Vastaamon tietomurtotapauksen opit yrityksille

Tanja Auer

Haaga-Helia ammattikorkeakoulu
Tradenomin tutkinto
AMK-opinnäytetyö
2024

Tiivistelmä

Tekijä(t)
Tanja Auer

Tutkinto
Tradenomi

Opinnäytetyön nimi
Vastaamon tietomurtotapauksen opit yrityksille

Sivu- ja liitesivumäärä
29 + 4

Tämän opinnäytetyön tavoitteena oli tarkastella Vastaamon tietomurtotapauksen ongelmakohtia sekä tutkia sitä, mitä kyseinen tapaus on opettanut suomalaisille yrityksille tietoturvasta ja siihen liittyvästä lainsäädännöstä. Tämän lisäksi tarkasteltiin ammattikirjallisuuden avulla sitä, mitä tietoturvatoimia tulisi tehdä noudattaakseen tietoturvaan liittyvää lainsäädäntöä. Tietosuoja ja tietoturva ovat tärkeitä aiheita kaikille yrityksille, sillä lähtökohtaisesti kaikissa yrityksissä käsitellään jonkinlaisia henkilötietoja ja näiden henkilötietojen käsittely on olennaista monen yrityksen toiminnalle.

Tämän kvalitatiivisen opinnäytetyön tutkimusmenetelmänä toimi kvalitatiivinen sisällönanalyysi. Tutkimuksessa oli aineistona suomalaisten yritysten uutismediassa näkyneitä tietoturvalouk-kauksia sekä asiantuntijoiden lausuntoja aiheesta. Tämän lisäksi aineistona oli Suomen yrittäjien järjestön suorittama kyselytutkimus aiheesta tietomurrot. Tämän opinnäytetyön tuloksena syntyi katsaus suomalaisten yritysten tietoturvan ja valmistautumisen tasoon kyberhyökkäyksiä vastaan. Tietoturva on tärkeä aihe verkkoon muuttavassa maailmassa ja kyberhyökkäysten keinojen tehostuessa. Tämä opinnäytetyö antaa katsauksen tietoturvaan liittyvään lainsäädäntöön Vastaamon tietomurtotapauksen kautta sekä tarkastelee ammattikirjallisuuden avulla sitä, miten yrityksen tietoturvatoimet voi suorittaa hyvin. Opinnäytetyö tehtiin maaliskuun ja toukokuun välisenä aikana vuonna 2024.

Työn ensimmäisessä luvussa käydään läpi työn kulku. Toisessa luvussa käydään läpi opinnäytetyön aiheen keskeiset käsitteet. Kolmannessa luvussa käydään läpi Vastaamon tietomurtotapaus ja sen ongelmakohdat. Neljännessä luvussa käsitellään tietoturvaa parantavia ja lainsäädännön vaatimia toimenpiteitä. Viidennessä luvussa käsitellään tietoturvan näkymistä uutismediassa ja yrittäjien käsityksiä yritystensä tietoturvasta. Lopuksi on pohdinta, johon kuuluvat yhteenveto ja opinnäytetyön sekä oman oppimisen arviointi.

Asiasanat
tietosuoja, tietoturva, tietomurto, Vastaamo, tietosuojalainsäädäntö

Sisällys

1 Johdanto

Tämän opinnäytetyön tavoitteena on tarkastella Vastaamon tietomurtotapauksen ongelmakohtia sekä tutkia sitä, mitä kyseinen tapaus on opettanut suomalaisille yrityksille tietoturvasta ja siihen liittyvästä lainsäädännöstä. Tämän lisäksi tarkastellaan ammattikirjallisuuden avulla sitä, mitä tietoturvatoimia tulisi tehdä noudattaakseen tietoturvaan liittyvää lainsäädäntöä. Tietoturva on tärkeä aihe kaikille yrityksille, sillä lähtökohtaisesti kaikissa yrityksissä käsitellään jonkinlaisia henkilötietoja ja näiden henkilötietojen käsittely on olennaista monen yrityksen toiminnalle (Andreasson & Ylipartanen 2022). Yrityksillä on yhteiskunnallinen vastuu luotettavuuteen ja niiden tulisi ottaa vastuu toiminnan vaikutuksista sidosryhmiinsä, mihin kuuluu tietysti myös tietoturvan riittävyys (Kuluttajaliitto 2024). Varsinkin Venäjän Ukrainaan hyökkäyksen jälkeen verkkohyökkäykset ovat lisääntyneet, mikä lisää tarvetta riittävälle tietoturvalle. Opinnäytetyön tutkimusmenetelmänä on sisällönanalyysi. Sisällönanalyysin aineisto on valittu vastuullisesti luotettavia medialähteitä käyttäen.

1.1 Aiheen rajaus ja tutkimuskysymykset

Tutkimuksen kohteena on selvittää, mitä Vastaamon tietomurto opetti yrityksille tietoturvasta ja tietosuojaan liittyvästä lainsäädännöstä. Tässä opinnäytetyössä käsitellään suoraan Vastaamon tietomurtotapauksessa esille tulleita ongelmakohtia, jotka liittyvät laajalti tietojärjestelmän heikkouteen.

Alaongelmina opinnäytetyössä ovat

- Mitä Vastaamon tapauksessa tarkalleen ottaen tapahtui ja mitä tietosuojalainsäädännön osia siinä rikottiin?
- Miten yritysten tietoturva ja mahdolliset tietomurrot ovat olleet esillä mediassa Vastaamon tietomurtotapauksen jälkeen?
- Mitä yrityksen tulee käytännössä tehdä välttääkseen vastaavanlaiset tapaukset tai miten sellaiseen tulisi reagoida?

1.2 Työn rakenne

Tässä opinnäytetyössä on 6 lukua. Johdannon jälkeen toisessa luvussa avataan opinnäytetyön kannalta tärkeitä käsitteitä. Kolmannessa luvussa käydään läpi Vastaamon tietomurtotapaus ja sen ongelmakohdat. Neljännessä luvussa käsitellään tietoturvaa parantavia ja lainsäädännön vaatimia toimenpiteitä. Viidennessä luvussa käsitellään tietoturvan näkymistä uutismediassa ja yrittäjien käsityksiä yritystensä tietoturvasta. Viimeinen eli kuudes luku on pohdinta.

2 Käsitteet

Tässä luvussa käydään läpi tämän opinnäytetyön kannalta tärkeät käsitteet. Nämä käsitteet ovat henkilötieto, rekisteri, rekisterinpitäjä, tietosuoja, tietoturva ja tietoturvaloukkaus.

2.1 Henkilötieto

Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, eli yleisessä tietosuoja-asetuksessa, tarkoitetuilla henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön suoraan liittyviä tietoja sekä sellaisia erillisiä tietoja, jotka yhdistettyinä tekevät mahdolliseksi tietyn henkilön tunnistamisen. Anonymisoidut, salatut tai pseudonymisoidut henkilötiedot, joita voidaan käyttää henkilön tunnistamiseen, ovat yleisen tietosuoja-asetuksen soveltamisalaan kuuluvia henkilötietoja. Jos henkilö ei ole enää tunnistettavissa henkilötietojen peruuttamattoman anonymisoinnin vuoksi, näitä henkilötietoja ei katsota enää laissa tarkoitetuiksi henkilötiedoiksi. (Euroopan komissio 2024c.)

