tietomurto, ovat nostaneet organisaatioiden vastuullisuuden tärkeyttä. Verkkorikollisuuden eri muodot voivat aiheuttaa suuria vahinkoja yksityishenkilöille kuin myös organisaatioille, jonka takia riittäviä ehkäiseviä toimenpiteitä on tärkeää harjoittaa jo prosessien varhaisissa vaiheissa tietojen arkistointiin asti. Organisaatioilla on lakien ja säännösten lisäksi myös vastuu käyttäjien eli asiakkaiden riittävästä tiedottamisesta. Luottamuksen rakentaminen ja sen jatkuva vahvistaminen ovat siis perusteellinen osa

organisaatioiden toimintaa. Antamalla käyttäjille mahdollisuuden muokata, poistaa ja tarkistaa omia tietojaan, voivat organisaatiot lisätä luottamusta ja kontrollia käyttäjien välillä. Tämä myös kattaa käyttäjille helpon pääsyn sekä ymmärrettävät vaihtoehdot yksityisyysasetusten hallintaan. (Kyberturvallisuuskeskus 26.2.2024)

Fortumin yhteiskuntasuhteiden johtaja ja hallituksen jäsen Arto Räty kertoo Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen vuosittaisessa tietoturvaseminaarissa, ettei organisaatioiden johdossa välttämättä ole tarpeeksi kokemusta verkkorikollisuuteen liittyvissä turvallisuusasioissa, jonka seurauksena organisaatioiden johto ei välttämättä osaa reagoida tarpeeksi ajoissa tai riittävin toimin. Rädyn mukaan organisaatioiden olisi hyvä panostaa toimiviin prosesseihin, joka olisi osanaan auttamassa kyberturvallisuuden pulan voittamisessa. Riittävien resurssien sekä tehokkaan raportoinnin avulla, voidaan kyberturvallisuuden tehostamista aloitella. (Kyberturvallisuuskeskus 2020)

Organisaatiot voivat käyttää tukenaan Kyberturvallisuuskeskuksen luomaa Kybermittaria, joka antaa hyvät työkalut kyberturvallisuuden arviointiin ja sen kehittämiseen organisaation sisällä sekä toiminnassa. (Kyberturvallisuuskeskus s.a. b)

Vaikka vastuu pelkästä yksityisyyden suojaamisen ennakoinnista on suuri, on organisaatioilla myös vastuu ilmoittaa mahdollisista tietoturvaloukkauksista, jos niiden arvioidaan aiheuttavan haittaa tietovuodon kohteelle. Tietovuotojen ilmoittaminen perustuu usein lakiin, ja siksi niistä ilmoittaminen onkin tärkeää organisaation ja asiakkaiden kannalta. Vaikka organisaatio ei olisi varma täytyykö ilmoitusta tehdä, on se kuitenkin hyvä varotoimi, jos tietoja onkin vuotanut. Eri viranomaiset pystyvät tapauksesta riippumatta ryhtyä selvittämään onko vuodosta aiheutunut vahinkoja. (Suomi.fi 2024)

6 Kehityssuunnat ja tulevaisuuden näkymät

Siinä missä verkkorikollisuus tuntuu kasvavan ja rikosten taitojen karttuvan on myös yritysten tietoisuuden sekä toiminnan tarkoituksellisuuden kasvettava. Pääsääntöisesti valtiot ovat lähivuosina ottaneet enemmän askelia kyberturvallisuuden takaamisen eteen. Tulevaisuuden verkkorikollisuuden uhkat tulevat kuitenkin pysymään suhteellisen samoina mitä ne tänä päivinäkin ovat. Vaikka rikollisten keinot tehdä rikoksia verkossa kehittyy, eivät rikosten tyypit välttämättä muutu. Vuosien päästä tullaan varmasti tekemään samoja palvelunestohyökkäyksiä tai identiteettivarkauksia kuin nykypäivänä. On siis tärkeää, että jokainen, oli sitten yksittäinen henkilö tai organisaatio, alkaa katsomaan verkkorikoksia oikeina uhkina ja ryhtyy tekemään erilaisia toimenpiteitä, joilla rikollisuutta voidaan ehkäistä tai jopa lieventää sen aiheuttamia vahinkoja. (Enisa 2022)

Verkkorikollisuuden täydelliseksi torjumiseksi tarvitsemme kuitenkin resursseja. Tämän hetken resurssit kyberturvallisuuden takaamiseksi ovat olleet eri toimialoilla kuitenkin riittämättömiä. Kehityksen positiivista jatkua varten olisi siis erityisen tärkeää keskittyä uuteen resursointiin. Suomi käyttääkin tällä hetkellä melkein 300 miljoonaa euroa valtiohallinnon kyberturvallisuuden varmistamiseen. Kyberosaamiseen kuitenkin panostetaan Suomessa koulutusasteilla ja erilaisissa tutkimushankkeissa. Kyberturvallisuuden kehittämisen mahdollisuuksiin kuitenkin vaikuttaa suuresti työvoimapula, teknologinen korjausvelka sekä EU:n lisääntyvä sääntely. Työvoimapula johtuu tällä hetkellä kyberturvallisuusalan osaamisvajeesta. Ala ei välttämättä tarjoa erittäin houkuttelevia työllistymismahdollisuuksia juurikin näiden resurssien puutteen vuoksi. Pienemmillä tai keskikokoisilla yrityksillä ei siis välttämättä ole resursseja kehittää omia kyberturvallisuuden tiimejään. (Valtioneuvoston kanslia 2024, 40)