Suoraan henkilöön liittyviä henkilötietoja ovat esimerkiksi nimi, kotiosoite, puhelinnumero ja sähköpostiosoite. (Euroopan komissio 2024.) Välillisiä henkilötietoja, joista henkilön voi yhdistämällä tunnistaa, ovat esimerkiksi henkilölle tunnusomaiset fyysiset, taloudelliset, kulttuurilliset ja sosiaaliset tekijät. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Henkilötietojen käsittelyn tekniikalla tai niiden säilytystavalla ei ole merkitystä tietosuoja-asetuksen soveltamisen kannalta. Henkilötiedot voivat siis sijaita esimerkiksi IT-järjestelmässä, paperiarkistossa tai videovalvontajärjestelmässä. (Tietosuojavaltuutetun toimisto 2024c.)

Yleisessä tietosuoja-asetuksessa erityisillä henkilötietoryhmillä tarkoitetaan arkaluonteisia tietoja, joita ovat rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveystiedot, henkilön tunnistamiseen käytetyt geneettiset ja biometriset tiedot sekä seksuaalisen suuntautuminen ja käyttäytyminen. (Euroopan komissio 2024b.)

2.2 Rekisteri

Yleisessä tietosuoja-asetuksessa rekisteri on mitä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Tietojoukon muoto voi olla moninainen, eli se voi olla keskitetty, hajautettu tai jaettu toiminnallisin tai

maantieteellisin perustein. Toisin sanoen siis rekisteri on samaa käyttötarkoitusta varten kerättyjä ja käytettyjä tietoja, joiden sijainnin teknisellä toteutustavalla ei ole väliä. Tiedot voivat olla siis esimerkiksi sekä sähköisesti että paperisena. (Hanninen, Laine, Rantala, Rusi, & Varhela 2017, 22.)

2.3 Rekisterinpitäjä

Yleisessä tietosuoja-asetuksessa rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot yksin tai yhdessä toisten kanssa. Lyhyesti siis rekisterinpitäjä on henkilötietojen keruusta ja niiden käyttötarkoituksista päättävä organisaatio. (Hanninen ym. 2017, 22.) Rekisterinpitäjästä esimerkkinä ovat esimerkiksi potilastietoja keräävä sairaala, verkkokauppa tai jäsenistään tietoja keräävä yhdistys (Tietosuojavaltuutetun toimisto 2024b).

Rekisterinpitäjän vastuulla on henkilötietojen käsittelyn lainmukaisuus koko käsittelyn elinkaaren ajan (Tietosuojavaltuutetun toimisto 2024a).

2.4 Tietosuoja ja tietoturva

Tietosuojalla tarkoitetaan perusoikeutta siihen, että rekisteröidyn oikeudet ja vapaudet toteutuvat henkilötietoja käsiteltäessä (Tietosuojavaltuutetun toimisto 2024h). Näitä oikeuksia ovat mahdollisuus seuraaviin: tiedon saaminen henkilötietojen käsittelystä, tietoihin tutustuminen, tietojen oikaiseminen, tietojen poistaminen, tietojen käsittelyn rajoittaminen, tietojen siirtäminen, tietojen käsittelyn vastustaminen ja automaattisen päätöksenteon kohteeksi joutumatta oleminen (Tietosuojavaltuutetun toimisto 2024i). Tietosuoja liittyy useiden muiden perusoikeuksien turvaamiseen, kuten yksityisyydensuoja, yhdenvertaisuus, turvallisuus ja syrjinnän kielto. Tietosuojaan liittyvä keskeinen lainsäädäntö on Euroopan unionin tietosuoja-asetus. (Keller 2023, 88–99.)

Tietoturvalla tarkoitetaan muun muassa tietosuojan toteuttamiseksi tehtyjä tietynlaisia käytännön organisatorisia ja teknisiä toimenpiteitä, eli tietoturvatoimenpiteillä suojataan tietoaineisto ja tietojärjestelmät (Tietosuojavaltuutetun toimisto 2024h). Tietoturva ei koske vain henkilötietoja, vaan sillä tarkoitetaan myös muiden salassa pidettäviä tietoja, kuten yrityssalaisuuksia, turvaavia toimenpiteitä (Keller 2023, 54.).

2.5 Tietoturvaloukkaus

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena ovat henkilötietojen häviäminen, tuhoutuminen, muuttuminen, henkilötietojen luvaton luovuttaminen tai henkilötietoihin pääsy niiden käsittelyoikeutta vailla olevalla taholla. Henkilötietojen

tietoturvaloukkauksiin kuuluvat esimerkiksi varastettu tietokone, hakkerointi, kyberhyökkäys tai hävinnyt USB-tikku. (Tietosuojavaltuutetun toimisto 2024g.)

Tietoturvaloukkauksen seurauksena, henkilön henkilötietojen vuotaessa, voi olla esimerkiksi identiteettivarkaus, maineen vahingoittuminen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen (Tietosuojavaltuutetun toimisto 2024g).

Tietoturvaloukkauksen tapahtuessa yrityksen tulee ilmoittaa asiasta valvontaviranomaiselle ilman aiheetonta viivytystä, mutta viimeistään 72 tunnin määräajassa tietoturvaloukkauksen havaitsemisesta. Yrityksen ollessa rekisterinpitäjä, henkilötietojen käsittelijälle pitää ilmoittaa kaikista tietoturvaloukkauksista. (Euroopan komissio 2024a.)

Yksi tietoturvaloukkauksen muoto on tietomurto. Tietomurto on toimintaa, jossa käyttäjätunnusta käytetään luvattomasti tai tietojärjestelmään murtaudutaan ohittamalla turvajärjestely (Poliisi 2024).

Toinen tietoturvaloukkauksen muoto on palvelunestohyökkäys. Palvelunestohyökkäyksillä tarkoitetaan hyökkäystä, jolla verkkoresurssin tai palvelun käyttöä pyritään tahallisesti estämään sen toimintaa häiritsemällä. Palvelunestohyökkäyksessä palvelu kuormitetaan ylimääräisellä liikenteellä, paljon palvelun muisti- tai laskentaresursseja käyttävällä liikenteellä tai hyödyntämällä palvelun haavoittuvuutta. Palvelunestohyökkäyksen seurauksena verkkoresurssi tai palvelu on toimimaton tietyn aikavälin, mutta palautuu yleensä toimintakuntoon itsestään. (Kyberturvallisuuskeskus 2022.)

3 Vastaamon tietomurto

Vastaamo oli Ville Tapion vuonna 2008 perustama psykoterapiakeskus, jonka tavoitteena oli uudistaa mielenterveyspalveluiden tarjonta digitalisaation avulla. Yrityksen toiminta oli laajennut 20 paikkakunnalle ja työllisti jopa 250 terapeuttia. (Hyppönen 2021, 199; Järvinen 2022, 30.)

Psykoterapiakeskus Vastaamon, tästä lähtien Vastaamo, tietokantaan murtauduttiin kaksi kertaa. Ensimmäinen tietomurto Vastaamon asiakastietokantaan tapahtui joulukuussa 2018, jolloin tuntematon hyökkääjä löysi Vastaamon huonosti suojatun potilastietokannan verkosta ja vei sen. Potilaskanta sisälsi 31 980 potilaan henkilötiedot, joihin kuuluivat muun muassa nimi, osoite henkilötunnus ja puhelinnumero. Näiden lisäksi tietokannassa oli potilaiden kanssa käydyistä keskusteluista tehdyt terapeuttien kirjaukset. Tätä tietomurtoa ei tällöin huomattu Vastaamolla. (Hyppönen 2021, 199–200.)

Toinen tietomurto tapahtui maaliskuussa 2019, kun Vastaamon heikosti suojattu tietojärjestelmä oli löydetty luultavasti jollain verkkoskannausohjelmalla. Tässä tietomurrossa ei ollut ilmeisesti viety merkittäviä määriä tietoja, mutta tällä kertaa tietomurto huomattiin Vastaamolla, joka päätti siirtää tiedot paremmin turvattuun paikkaan. Tämä tapaus ei päätynyt uutisiin asti, vaikka palvelimelle oli jätetty jo tällöin kiristysviesti, koska Vastaamo laiminlöi lakisääteisen ilmoitusvelvollisuutensa ja pysyi hiljaa tapahtuneesta. (Hyppönen 2021, 200; Järvinen 2022, 30.)

Vastaamon tietoturva oli ollut alkeellinen ja huono jo vuosien ajan, sillä potilastietokanta oli ollut suojaamattomassa verkossa jo syksystä 2017 lähtien (Hämäläinen 2021). Vastaamon suojauskeinot olivat puutteellisia tai ne puuttuivat kokonaan, sillä puutteita oli ollut muun muassa palomuurissa, etäyhteyksien suojauksessa, salasanoissa, salaamisessa, lokituksessa ja tietoturvan dokumentoinnissa. (Rimpiläinen 2023.)

Vastaamon lokakuussa 2020 palkkaamat asiantuntijat sanoivat yrityksen tietoturvan olevan erittäin heikkoa ja alkeellista, eikä heidän mielestään missään tavalla sen kanssa ollut noudatettu alan parhaita käytäntöjä. Vastaamon järjestelmäarkkitehtien mukaan Vastaamon terapeutit olivat käyttäneet potilastietojärjestelmää etäyhteyksin ja omilla laitteillaan suojaamattomana sekä ilman valvontaa. (Rimpiläinen 2023.)

Yrityksen potilastietojärjestelmien käyttäjätunnukset ja salasanat olivat myös erittäin suojattomia. Esimerkiksi yhdeltä käyttäjätunnukselta puuttui salana kokonaan ja toisen käyttäjätunnuksen salasana oli ollut erittäin lyhyt ja yksinkertainen. Salasanoja oli myös jaettu suojaamattoman sähköpostiviestinnän välityksellä. (Rimpiläinen 2023.)

Kaikissa työasemassa oli ollut sama salasana, jota käytettiin niiden lisäksi myös hälytysjärjestelmissä ja vartiointiliikkeiden koodisanana. Tämä oli sen vuoksi, että yhtiön tietohallintokonsepti oli sellainen, ettei käyttäjätunnuksia tai salasanoja voinut vaihtaa aiheuttamatta kaaosta toimipisteissä. (Rimpiläinen 2023.)

Tietomurtojen julkiseksi päätymiseen johtaneet tapahtumat alkoivat 28. syyskuuta 2020, jolloin Ransom_man-nimimerkkiä itsestään käyttävä hyökkääjä lähetti Vastaamon toimitusjohtajalle Ville Tapiolle kiristysviestin, jossa hän uhkasi julkaista asiakkaiden potilastietoja internetissä, ellei hänelle makseta 40 bitcoinin suuruisia lunnaita. Tämä summa vastasi noin 450 000 euroa kiristyshetkellä. (Hyppönen 2021, 201.) Vastaamo ilmoitti kiristysviestistä poliisille ja tietosuojavaltuutetulle (Järvinen 2022, 30).

Vastaamoon kohdistuneet tietomurrot tulivat julkisuuteen keskiviikkona 21. lokakuuta 2020. Vastaamo ei maksanut lunnaita, joten Ransom_man alkoi julkaista asiakasrekisterin tietoja pimeässä verkossa, julkaisten kerrallaan sadan asiakkaan potilastiedot. (Järvinen 2022, 30.)

Muutaman päivän kuluessa kuitenkin hyökkääjän virheen vuoksi koko 10,9 gigatavun tiedosto, sisältäen kaikki tietomurroista saadut potilastiedot, olivat internetissä muutaman tunnin ajan kenen tahansa ladattavissa. (Hyppönen 2021, 201–204.) Tämän seurauksena Ransom_man lähetti kiristysviestejä myös uhreille (Järvinen 2022, 31).

Tietomurron seurauksena Vastaamo oli menettänyt asiakkaiden luottamuksen niin pahasti, että yhtiö hakeutui konkurssiin helmikuussa 2021, noin neljä kuukautta tietomurtojen paljastumisen jälkeen. Joulukuussa 2021 tietosuojavaltuutettu määräsi Vastaamolle 608 000 euron seuraamusmaksun henkilötietojen käsittelyn turvallisuuden laiminlyönnistä. Vastaamo ei ollut myös ilmoittanut tietovuodon uhreille tapahtuneesta heti tullessaan itse siitä tietoiseksi. (Järvinen 2022, 31.)

Vastaamon tietomurron aikainen toimitusjohtaja Tapio tuomittiin 18. huhtikuuta 2023 kolmen kuukauden ehdolliseen vankeusrangaistukseen rikoksenaan tietosuojarikos (Mäntysalo & Salumäki 2023).

Ransom_manin henkilöllisyydeksi paljastui tutkinnassa Aleksanteri Kivimäki, joka sai 30. huhtikuuta 2024 Vastaamon tietomurrosta tuomioksi 6 vuotta ja 3 kuukautta vankeutta rikoksinaan törkeä tietomurto, törkeä kiristyksen yrittäminen, 9 231 törkeää yksityiselämää loukkaavan tiedon levittämistä, 20 745 törkeän kiristyksen yrittämistä sekä 20 törkeää kiristystä. (Länsi-Uudenmaan käräjäoikeus 24/119144.)