Suuret taloudelliset investoinnit koko yhteiskunnan tasolla ovat tällä hetkellä avain toimivan kyberturvallisuuden pohjalle. Tämä lisää alan työpaikkoja sekä tuottaa kasvua kuin myös parantaa osaamista ja digitaalisen yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristön haitallisia alueita vastaan. Keskeisiä keinoja kyberturvallisen ja -kriisinkestävän yhteiskunnan säilyttämiseksi ovat korkeatasoinen tutkimus- ja kehitystoiminta, joka keskittyy murrosteknologioihin. Suomen kyberturvallisuuden kehittämisen keskeisiä kehityksen suuntia ovat EU:n kehittämisrahoituksen ja Naton innovaatiorahoituksen hyödyntäminen. Vastaisuudessaan tämä vaatii Suomelta vastinrahaa ja hallinnonalojen välistä resurssien käytön koordinointia. Suomen liityttyä Natoon, vaatii se toisenlaista suorituskykyä ja resursseja liittolaisten tukemiseksi, sekä lisäpanostusta kyberturvallisuuteen ja -puolustukseen. (Valtioneuvoston kanslia 2024, 41)

6.1 Teknologian kehitys ja uudet haasteet

Tekoälytyökalujen ja -palveluiden laajempi käyttöönotto verkkorikollisten keskuudessa on luonut uusia uhkia, joihin voi liittyä niin laillisten työkalujen ja palveluiden väärinkäyttöä kuin niiden haitallisia versioita, joita rikolliset ovat luoneet tilapäisesti. Tekoälyn luomat mainokset houkuttelevat mahdollisia uhreja ja aiheuttavat yhä lisää verkkorikoksia. Tekoälyä voi niin luomisen sijaan käyttää myös rikollisten menetelmien parantamiseksi. Tekoäly alentaa verkkorikollisuuden markkinoille pääsyn esteitä, mikä tarkoittaa sitä, että henkilöt kenellä on rajoitettu tekninen asiantuntemus, voivat suorittaa kyberhyökkäyksiä ja organisoida varsin kehittyneitä verkkopetosjärjestelmiä. Tekoälyn kanssa myös hajauttaminen sekä vertaisverkot luovat jatkossakin rikollisille uusia mahdollisuuksia, koska ne helpottavat huomattavasti suoriutumista anonyymisti ja poissa viranomaisten silmistä. (Europol 2024, 33-34)

Tekoälyn vahvuuksina on myös kielet. Tekoäly ja uudet työkalut tekevät kansainvälisestä rikollisuudesta entistä helpompaa, sillä kielten kääntäminen onnistuu minuuteissa. Tämä kasvattaa rikollisten aluetta ja kohteita, koska nyt ei alueet ole enää rajana näin ei ole myöskään kieli. Suomella on ollut turvanaan oma kielemme, jota ei maailmalla puhuta, mutta nyt tämäkin pieni vahvuus voi saada loppunsa. Tämä tekoälyn käyttö mahdollistaa myös useammalle taholle suunnatut hyökkäykset. (Second Nature Security 2023)

Tekoäly herättää edelleen hieman epäilyä ihmisten keskuudessa. Digiturvabarometrin tutkimukseen vastanneista vain 22 prosenttia luottaa melko/erittäin paljon siihen, että erilaiset tekoälypalvelut käsittelisivät tietoja turvallisesti. Kasvavassa määrin yhteiskunnan osalliset haluavat kuitenkin oppia lisää tekoälyn turvallisesta käytöstä, ja 62 prosenttia vastanneista haluavatkin lisää tietoa tekoälyn käyttämisestä. Tulos oli sama kaikissa ikäryhmissä, vaikka nuoret 18-24 vastasivatkin käyttävänsä tekoälyä kuukausittain tai useammin. (Digi- ja väestötietovirasto 2024)

Euroopan komissio julkisti vuoden 2023 kesäkuussa joukon lainsäädäntöehdotuksia verkko- ja maksupetoksiin liittyen. Esimerkiksi PSD3 maksupalveluasetuksen maksupetosten torjumiseksi ja lieventämiseksi. Sen tavoitteena on ehkäistä ja vähentää maksupetoksia, parantaa kuluttajien oikeuksia, tasata pankkien toimintaedellytyksiä, parantaa avointa pankkitoimintaa, parantaa käteisen saatavuutta kaupoissa ja pankkiautomaattien kautta sekä harmonisoida EU:n maksumarkkinoita (Nordea 15.3.2024). Se kannustaa maksulaitoksia jakamaan vapaaehtoisesti petokseen liittyviä tietoja toimielinten välisen yhteistyön parantamiseksi. Se myös laajentaa kuluttajan hyvitysoikeuksia, jotka ovat joutuneet verkkorikoksen uhreiksi. (Europol 2024, 34)