3.1 Tekniset ja organisatoriset toimenpiteet

Tietosuoja-asetuksen 24 artiklan 1 kohdan mukaan rekisterinpitäjän on käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit huomioon ottaen toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta. Näitä toimenpiteet tulee myös tarkistaa ja päivittää tarvittaessa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Rekisterinpitäjän on siis arvioitava, millaisia riskejä henkilötietojen käsittely sisältää ja millaisia vahinkoja käsiteltävien henkilötietojen paljastuminen ulkopuolisille voi aiheuttaa rekisteröidyille, ja suhteutettava suojatoimet riskin suuruuteen. Esimerkiksi arkaluonteisia henkilötietoja kuten terveystietoja käsiteltäessä riskin määrä on suurempi kuin pelkän sähköpostin ja puhelinnumeron käsittelyssä, jolloin terveystietojen käsittelyn turvatoimissa odotetaan suurempaa huolellisuutta ja enemmän toimenpiteitä. (Hanninen ym. 2017, 26–27.)

Tietosuoja-asetuksen 25 artiklan 1 kohdan mukaan rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden täytäntöönpanoa varten riittävät tekniset ja organisatoriset toimenpiteet, jotta ne saataisiin käsittelyn osaksi ja jotta käsittely vastaisi tietosuoja-asetuksen vaatimuksia ja suojattaisiin rekisteröityjen oikeuksia. Käsittelyn yhteydessä on otettava huomioon uusin tekniikka ja toteuttamiskustannukset sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Rekisterinpitäjällä tulee siis olla henkilötietoja käsiteltäessä sisäänrakennettu tietosuoja. Sisäänrakennettu tietosuoja tarkoittaa sitä, että jo tietoturvatoimia suunnitellessa rekisterinpitäjän tulee ottaa huomioon tietosuoja-asetuksen vaatimat tietosuojaperiaatteet kuten pseudonymisointi tai tietojen minimointi. (Hanninen ym. 2017, 54.)

Tietosuoja-asetuksen 32 artiklan 1 kohdan mukaan rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että turvallisuustaso vastaa riskiä. Näitä toimenpiteitä ovat muun muassa henkilötietojen pseudonymisointi ja salaus, käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuuden, eheyden ja käytettävyyden takaaminen, kyky palauttaa tietojen saatavuus ja tietoihin pääsy fyysisen tai teknisen vian sattuessa, sekä säännöllinen teknisten ja organisatoristen toimenpiteiden tehokkuuden testaaminen, tutkiminen ja arviointi

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

Tietosuoja-asetuksen 32 artiklan 2 kohdan mukaan asianmukaisen tietosuojan turvallisuustason arvioimisessa on kiinnitettävä erityishuomio käsittelyn sisältämiin riskeihin, joita voivat olla siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Vastaamon tietokanta oli ollut ilman palomuurisuojausta internetissä vähintään noin puolentoista vuoden ajan vuoden 2017 marraskuusta vuoden 2019 maaliskuun tietomurtoon asti (Hämäläinen 2021). Tietokannan root-pääkäyttäjätunnukselta puuttui salasana ja tälle käyttäjätunnukselle oli annettu oikeus kirjautua sisään tietokantaan mistä tahansa IP-osoitteesta eikä vain Vastaamon omista toimipisteistä (Tietosuojavaltuutettu 2021). Root-pääkäyttäjällä on valtuus tehdä järjestelmään tietoturvallisuuden kannalta keskeisiä toimintoja, joihin peruskäyttäjällä ei ole oikeuksia (National Institute of Standards and Technology 2024). Yhden peruskäyttäjätunnuksen salasana oli ”skuja66” ja tätä salasanaa ei ollut vaihdettu sen asettamisen jälkeen vuonna 2012. Toinen käyttäjätunnus taas oli nimeltään vain ”vastaamo” ja salasanana oli ollut ”malmi70”. (Rimpiläinen 2023).

Vastaamon organisatoriset toimenpiteet eivät siis olleet riittävät. Vastaamon käsittelemät tiedot ovat erityisen arkaluonteisia, joten rekisteröityjen oikeuksille ja vapauksille todennäköisesti kohdistuva riski on siten korkea ja näin ollen toimenpiteet eivät ole olleet riittävät tämäkin huomioon ottaen.

3.2 Vaikutustenarviointi

Tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan rekisterinpitäjän on toteutettava henkilötietojen käsittelytoimien tietosuojan vaikutustenarviointi, jos tietyntyyppinen käsittely aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679).

Tietosuojan vaikutustenarvioinnilla tarkoitetaan tässä prosessia, jossa tarkastellaan tietoturvatoimenpiteitä, suojatoimia ja mekanismeja, jotka on suunniteltu luonnollisten henkilöiden oikeuksille aiheutuvien riskien lieventämiseksi henkilötietojen käsittelyssä. Vaikutustenarviointi kuvaa henkilötietojen käsittelyä ja arvioi käsittelyn tarpeellisuutta suhteessa riskeihin. Rekisterinpitäjän on vähintään tehtävä arvio siitä, tuleeko sen tehdä vaikutustenarviointi. (Hanninen ym. 2017, 115.)

Tietosuoja-asetuksen 35 artiklan 3 kohdan b alakohdan mukaan tietosuojaa koskeva vaikutustenarviointi vaaditaan erityisesti laajamittaisessa käsittelyssä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Tietosuoja-asetuksen 35 artiklan 7 kohdan mukaan vaikutustenarvioinnin on sisällettävä vähintään järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä, ja suunnitellut toimenpiteet riskeihin puuttumiseksi. Toimenpiteisiin lasketaan mukaan suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tietosuoja-asetusta on noudatettu ja rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut on otettu huomioon. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Vastaamon käsitteli toiminnassaan potilastietoja, jotka lasketaan erityisiksi henkilötietoryhmiksi. Vastaamon toiminnan ollessa psykoterapiapalvelut, voidaan näiden henkilötietojen olleen myös erityisen arkaluonteisia ja korkean riskin ja uhan alla tietoturvaloukkauksen sattuessa. Vastaamolla oli siis velvoite tehdä vaikutustenarviointi. (Tietosuojavaltuutettu 2021.)

Vastaamo loi tietosuojaa koskevan vaikutustenarvioinnin ennen tietomurtoja huhtikuussa 2018, jossa se arvioi jonkin verran erilaisten riskien, kuten luvattoman potilastietojen käsittelyn ja tietojen katoamisen tai tuhoamisen, vakavuutta ja todennäköisyyttä sekä näihin riskeihin puuttumisen toimenpiteitä. Tässä vaikutustenarvioinnissa ei kuitenkaan ollut tarpeeksi hyvin tuotu esille riskien tai uhkien arviointia tai näihin puuttumisen toimenpiteitä. Siinä ei esimerkiksi otettu tarpeeksi huomioon henkilötietojen käsittelyn luonnetta, laajuutta ja asiayhteyttä, riskien luonnetta tai alkuperää, laittomaan henkilötietoihin pääsyyn johtavia uhkia tai näiden uhkien mahdollisia vaikutuksia rekisteröityjen oikeuksille tai vapauksille eikä siinä ollut esitetty käsittelytoimien toiminnallista kuvausta. Kaiken kaikkiaan vaikutustenarvioinnin sisältö oli suppea eikä vastannut lainsäädännön vaatimuksia. (Tietosuojavaltuutettu 2021.)