6.2 Kansainvälinen yhteistyö

Verkkorikollisuuden hankalimpia puolia on se, ettei se tiedä valtioiden rajoja. Kansainvälinen yhteistyö on nousevassa roolissa paremman huomisen rakentamisessa. Suomen kyberturvallisuusstrategiassa nostettiinkin Suomen Nato-jäsenyyttä vahvistavana tekijänä turvallisuuden ja puolustuksen kannalta. Nato-jäsenyys tuo Suomelle kuitenkin myös haasteita, sillä se voi lisätä vihamielisen toiminnan painetta sen aiheuttaman pelotevaikutuksen myötä. Strategiassa mainitaan, miten EU- ja Nato-jäsenyyden kanssa muu kansainvälinen yhteistyö kyberturvallisuudessa ja -puolustuksessa on laajentunut ja syventynyt. (Valtioneuvosto 2024, 14-15)

Kansainvälistä yhteistyötä kyberuhkiin liittyvissä asioissa pyritään edistämään pitämällä tiivistä keskustelua valtioiden välillä kybertoimintakysymyksiin liittyvissä kysymyksissä. Näitä kysymyksiä käydään läpi niin EU:ssa, Natossa, Euroopan neuvostossa, YK:ssa kuin OECD:ssä. Kansainvälisen keskustelun tavoitteena on edistää avoimen tiedonvälityksen ja sananvapauden toteutumista ja syrjimättömyyttä. Euroopan turvallisuus- ja yhteistyöjärjestö Etyj on ottanut agendalleen aikaisempien turvallisuuskysymysten lisäksi myös kyberuhat ja niiden vaikutuksen turvallisuuteen. (Ulkoministeriö s. a.)

Suomi on myös esimerkillisesti jatkanut tiivistä osallistumistaan kybertoimintaympäristöä koskevaan kansainväliseen yhteistyöhön. Kyberturvallisuusstrategian mukaan Suomi on luotettava toimija euroatlanttisessa yhteisyössä ja turvallisuuden tuottaja. Kyberturvallisuutta kehitetään jatkuvasti samanmielisten maiden kanssa ja etenkin Pohjoismaisten yhteisarvojen pohjalta. Suomen tavoitteena on vakaan kyberympäristön luominen ja säilyttäminen kyberdiplomatian edistämisen valossa. (Valtioneuvoston kanslia 2024, 32)

6.3 Tulevaisuuden lainsäädännölliset muutokset

Jos tulevaisuudessa ei näy positiivisia muutoksia kyberturvallisuuden suhteen, tietoturvalainsäädäntöön tulee varmasti lisää tiukennuksia ja kiristyksiä tarpeen mukaan. (LähiTapiola 2024)

Euroopan unionin neuvosto, Euroopan komissio ja Euroopan parlamentti ovat hyväksyneet sähköisen oikeuden strategian vuosille 2024-2028. Sähköisen oikeuden strategian katsotaan EU:n oikeusministerien mukaan vauhdittavan lainsäädäntöaloitteiden ja muiden kuin lainsäädäntöaloitteiden täytäntöönpanoa. Strategian myös toivotaan saavan aikaan edistystä uusilla ja täydentävillä aloilla. (Euroopan unionin neuvosto 2023, 2) Vaikka strategia painottuukin oikeusalan digitalisaation, sivuaa se kuitenkin samalla kyberuhkia, kyseessä on kuitenkin digitalisaation edistämisen tavoitteleminen. Strategiassa mainitaankin kyberturvallisuuden

tärkeydestä unohtamatta yksityisyyden suojaa ja tietosuojaa koskevaa lainsäädäntöä. (Euroopan unionin neuvosto 2023)

Identiteettivarkauden noustessa yhä pinnalle on mietittävä myöskin uhreja tukevaa toimintaa rikoksen jälkeen. Esimerkiksi henkilötunnusten suojaamisen tärkeyden takia, niiden vaihtamisen helpottamisesta on puhuttu. Lain mukaan henkilötunnukset on tarkoitettu pysyviksi eikä niitä voi muuttaa kuin vain poikkeuksellisissa tapauksissa. Digi- ja väestövirasto onkin vuosien mittaa saanut kysymyksiä, henkilötunnuksen muuttamisen helpottamisesta, auttaakseen tietomurtojen tai identiteettivarkauden kohteeksi joutuneita henkilöitä (Valtioneuvosto 2024b). Vaikka henkilötunnuksen muuttaminen ei poista tulevaisuuden mahdollisia riskejä, olisi kuitenkin ehkä hyvä pohtia uusia käytäntöjä uhrien vahinkojen lieventämiseksi.

7 Pohdinta

Verkkorikollisuuden uhat ja yksityisyyden suojan turvaaminen eivät enää pitäisi tulla yllätyksenä yksilöille tai organisaatioille. Verkkorikollisuuden trendien ollessa pysyneet samoina ja niiden suhteellisen helpon ennustettavuuden takia, panostaminen ennaltaehkäiseviin toimiin olisi tärkeää. Jokaisen organisaation tulisi ottaa prosesseihin kunnolla mukaan toimia, joita voidaan tehdä ennen rikoksien tapahtumista ja niiden jälkeen. Pääpainona tulisi kuitenkin toimia ennaltaehkäisy eikä vahinkojen lieventäminen. Tämä säästää niin organisaatioiden kuin yksilöiden aikaa ja rahaa. Suomessa kuitenkin on tällä hetkellä vertailujen pohjalta hyvät valmiudet verkkorikollisuuden torjuntaan ja valtio käyttääkin resursseja hyviin kohteisiin kuten Kyberturvallisuuskeskuksen kehittämiseen. Tutkimuksessa huomataan kuitenkin, että vaikka resursseja käytetään, ovat pienet ja keskikokoiset organisaatiossa heikossa asemassa. Näillä organisaatioilla ei nimittäin vielä ole tarpeeksi resursseja torjuntaa vaativiin toimenpiteisiin. Valtion tulisi siis jatkossa myös keskittyä näiden organisaatioiden tukemiseen.

Resurssien puute on yksi johtavista ongelmista digiturvallisuuden parantamiselle. Suomi ei resursseja pysty kasvattamaan ilman lisätoimia. Siispä väliaikaisena ratkaisuna olisi syytä pohtia, että jos tämänhetkinen resurssien käyttö ei tuota haluttua tulosta, pitäisikö resursseja jakaa eri lailla, tai kokeilla uusia ja innovaatioisia keinoja. Tutussa ja turvallisissa keinoissa pysyminen on varmasti helppo keino jatkaa, mutta verkkorikosten kasvaessa ja uhrien lisääntyessä, strategiaa pitäisi kehittää ja keskittyä sen eri epäkohtiin.

Monet yritykset onneksi kuitenkin keskittyvät suuresti verkkorikollisuuden uhista tiedottamiseen, ja tiedot ovat melko helppoja löytää. Tänä päivänä verkkoympäristö tarjoaakin hyvän alustan etsiä vastauksia omiin ongelmiin, ja melkein kaikkeen löytyy vastaus. Kaikki eivät kuitenkaan ole digitaalisesti yhtä lahjakkaita, eivätkä välttämättä tiedä mistä hakea tietoa. Yksilöiden tiedottamiseen olisi syytä panostaa yhä enemmän, jotta voimme taata jokaiselle digiturvallisen ympäristön, jossa omat tiedot ovat suojassa ja uhriksi joutumisen riski pieni.

Tärkeimpinä opinnäytetyön aikana löytyneitä tuloksia on ehdottomasti, kuinka liitoksissa digiturvallisuus on jokaisen elämään. Käytämme jatkuvasti verkkoympäristöä, olimme sitten töissä, koulussa tai viettämässä vapaa-aikaa. Yksilöiden tulisi ottaa yhä suurempi vastuu omasta verkkokäyttäytymisestään ja mieleemme pitäisi saada asenne uuden tiedon jatkuvasta kiinnostuksesta. Vaikka riskit eivät näkyisi meidän elämässämme ja vaikka Suomi onkin melko turvallinen maa, ei se saisi tuoda liian helpotuksen ja turvallisuuden tunnetta. Tarkoituksena ei ole lisätä paniikkia ja epäluottamusta kaikkia digipalveluita kohtaan, mutta herättää hieman spekulointia ja varovaisuutta. Verkkoympäristö on kehittynyt vuosien saatossa, on se silti erittäin

ennalta-arvaamaton. Viranomaisten tulisi siis jatkaa erilaisten tulosten mittaamista kyberturvallisuuteen liittyen, ja jakaa tuloksia yhä enemmän.

Tutkimuksessa on käytetty laajasti verkosta löytyviä artikkeleita, kirjallisuutta, uutisia, julkaisuja sekä lakitekstejä. Luotettavuuteen vaikuttavimpia tekijöitä ovat artikkelien aitous sekä esimerkiksi kirjottajien asiantuntijuus. Lain ja säädösten mukaan luotettavuutta voi pitää melko korkeana, sillä verkosta löytyvät lakitekstejä voidaan pitää luotettavana. Lakien kuvailu on myös pyritty etsimään suoraan Finlexin sivuilta, eikä esimerkiksi muilta verkkosivuilta, joiden asiantuntijuudesta ei ole takuuta. Luotettavuuteen voi tietysti vaikuttaa lakien oma tulkinta opinnäytetyötä työstäessä.

Pääosin tutkimusta kirjoittaessa materiaalina on käytetty mahdollisimman ajankohtaisia lähteitä. Tutkimuksen peruspohjana lähteitä on myös ollut pidemmältäkin aikaväliltä, mutta tulokset on pyritty muodostamaan käyttäen uusimpia julkaisuja. Ajankohtaisuutta haasteellisemmaksi tekee sen, että esimerkiksi lait kestävät monia vuosia astua voimaan, ja uusimmista tehokeinoista ei välttämättä ole kansalaisilla tietoa. Erilaisten tutkimusten tarkasteleminen toi ajankohtaisuudesta myös toisen ongelman. Monet raportit julkaistaan vuosittaisen tutkimusten muodossa, ja koska vuosi on vasta lopussa, ei tämän vuoden kokonaisia tutkimustuloksia ole vielä julkaistu. Verkkorikollisuuden kehitystä ei voi siis aivan täysin tähän vuoteen vertailla ajankohtaisesti vaan vuosittaisia tuloksia on jouduttu tarkastelemaan viime vuosilta.