3.3 Osoitusvelvollisuus

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan mukaan henkilötietoja on käsiteltävä niin, että pystytään takaamaan niiden turvallisuus, eheys ja luottamuksellisuus. Henkilötietoja tulee suojata asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679). Luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin

laitteistoihin on siis ehkäistävä sekä estettävä henkilötietojen ja laitteistojen luvaton käyttö (Hanninen ym. 2017, 51).

Tietosuoja-asetuksen 5 artiklan 2 kohdan mukaan rekisterinpitäjä vastaa siitä, että 5 artiklan 1 kohtaa on noudatettu, eli rekisterinpitäjällä on osoitusvelvollisuus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679). Rekisterinpitäjän on siis pystyttävä käytännön tasolla osoittamaan, että tietosuojaperiaatteita on noudatettu kaikissa henkilötietojen käsittelyn vaiheissa. Rekisterinpitäjän, eli yleensä yrityksen, on siis arvioitava ja dokumentoitava, mitä tietosuojaperiaatteet käytännössä tarkoittavat ja miten niiden toteutuminen tapahtuu sen omassa toiminnassa. (Hanninen ym. 2017, 51.)

Osoitusvelvollisuus on tärkeä siksi, että rekisterinpitäjä pystyy dokumentoinnin avulla esimerkiksi tietoturvaloukkaustilanteessa osoittamaan, kuinka se on aktiivisesti pyrkinyt tekemään tietosuojaan liittyvää riskienhallintaa ja suorittanut henkilötietojen suojaamiseksi tarpeellisia toimenpiteitä. Osoitusvelvollisuus myös lisää luottamusta rekisterinpitäjän toimintaan, sillä se näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen tietosuojaa. (Tietosuojavaltuutetun toimisto 2024d.)

Vastaamolla oli ollut käytössään omavalvontasuunnitelma, jossa oli eritelty tietoturvatoimenpiteet ja niistä vastuussa olevat henkilöt. Sen mukaan Vastaamolla oli tehty riittävät tietoturvakäytännöt, ja heillä oli ollut myös tietosuojavastaava sekä potilasjärjestelmän kehittämiseen, ylläpitoon ja tietoturvasta huolehtimiseen palkatut asiantuntijat. Tietoturvatoimien käytännön toteuttamisen vastuu oli ollut Vastaamon tietosuojavastaavalla ja järjestelmäarkkitehdilla. Omavalvontasuunnitelman mukaan potilastietojärjestelmän palvelimella oli ollut palomuuri ja käyttäjätunnus- ja salasanasuojaukset. Omavalvontasuunnitelmasta huolimatta näitä toimenpiteitä ei kuitenkaan ollut selkeästi noudatettu eikä osoitusvelvollisuutta ollut näin täytetty. (Tietosuojavaltuutettu 2021.)

3.4 Tietoturvaloukkausten ilmoitusvelvollisuus

Tietosuoja-asetuksen 33 artiklan 1 kohdan mukaan henkilötietojen tietoturvaloukkauksen tapahtuessa rekisterinpitäjän on ilmoitettava siitä viipymättä toimivaltaiselle valvontaviranomaiselle, mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on tullut ilmi. Ilmoitusta ei tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Valvontaviranomaiselle tulee toimittaa perusteltu selitys, jos ilmoitusta ei anneta 72 tunnin kuluessa tietoturvaloukkauksesta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Tietosuoja-asetuksen 34 artiklan 1 kohdan mukaan rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle viipymättä, kun henkilötietojen

tietoturvaloukkauksesta todennäköisesti aiheutuu korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Arvioitaessa tietoturvaloukkauksesta aiheutuvaa riskiä on huomioitava henkilötietojen luonne, arkaluonteisuus ja määrä, henkilöiden tunnistamisen helppous, henkilöille aiheutuvien seurausten vakavuus, henkilön ja rekisterinpitäjän erityiset ominaisuudet, tietoturvaloukkauksen vaikutustenalaisten henkilöiden määrä sekä tietoturvaloukkauksen tyyppi. Tietoturvaloukkauksen tyypillä tarkoitetaan sitä, onko tietoturvaloukkauksella vaarantunut henkilötietojen luottamuksellisuus, eheys vai käytettävyys. (Tietosuojavaltuutettu 2021.)

Rekisterinpitäjällä olisi hyvä ilmoittamista helpottava dokumentoitu ilmoitusmenettely, jossa on kuvattu prosessi noudatettavaksi havaitun tietoturvaloukkauksen jälkeen. Tähän prosessiin kuuluvat muuan muassa keinot tietoturvaloukkauksen leviämisen estämiseen, sen hallintaan, tietoturvaloukkauksen kohteeksi joutuneiden tietojen palauttamiseen, riskien arvioimiseen ja tietoturvaloukkauksesta ilmoittamiseen. Yrityksen työntekijöille tulisi myös ilmoittaa tämänlaisesta menettelystä ja varmistaa, että he osaavat toimia sen mukaisesti tietoturvaloukkaustilanteessa. (Tietosuojavaltuutettu 2021.)

Vastaamon maaliskuun 2019 tietoturvaloukkauksen voidaan katsoa aiheuttaneen luonnollisten henkilöiden oikeuksille ja vapauksille korkean riskin, sillä rekisteröidyt olivat suoraan tunnistettavissa potilasjärjestelmässä heistä olevien tietojen perusteella ja potilastiedot kuuluvat erityisiin henkilötietoryhmiin, joiden osalta fyysisten, aineellisten tai aineettomien vahinkojen aiheutuminen rekisteröidyille olisi pidettävä todennäköisenä. Tämän lisäksi Vastaamo oli saanut tietomurrosta lunnasvaatimuksen, jolloin voi katsoa tietomurron tekijän aikeen ollen pahantahtoinen ja näin ollen rekisteröidyille aiheutuvat vahingot olivat todennäköisiä ja luonteeltaan vakavia. (Tietosuojavaltuutettu 2021.)

Vastaamo ei kuitenkaan ollut ilmoittanut maaliskuussa 2019 tapahtuneesta tietoturvaloukkauksesta tietosuojavaltuutetulle eikä rekisteröidyille, joten he eivät olleet noudattaneet tietosuoja-asetuksen 33 artiklan 1 kohtaa tai 34 artiklan 1 kohtaa. Vastaamolla ei myös ole ollut tietoturvaloukkauksien aikaan käytössään mitään ilmoitusvelvollisuuden täyttämistä helpottavaa dokumentoitua ilmoitusmenettelyä, mutta heillä oli kesäkuussa 2017 laadittu omavalvontasuunnitelma, jossa oli annettu tietoturvapoikkeamien käsittelyä koskevia toimintaohjeita. Tätä omavalvontasuunnitelmaa ei kuitenkaan ollut noudatettu tietoturvaloukkausten sattuessa. (Tietosuojavaltuutettu 2021.)