Verkkorikollisuuden tutkimista ja sen vaikutuksia olisi syytä tutkia jatkossa julkisesti ehkä hieman jopa enemmän ja luoda käyttäjille enemmän pohjaa kiinnostukselle. Opinnäytetyö käsittelee haittoja yksilön tasolla, ja jatkotutkimuksena voisi tutkia esimerkiksi verkkorikollisuuden vaikutusta vanhenevaan tai uuteen väestöön. Miten vanheneva väestö pärjää yhä digitalisoituvan maailman kanssa ja miten heitä voitaisiin tukea ja auttaa yhteiskunnassa heidän ollessa helpoin uhri verkkorikollisuuden eri muodoille. Vanhenevalla väestöllä ei ole kykyä tunnistaa verkossa toimimisen vaaroja, joten heidän tukemiseen olisi kehitettävä lisää keinoja. Yritysten normaali toiminta, eli esimerkiksi tietosuojasta ilmoittaminen, ei välttämättä saavuta vanhemmissa samanlaista tietoisuuden astetta kuin nuoremmassa väestössä, jos he eivät edes alussa tiedä mihin suostuvat. Myös uusi nuori väestö voisi olla jatkotutkimuksen kohteena pohdittaessa melko samanlaisia kysymyksiä. Nuorille oiva mahdollisuus oppia verkkorikollisuudesta ja sen vaaroista, olisi järjestää enemmän koulutusta aiheesta. Nuoret eivät myöskään ymmärrä täysin verkkoympäristön vaaroja ja joutuvat siten helposti uhreiksi.

Jatkotutkimuksissa pääpainona voisi ajatella olevan erilaisten tehokkaiden toimenpiteiden pohtiminen, ilman huomattavaa resurssien kasvua. Jatkotutkimuksissa tutkimuksen pohjana asiantuntijoiden haastatteleminen loisi toisen näkökulman verkkorikollisuuden torjunnalle ja toimenpiteelle. Keskustelua asiantuntijoiden välillä voisi luoda juurikin esimerkiksi heidän

kokemuksistaan ja ajatuksista siitä minkälaisia toimenpiteitä Suomi tarvitsisi tulevaisuudessa turvallisen digiympäristön luomiselle.

Opinnäytetyö on ollut melko pitkä ja hidas projekti. Aluksi ongelmana esiintyi aiheen valinnan vaikeus. Opintojen edetessä mielenkiinnon kohteet olivat tulleet selväksi, mutta aihe opinnäytetyölle oli vaikeaa valita. Haasteita myös toi ajatus siitä, riittäisikö mielenkiinto aiheesta opinnäytetyön loppuun saattamiseen asti. Opinnäytetyön kirjoittaminen itsessään oli suhteellisen nopeaa suuresti materiaalin laajan kirjon ansiosta. Työn tekeminen ei itsessään myös tuntunut liian haastavalta, mikä toisinaan johtui aikataulun nopeudesta. Tämä toi painetta kirjoittamiseen, mikä helpotti siinä, ettei prosessia ehtinyt ajatella liikaa. Prosessin aloitus tapahtui mielestäni ajallaan, mutta sen loppuun saattaminen jäi ja loppua kohden voin todeta, että kiire tuli.

Toisena haasteena yllättävästi ilmeni materiaalin paljous ja rajaamisen ongelma. Koen, että rajaamista olisi voinut tehdä vielä enemmän. Materiaalia myös kertyi todella paljon, ja niistä olikin hyvin vaikeaa valita, mitä käyttäisi. Materiaaliakin olisi voinut rajata vielä enemmän, ja sitä onkin valmiissa työssä käytetty ehkä liikaa. Opinnäytetyön aiheellinen rajaus ideana oli puolestaan melko helppoa, vaikka kansainvälisyys kiinnostaakin itseäni. Kansainvälinen oikeus ei ole kuitenkaan ollut itselle mielenkiinnon kohteena, joten keskittyminen Suomen näkökulmaan opinnäytetyötä tehdessä tuntui luontevalta valinnalta. Opinnäytetyöprosessin aikana verkkorikollisuus on tullut hyvin tutuksi ja se onkin ehkä jopa kasvattanut omaa mielenkiintoa aihetta kohtaan entistä enemmän.

Ennakkoluuloja ei opinnäytetyötä aloittaessa oikeastaan ollut, oli melko selvää, mitä prosessi tuo sisällään. Prosessi toi aavistelemani haasteet ja aluksi suhtautuminen niihin olikin positiivisella asenteella. Kokonaisuutena koin opinnäytetyön kuitenkin mielenkiintoisena prosessina, sekä oli kiva tuntea, oman mielenkiinnon kasvua uusia ja jo opittuja asioita kohtaan. Aiheeseen tutustuminen on myös itselle hyväksi, sillä opitut asiat auttavat myös minua pärjäämään paremmin digitaalisessa maailmassa.

Lähteet

Arctic Wolf 2024. A brief History of Cybercrime. Luettavissa: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. Luettu: 3.11.2024.

Business Finland 2022. Asiakkaidemme tietoturvallisuus. Luettavissa: https://www.businessfinland.fi/suomalaisille-asiakkaille/tietoa-meista/asiakkaidemme-tietoturvallisuus. Luettu: 27.10.2024.

Cyber security Intelligence 2021. Cyber Crime Just Keeps On Growing. Luettavissa: https://www.cybersecurityintelligence.com/blog/cyber-crime-just-keeps-on-growing-5888.html. Luettu: 24.10.2024.

Cyber security Intelligence 2024. Cyber Security Teams Feel The Pressure. Luettavissa: https://www.cybersecurityintelligence.com/blog/cyber-security-teams-feel-the-pressure-8028.html. Luettu: 8.11.2024.

Digi- ja väestötietovirasto 2023. Digiturvabarometri: Yli puolet digimaailman rikoksista jää ilmoittamatta viranomaisille. Luettavissa: https://dvv.fi/-/digiturvabarometri-yli-puolet-digimaailman-rikoksista-jaa-ilmoittamatta-viranomaisille. Luettu: 4.11.2024.

Digi- ja väestötietovirasto 2024. Digiturvabarometri: Verkkorikollisuus on laskenut luottamusta digimaailmaan, mutta siitä huolimatta siedämme hyvin muuttunutta uhkatilannetta. Luettavissa: https://www.sttinfo.fi/tiedote/70539029/digiturvabarometri-verkkorikollisuus-on-laskenut-luottamusta-digimaailmaan-mutta-siita-huolimatta-siedamme-hyvin-muuttunutta-uhkatilannetta?publisherId=3777&lang=fi. Luettu. 1.11.2024.

Digi- ja väestövirasto s.a. Digiturvan tietopalvelut. Luettavissa: https://dvv.fi/digiturvan-tietopalvelut. Luettu: 11.11.2024.

Enisa 2022. Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! Luettavissa: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030. Luettu: 2.11.2024.

Euroopan komissio 2023. Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi). Luettavissa: https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive. Luettu: 14.11.2024.

Euroopan parlamentti 2022. Kyberrikollisuuden torjunta: EU:n uudet kyberturvallisuussäädökset. Luettavissa:

https://www.europarl.europa.eu/topics/fi/article/20221103STO48002/kyberrikollisuuden-torjunta-eu-n-uudet-kyberturvallisuussaadokset. Luettu: 9.11.2024.

Euroopan unionin neuvosto 2023. Euroopan sähköisen oikeuden strategia 2024-2028. Luettavissa: https://data.consilium.europa.eu/doc/document/ST-15509-2023-INIT/fi/pdf. Luettu: 26.10.2024.

European Data Protection Board s.a. Data protection benefits for you. Luettavissa: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en. Luettu: 15.11.2024.

Europol 2024. Iocta: Internet organised crime threat assessment. Luettavissa: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf. Luettu: 8.11.2024.

Eur-Lex 2022. Yleinen tietosuoja-asetus (GDPR). Luettavissa: https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html. Luettu: 14.11.2024.

F-Secure 2022a. Mitä on tietojenkalastelu? Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 6.11.2024.

F-Secure 2022b. Mikä on ransomware? Luettavissa: https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack. Luettu: 4.11.2024.

F-Secure 2022c. What is a distributed denial of service attack (DDoS)? Luettavissa: https://www.f-secure.com/en/articles/what-is-ddos. Luettu: 5.11.2024.

F-Secure 28.10.2023. Mikä on kaksivaiheinen tunnistautuminen (2FA). Luettavissa: https://www.f-secure.com/fi/articles/what-is-two-factor-authentication. Luettu: 3.11.2024.

F-Secure 14.12.2023. 5 quick and easy ways to avoid identity theft. Luettavissa: https://www.f-secure.com/en/articles/5-quick-and-easy-ways-to-avoid-identity-theft. Luettu: 26.10.2024.

Henkilötietolaki 523/1999.

Holmberg, L. 2024. Verkkorikollisuuden kasvu uhkaa kansalaisten luottamusta digitaalisiin palveluihin ja laitteisiin. Turun Sanomat. Luettavissa: https://www.ts.fi/lukijoilta/6448214. Luettu: 27.10.2024.

ITU 2024. Global Cybersecurity Index 2024. Luettavissa: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024. Luettu: 10.11.2024.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Kauppakamari. Helsinki. E-kirja. Luettu. 2.11.2024.

Kananoja, K. 2024. Pienet yrityksen verkkorikollisuuden kohteena. Suomen Yrittäjäopisto. Luettavissa: https://www.syo.fi/blogi/pienet-yritykset-verkkorikollisuuden-kohteena/. Luettu: 26.10.2024.

Kinnunen, E. 2023. Organisaation Digiturvakysely. Digi- ja väestötietovirasto. Luettavissa: https://dvv.fi/documents/16079645/110183105/Organisaation+digiturvakysely,+raportti+kevät+2023.pdf/f8bededb-4702-85d3-2623-fadd5096458d/Organisaation+digiturvakysely,+raportti+kevät+2023.pdf?t=1685522697888. Luettu: 2.11.2024.

Kuluttajaliitto 2024. Huijausviestit ja tietojenkalastelu. Luettavissa: https://www.kuluttajaliitto.fi/materiaalit/huijausviestit-ja-tietojenkalastelu/. Luettu: 1.11.2024.

Kyberturvallisuuskeskus 30.7.2020. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon. Luettu: 27.10.2024.

Kyberturvallisuuskeskus 2020. Tulevaisuus, yhteistyötä ja johdon vastuu puhuttivat Tietoturva 2020 -seminaarissa. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tulevaisuus-yhteistyo-ja-johdon-vastuu-puhututtivat-tietoturva-2020-seminaarissa. Luettu: 23.10.2024.