3.5 Tietoturvaloukkausten dokumentointi

Tietosuoja-asetuksen 33 artiklan 5 kohdan mukaan rekisterinpitäjän tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset ja niihin liittyvät seikat. Tämän lisäksi

tulee dokumentoida tietoturvaloukkausten vaikutukset ja toteutetut korjaavat toimet. Valvontaviranomaisen tulee pystyä tästä dokumentoinnista tarkistamaan, että ilmoitusvelvollisuutta on noudatettu. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.)

Myös sellaiset tietoturvaloukkaukset, joista ei tarvitse tehdä ilmoitusta viranomaisille, tulisi dokumentoida perusteluineen ilmoittamatta jättämiselle juuri sen vuoksi, että tällöin on selkeästi dokumentoitu miksi kyseisestä tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä rekisteröityjen oikeuksille ja vapauksille. (Tietosuojavaltuutettu 2021.)

Vastaamo oli laatinut 28.4.2019 asiakirjan maaliskuun 2019 tietoturvaloukkauksesta, jossa oli käsitelty mitä tietoturvaloukkauksessa oli tapahtunut, tietoturvaloukkauksen vaikutukset henkilötietoihin, tietoturvaloukkauksen muut vaikutukset ja seuraukset, tietoturvaloukkauksen mahdollinen riski henkilöiden oikeuksille ja vapauksille, toteutetut korjaavat toimet, perustelut ilmoittamatta jättämiselle sekä tietoturvaloukkauksen käsittely. Tämä asiakirja vastasi siten tietosuoja-asetuksen 33 artiklan 5 kohdan edellyttämää dokumentointia. (Tietosuojavaltuutettu 2021.)

Marraskuun 2018 tietoturvaloukkauksesta sen sijaan Vastaamo ei ollut tehnyt dokumentointia tai sellaista ei ainakaan ollut toimitettu valvontaviranomaiselle. Vastaamo oli siis rikkonut tietosuoja-asetuksen 33 artiklan kohdan 5 edellyttämää dokumentointivelvollisuutta. (Tietosuojavaltuutettu 2021.)

4 Tietoturvan parantaminen

Tässä luvussa käsitellään käytännön toimia tietoturvan hoitamiseksi. Tässä keskitytään niihin tietoturvatoimiin, mitkä Vastaamolla eivät olleet kunnossa, eli järjestelmiin liittyvät tietoturvatoimet. Käsittelyssä tässä ei siis ole niinkään sitä, miten henkilötietojen käsittely itsessään tulisi hoitaa, vaan miten henkilötietoja tulisi suojata tietotekniikkaa käyttäen ja miten tulisi täyttää osoitus- ja ilmoitusvelvollisuus tietoturvatoimiin liittyen.

4.1 Salasanat

Salasanat ovat olennainen osa tietoturvaa sekä yksityishenkilölle että yritykselle. Salasanoilla on pääsy yritysjärjestelmiin, sähköposteihin ja tärkeisiin dokumentteihin, minkä vuoksi varsinkin yrityskäytössä tulisi kiinnittää erityishuomiota salasanan vahvuuteen ja varmistaa, ettei kukaan ulkopuolinen pysty arvaamaan tai vahingossa löytämään niitä

Salasanan turvallisuutta lisää sen pituus ja monimutkaisuus. Salasanan tulisikin olla mahdollisimman pitkä, mutta vähintään 10 merkkiä pitkä, ja sisältää pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Salasana voi olla myös rivi erilaisia sanoja tahallisilla kirjotusvirheillä tai kokonainen lause. (Järvinen 2022, 95.)

Tärkeää on myös tehdä jokaiseen palveluun eri salasana ja vaihtaa salasanoja säännöllisesti. Jos jokin palvelu murretaan ja tilin salasana päätyy tietomurron kohteeksi, ja samaa salasanaa on käytetty muissakin palveluissa, myös näissä palveluissa olevilla tileillä on tietoturva vaarantunut. Salasanan vaihtamisella estetään tai vähennetään vahinkoja, jotka syntyisivät salasanan päätyessä ulkopuolisten käsiin. Monet järjestelmät vaativat salasanan säännöllistä vaihtoa, mutta se kannattaa tehdä myös sellaisissa palveluissa, jotka eivät sitä vaadi. (Järvinen 2022, 96.)

Monimutkaisia salasanoja saattaa olla hankala muistaa. Niitä ei kuitenkaan saisi silti kirjoittaa ylös näkyville, mistä joku ulkopuolinen voisi ne nähdä. Salasanojen muistaminen ulkoa on kaikkein turvallisin vaihtoehto, mutta käytännössä helpointa on kirjoittaa ne ylös turvalliseen paikkaan pois käyttölaitteen läheltä tai ottaa käyttöön salasanojen hallintaohjelma. Salasanojen hallintaohjelmia käytettäessä tulee kuitenkin muistaa se, että hallintaohjelman salasana on erittäin tärkeää muistaa ja tulisi varmistaa palveluun pääsy milloin tahansa, sillä jos salasanapalveluun ei pääse, ei myös pääse käsiksi mihinkään salasanoistaan. (Järvinen 2022, 96.)

Vahvan salasanan lisäksi olisi hyvä olla kaksivaiheinen todennus. Kaksivaiheisessa todennuksessa tarvitaan käyttäjätunnuksen ja salasanan lisäksi myös tunnuksen omistajan puhelin, johon koodi tulee. Tämän avulla pelkkä salasanan tietäminen ei siis riitä. (Järvinen 2022, 97.)

4.2 Tietoturvasuunnitelma

Yrityksen tietosuojan ja tietoturvan toteutumisen seurannassa edellytetään omavalvontaa. Tätä varten kannattaa tehdä tietoturvasuunnitelma, joka toimii kaikkien annettujen ohjeistusten, linjausten ja keinojen runkona ja yhdistäjänä. Tietoturvasuunnitelman tehtävänä on parantaa ja yhdenmukaistaa tietosuoja- ja tietoturvakäytäntöjä sekä varmistaa, että henkilöstö tietää tietoturvamenettelyt ja noudattaa niitä. (Andreasson & Ylipartanen 2022, 115–117.)

Tietoturvasuunnitelman tulisi sisältää tiedot tietoturva-asioiden vastuunpitäjistä, yrityksen hallitsemista tiedoista ja niiden säilytystavoista ja -paikoista, mahdollisen erityistä suojausta vaativan tiedon erittely ja niiden suojaustason määrittely, käytännön toimenpiteet tietojen suojaukseen, käytännön toimenpiteiden suorittajat sekä poikkeustilanteiden toimintatavat vahinkojen minimoimiseksi (Data Group 2024a). Eri henkilöiden ja tahojen vastuut ja roolit ovat keskeistä huomioida tietoturvasuunnitelmassa. Tietoturvasuunnitelmassa on myös tultava esille, miten sen toteutumista seurataan. (Andreasson & Ylipartanen 2022, 117–118.)

4.3 Palvelimen tietoturvariskien hallinta

Vastaamon tietomurtotapauksessa yksi suurimmista virheistä oli ollut se, että heidän tietokantajärjestelmänsä oli ollut suojaamattomana internetissä vuosien ajan. Palvelinalusta, käyttöjärjestelmät ja sovellukset tulisikin suojata. (Juvonen, Koskensyrjä, Kuhanen, Kämppi & Talala 2023.)

Palvelimista tulisi ottaa pois käytöstä kaikki palvelimen käyttötarkoituksen kannalta tarpeettomat palvelut ja ominaisuudet sekä käyttää käyttäjätunnuksien kanssa riittävä vahvoja salasanoja. Palvelimille tallennettu tieto tulisi salata käyttötarkoituksen ja tiedon luottamuksellisuuden mukaan. Käyttöjärjestelmään ja siihen asennettuihin ohjelmiin tulisi myös säännöllisesti suorittaa päivitykset mahdollisimman pian ennen kuin mahdollisesti syntyneitä haavoittuvuuksia voidaan hyödyntää. Palvelimen tiedot tulisi myös säännöllisesti varmuuskopioida, jotta palvelinrikon tai tietokannan korruptoitumisen tapahtuessa tiedot voidaan helposti palauttaa. (Juvonen ym. 2023.)

Palvelimiin tulisi myös asentaa palomuuri. Palomuurilla tarkoitetaan järjestelmää, joka estää asiattoman pääsyn verkosta toiseen (Kotimaisten kielten keskus 2024). Palomuurin tulisi vastata palvelimen tyyppiä, joita ovat muun muassa käyttöjärjestelmätaso ja sovellustaso (Juvonen ym. 2023). Palomuurin luominen, operointi ja valvonta on resursseja vievä seikka, joka täytyy hoitaa erityisellä tarkkuudella, joten sen ulkoistaminen voi olla yritykselle hyödyllistä ja kustannustehokkaampaa kuin itse asian hoitaminen (Hermans 2022).

4.4 Päätelaitteiden tietoturvariskien hallinta

Päätelaitteisiin kuuluvat pöytätietokoneet, kannettavat tietokoneet, tabletit ja älypuhelimet. Päätelaitteisiin tulisi laittaa vahva salasana, laitteen lukitseva näytönsäästäjä ja palomuuriohjelmisto sekä säätää laitteiden käyttäjäprofiileiden käyttöoikeuksia eli esimerkiksi oikeus asentaa sovelluksia. Laitteista kannattaa myös poistaa kaikki tarpeettomat sovellukset. Laitteet tulisi myös säännöllisesti päivittää ja varmuuskopioida. (Juvonen ym. 2023.)

Suuri riski päätelaitteen turvallisuudelle ovat haittaohjelmat. Haittaohjelmalla tarkoitetaan ohjelmistoa, jonka tarkoitus on vahingoittaa tai hyödyntää laitetta, palvelua tai verkkoa. Haittaohjelman kautta laitteesta on mahdollista kerätä esimerkiksi henkilötietoja tai salasanoja ulkopuolisten käsiin. Haittaohjelmilta suojaudutaan käyttämällä antivirusohjelmaa, pitämällä sovellukset ja käyttöjärjestelmät ajan tasalla, käyttämällä palomuuria, tarkastamalla laitteen asetukset säännöllisesti ja välttämällä avoimia Wi-Fi-verkkoja. (F-Secure 2024; McAfee 2024.)

4.5 Sähköpostiviestintä

Tavallinen sähköposti ei ole turvallinen tiedonvälityksen muoto, sillä se kulkee verkossa selkokielisenä useiden palvelimien ja välityspalvelimien kautta ja siten kenen tahansa luettavissa. Tämän vuoksi tavallisella sähköpostilla ei kannata lähettää arkaluonteisia tietoja kuten salasanoja tai henkilötietoja, vaan niitä sisältävät sähköpostiviestit tulisi suojata salauksella. Sähköpostin salaus on yleisissä sähköpostiohjelmissa valmiina vaihtoehtona. (Data Group 2024b.)

Sähköpostin välityksellä saapuneisiin linkkeihin ja liitteisiin tulee suhtautua terveellä epäluulolla ja varmistaa tarkkaan sähköpostiosoitteen turvallisuus ja aitous ennen linkkien klikkaamista, sillä monet haittaohjelmia tai muita huijauksia sisältävät sähköpostit tulevat turvallisilta vaikuttavista osoitteista (Kyberturvallisuuskeskus 2020).

4.6 Dokumentointi ja ilmoittaminen

Täyttääkseen tietosuoja-asetuksen vaatiman osoitusvelvollisuuden, tulee yrityksen dokumentoida kaikki tietoturvatoimet ja henkilötietojen tietoturvaloukkaukset. Dokumentoinnilla varmistetaan, että tietosuoja on huomioitu yrityksen toiminnan suunnittelussa ja toteutuksessa ja että se on toiminut lain mukaan tietoturvaloukkauksen sattuessa.

Tietoturvan kannalta dokumentoinnissa tulisi olla kuvaus henkilötietojen suojaamisesta. Tämä voi olla kuvaus palomuureista, virustorjunnasta, henkilökohtaisista pääsyoikeuksista, yhtiön salassapito- ja salasanapolitiikasta, lokitiedoista sekä siitä, miten henkilöstön koulutus tietosuoja-asioista on suoritettu ja millaisin ohjein. Tietoturvaloukkauksiin

liittyen tulisi arvioida eri tietosuojaloukkaustilanteiden riskejä ja vaikutuksia rekisteröidyille. (Hanninen ym. 2017, 53.)

Dokumentaatiossa ei riitä, että sen tekee kerran yritystoiminnan alussa, vaan sitä on pidettävä ajan tasalla. Tietosuojakäytäntöjä ja niihin liittyviä asiakirjoja tulee päivittää aina kun siihen tulee tarve, esimerkiksi jos otetaan käyttöön uusi järjestelmä. (Hanninen ym. 2017, 53.)

Kun yritykselle joutuu tietoturvaloukkauksen kohteeksi, sen tulee suorittaa poikkeamaprosessi. Tietoturvaloukkaustapahtumien varalle tulisi olla kirjattu ylös dokumentointitapa, jotta tietoturvaloukkauksen havainnoidessa se osataan dokumentoida oikein. Dokumentoinnissa on oltava merkittynä mahdollisimman tarkka tietoturvaloukkaustapahtuman kuvaus, tapahtuma-aika, aika milloin asia saatiin tietoon, kuvaus riskin kohteeksi joutuneista henkilötiedoista, tapahtuman laajuus ja mahdollinen kuvaus jo tehdystä selvityksestä tai korjaavista toimenpiteistä. (Andreasson. & Ylipartanen 2022, 198.)