Kyberturvallisuuskeskus 2023a. Tietoturva on koko organisaation asia – vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston. Luettu: 15.11.2024.

Kyberturvallisuuskeskus 2023b. Tammikuun uudistettu kybersää julkaistu. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa_01/2023. Luettu: 8.11.2024.

Kyberturvallisuuskeskus 26.2.2024. Tietoturvasääntely. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturvasaantely. Luettu: 20.11.2024.

Kyberturvallisuuskeskus 15.8.2024. Mikä ihmeen kiristyshaittaohjelma? Luettavissa: https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma. Luettu: 27.10.2024.

Kyberturvallisuuskeskus 20.9.2024. Kyberturvallisuuskeskuksen viikkokatsaus – 38/2024. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-382024. Luettu: 10.11.2024.

Kyberturvallisuuskeskus 10.10.2024. Kybersää syyskuu 2024. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybersää%20syyskuu%202024.pdf. Luettu: 3.11.2024.

Kyberturvallisuuskeskus s.a. a. NIS2 – Euroopan unionin kyberturvallisuusdirektiivi. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi. Luettu: 3.11.2024.

Kyberturvallisuuskeskus s.a. b. Kybermittari. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari. Luettu: 13.11.2024.

Kyberturvallisuuskeskus 2024. Toimintamme. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme. Luettu: 14.11.2024.

Kärkkäinen, H. 23.4.2021. Henkilötunnuksen vaihtaminen helpottuu aikaisintaan 2023. Ilta Sanomat. Luettavissa: https://www.is.fi/digitoday/art-2000007937129.html. Luettu: 1.11.2024.

Kärkkäinen, H. 6.5.2021. Vastaamon it-järjestelmistä vastanneet miehet olivat aiemmin pidätettynä Tekesin tietomurtojutussa – epäiltiin törkeästä petoksesta. Ilta Sanomat. Luettavissa: https://www.is.fi/digitoday/tietoturva/art-2000007960986.html. Luettu: 3.11.2024.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Lapinkangas, J. 30.4.2024. Aleksanteri Kivimäelle kova tuomio. Iltalehti. Luettavissa: https://www.iltalehti.fi/kotimaa/a/78fc37b7-7caa-4799-9144-fe7e9ca8b4b4. Luettu: 26.10.2024.

LähiTapiola 2024. Mikä ihmeen NIS2-direktiivi? Uusi kyberturvallisempi aikakausi alkamassa. Luettavissa: https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/ajankohtaista/mika-ihmeen-nis2-direktiivi-uusi-kyberturvallisempi-aikakausi-alkamassa/. Luettu: 13.11.2024.

Mannermaa, J. & Salumäki, T. 2.8.2023. Vastaamo-tutkinta siirtymässä syyteharkintaan – kiristäjä onnistui saamaan vain muutamia tuhansia. Yle. Luettavissa: https://yle.fi/a/74-20043445. Luettu: 26.10.2024.

Microsoft 2024. Mikä on tietomurto? Luettavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-a-data-breach. Luettu: 27.10.2024.

Mielenterveystalo s.a. Luottamus työyhteisössä. Luettavissa: https://www.mielenterveystalo.fi/fi/mielenterveys-ja-toimintakyky/luottamus-tyoyhteisossa. Luettu: 20.11.2024.

Mysafety 2022. Tutkimus: Yksityishenkilöiden identiteettivarkaudet Suomessa. Kevät 2022. Luettavissa: https://www.lukusali.fi/index.html?p=mySafety&i=552c29bc-b653-11ec-9535-00155d64030a. Luettu: 27.10.2024.

Mysafety s.a. Identiteettivarkaudet ja petokset – tietoa ja tutkimustuloksia. Luettavissa: https://www.mysafety.fi/identiteettivarkaus. Luettu: 1.11.2024.

Mysafety 2024. Yritysten identiteettivarkaudet. Luettavissa: https://www.mysafety.fi/yritysten-identiteettivarkaudet. Luettu: 2.11.2024.

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. Kauppakamari. Helsinki. E-kirja. Luettu: 26.10.2024.

Nordea 15.3.2024. What are PSD3 and PSR? Luettavissa: https://www.nordea.com/en/news/what-are-psd3-and-psr?translation=fi. Luettu: 1.11.2024.

Nordea 11.11.2024. Mikä on palvelunestohyökkäys ja miksi se hidastaa palveluja? Luettavissa: https://www.nordea.com/fi/uutiset/mika-on-palvelunestohyokkays-ja-miksi-se-hidastaa-palveluja. Luettu: 16.11.2024.

Office of the Privacy Commissioner of Canada 2014. Privacy and Cyber Security Emphasizing privacy protection in cyber security activities. Luettavissa: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/#fn1. Luettu: 26.10.2024.

Oikeusministeriö s.a. Rikosoikeus. Luettavissa: https://oikeusministerio.fi/rikosoikeus. Luettu: 1.11.2024.

Poliisi 2024a. Tietomurrot. Luettavissa: https://poliisi.fi/tietomurrot. Luettu: 8.11.2024.

Poliisi 2024b. Palvelunestohyökkäykset. Luettavissa: https://poliisi.fi/palvelunestohyokkays. Luettu 4.11.2024.

Poliisi 2024. Kyberrikokset. Luettavissa: https://poliisi.fi/kyberrikokset. Luettu: 4.11.2024.

Petrosyan, A. 2024. Annual cost of cybercrime worldwide 2018-2029. Statista. Luettavissa: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Luettu: 1.11.2024.

Ralston, W. 9.12.2020. A dying man, a therapist and the ransom raid that shook the world. Wired. Luettavissa: https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/. Luettu: 26.10.2024.

Rautio, M. & Paukkeri, M. 26.4.2023. Vastaamon tietomurron uhreilla on toukokuun loppuun asti aikaa tehdä rikosilmoitus ja antaa lausunto – nyt ilmoituksia on tehty noin 24 000. Yle. Luettavissa: https://yle.fi/a/74-20028919. Luettu: 27.10.2024.

Rikoslaki 19.12.1889/39.

Rikosuhripäivystys 2017. RIKU-lehti nro. 2/2017. Luettavissa: https://www.riku.fi/content/uploads/su_file/1883__RIKU_2_2017.pdf. Luettu: 3.11.2024.

Rimpiläinen, T. 26.10.2020. Paljastaako pilkutus jotakin Vastaamon kiristäjästä? Miksi hän ei osaa teititellä suomeksi? Tämä tiedetään valtavasta kiristysvyyhdistä. Yle. Luettavissa: https://yle.fi/a/3-11613667. Luettu: 26.10.2024.

Salumäki, T. 19.5.2020. Syyttäjä ja ex-toimitusjohtaja Ville Tapio valittivat Vastaamo-tuomiosta. Yle. Luettavissa: https://yle.fi/a/74-20032508. Luettu: 27.10.2024.

Second Nature Security 2023. ChatGPT ja WormGPT: Tekoäly laittaa tietojenkalastelun turbovaihteelle. Luettavissa: https://www.2ns.fi/chatgpt-ja-wormgpt-tekoaly-laittaa-tietojenkalastelun-turbovaihteelle/. Luettu: 14.11.2024.

SIA Innovations s.a. Loss of Trust: A Cybersecurity Attack's Invisible Consequence. Luettavissa: https://www.siainnovations.com/blog/loss-of-trust-a-cybersecurity-attacks-invisible-consequence/. Luettu: 20.11.2024.

Sisäministeriö 2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys 14/2017. Helsinki. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1. Luettu: 4.11.2024.

Suomi.fi 2024. Organisaatioltani on viety tai vuotanut tietoja. Luettavissa: https://www.suomi.fi/oppaat/tietomurto/akuutit-toimet/ilmoita-viranomaisille. Luettu: 16.11.2024.

Tietosuojavaltuutetun toimisto s.a. Tietosuojalaki. Luettavissa: https://tietosuoja.fi/tietosuojalaki. Luettu: 8.11.2024.

Tietosuojalaki 1050/2018.

Tobin, D. 2024. What is Data Privacy – and Why Is It Important? Integrate.io. Luettavissa: https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/. Luettu: 8.11.2024.

Traficom 2024. SMS Sender ID -tunnus. Luettavissa: https://traficom.fi/fi/viestinta/laajakaista-ja-puhelin/sms-sender-id-tunnus. Luettu: 2.11.2024.

Ulkoministeriö s. a. Kyberturvallisuus ja kybertoimintaympäristö. Luettavissa: https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto#Kansainvälinen%20yhteistyö%20kyberasioissa. Luettu: 14.11.2024.

Valtanen, T. & Harjumaa, M. 24.10.2020. F-Securen Hyppönen Vastaamon asiakkaiden kiristämisestä: Kansainvälisestikin poikkeuksellinen tapaus. Yle. Luettavissa: https://yle.fi/a/3-11612224. Luettu: 27.10.2024.

Valtiokonttori 2024. Vastaamon uhrit. Luettavissa: https://www.valtiokonttori.fi/palvelut/korvaus-ja-vahinkopalvelut/vastaamo/. Luettu: 5.11.2024.

Valtioneuvosto 2024a. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä. LVM44:00/2022. Luettavissa: https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022. Luettu: 3.11.2024.

Valtioneuvosto 2024b. Henkilötunnuksen muuttaminen ei ole oikotie väärinkäytösten estämiseksi – tärkeintä on henkilöllisyyden vahva tunnistaminen. Luettavissa: https://valtioneuvosto.fi/-//16079645/henkilotunnuksen-muuttaminen-ei-ole-oikotie-vaarinkaytosten-estamiseksi-tarkeinta-on-henkilollisyyden-vahva-tunnistaminen. Luettu: 20.11.2024.

Valtioneuvoston kanslia 2024. Suomen kyberturvallisuusstrategia 2024-2035. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1&isAllowed=y. Luettu: 1.11.2024.

Veritas 2024. Data Privacy: Understanding Its Importance and Ensuring Compliance. Luettavissa: https://www.veritas.com/information-center/data-privacy. Luettu: 14.11.2024.

Yle 2021. Psykoterapiakeskus Vastaamo asetettiin konkurssiin. Luettavissa: https://yle.fi/a/3-11790537. Luettu: 20.11.2024.