Tietoturvaloukkauksesta tulee tehdä myös riskiarvio, jossa on arvioitu sitä, aiheutuuko tietoturvaloukkauksesta todennäköisesti riskiä, joka kohdistuu luonnollisten henkilöiden oikeuksiin ja vapauksiin, ja jos aiheutuu, onko riski korkea. Tämän perusteella tulee arvioida se, tuleeko tietoturvaloukkauksesta ilmoittaa tietosuojavaltuutetulle. Jos ilmoitus tulee tehdä, se on tehtävä 72 tunnin kuluessa tapahtuneesta. Tämän lisäksi tulee arvioida, onko tietoturvaloukkauksesta aiheutuva riski niin korkea, että siitä tulisi ilmoittaa myös rekisteröidyille. Rekisteröidyille ei tarvitse ilmoittaa, jos yrityksessä on toteutettu asianmukaiset suojatoimenpiteet ja jatkotoimenpiteet, ja rekisteröidyille ilmoittaminen vaatisi kohtuutonta vaivaa esimerkiksi siksi, että ei tiedetä, keitä rekisteröidyt ovat. (Andreasson. & Ylipartanen 2022, 199–202.)

Näiden jälkeen tulee tehdä tietoturvaloukkauksen jälkiarviointi, jossa käydään läpi tehty dokumentaatio ja kehitetään tietoturvatoimia jatkoa varten. Lopuksi tietoturvaloukkaus tilastoidaan, jotta mahdollisia trendejä voidaan seurata ja riskit voidaan minimoida (Andreasson. & Ylipartanen 2022, 200.)

4.7 Tietosuojavastaava

Tietosuojavastaava on yrityksen sisäinen tietosuojan asiantuntija, jonka tehtävänä on seurata tietosuojasäännösten noudattamista. Tietosuojavastaava tuo esiin havaitsemiaan puutteita, neuvoo ja tiedottaa yrityksen johtoa tietosuojasäännösten mukaisista velvollisuuksista ja on yhteyshenkilönä tietosuojaa koskevissa asioissa yrityksen ulkopuolisille henkilöille. (Tietosuojavaltuutetun toimisto 2024f.)

Tietosuojavastaavana voi toimia yrityksen työntekijä tai esimerkiksi ulkoistettu yritys. Tietosuojavastaava on kuitenkin riippumaton taho yrityksestä, eli esimerkiksi henkilötietojen käytöstä päättävä henkilö tai yrityksen IT-johtaja ei voi toimia tietosuojavastaavana. Tietosuojavastaava ei myös ole vastuussa yrityksen tietosuojasta ja siihen liittyen velvollisuuksien noudattamisesta vaan tämä vastuu ja sen osoitus kuuluu kaikissa tapauksissa rekisterinpitäjälle eli yritykselle, sekä henkilötietojen käsittelijälle. (Hanninen ym. 2017, 121–123.)

Yrityksen tulee antaa tehtävän suorittamiseen tarvittavat riittävät resurssit tietosuojavastaavan käytettäväksi. Tietosuojavastaava tulee pitää mukana yrityksen tietosuojaasioiden suunnitteluun ja toteutukseen liittyvässä keskustelussa ja häntä on kuultava näitä koskevassa päätöksenteossa. Tietosuojavastaavalla tulisi olla myös pääsy henkilötietoihin ja niiden käsittelytoimeen sekä hänelle tulisi antaa mahdollisuus asiantuntemuksensa ylläpitämiseen esimerkiksi koulutusta tarjoamalla. (Hanninen ym. 2017, 122.)

Tietosuojavastaavalle ei ole tiettyjä vaatimuksia koulutuksesta tai kokemuksen määrästä, mutta hänen tulisi olla kuitenkin tuntea tietosuojalainsäädäntö ja -käytännöt hyvin sekä omata muutenkin valmiudet selviytyä hänelle määrätyistä tehtävistä. Nämä tehtävät voivat vaihdella paljonkin riippuen yrityksen toiminnan laadusta ja laajuudesta, eli sopivia edellytyksiä tulisi tarkastella tapauskohtaisesti. Kokemus tietosuoja-asioista olisi kuitenkin joka tapauksessa hyvä tietosuojavastaavalla olla. (Hanninen ym. 2017, 121.)

Tietosuoja-asetuksen 37 artiklan 1 kohdan mukaan yritykseltä edellytetään tietosuojavastaavan nimittämistä, jos yritys käsittelee arkaluontoisia tietoja, seuraa ihmisiä laajamittaisesti, säännöllisesti ja järjestelmällisesti tai jos yritys on julkishallinnon toimija (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679). Tietosuojavastaavan yhteystiedot tulee ilmoittaa tietosuojavaltuutetun toimistolle ja niiden tulee olla myös helposti yleisön saatavissa. Tietosuojavastaavan voi kuitenkin nimittää myös silloin, kun sitä ei vaadita. Tällöin pätevät samat vaatimukset koskien tietosuojavastaavan nimittämistä, asemaa ja tehtäviä kuin tietosuojavastaavan nimittämistä edellyttäessä. (Hanninen ym. 2017, 121; Tietosuojavaltuutetun toimisto 2024e.)

4.8 Tietoturvaseteli

Liikenne- ja viestintävirasto Traficom myöntää tietoturvan kehittämisen tukea eli tietoturvasetelin kahden vuoden ajan aikavälillä 1.12.2022 ja 31.12.2024 Suomeen rekisteröityneille yhteiskunnan toiminnan kannalta kriittisten alojen yrityksille parantaakseen tietoturvan tasoa. Tietoturvasetelin määräraha on 6 miljoonaa euroa ja sitä aiotaan jakaa, kunnes määrärahat ovat loppuneet tai aikaraja menee umpeen. Tietoturvaseteli

perustuu valtioneuvoston asetukseen tietoturvan kehittämisen tuesta 13.10.2022/860. (Kyberturvallisuuskeskus 2024.)

Tietoturvaseteliä voivat hakea ne yritykset, joilla on ollut toimintaa vuoden 2021 päättyneellä tilikaudella ja jotka täyttävät tietyt edellytykset. 15 000 euron tukea pystyy hakemaan, jos yritys on pieni tai keskisuuri, ja tukea haetaan tietojärjestelmien tarkastus- ja arviointityötä varten, tietoturvan parantamiseksi tehtävää hankintaa varten, henkilökunnan kouluttamista varten tai muuta osaamisen kehittämistä tai muuta vastaavaa yrityksen tietoturvallisuutta kehittävää toimea varten. Sen sijaan 100 000 euron tukea pystyy hakemaan, jos tukea haetaan hyökkäyksenestotestausta varten, tärkeimpien sähköisten palveluiden varautumistason testaamista varten tai näihin perustuvaan muuta välittömään tietoturvallisuutta parantavaa toimea varten. (Valtioneuvoston asetus tietoturvan kehittämisen tuesta 860/2022.)

Tietoturvaseteliä oli hakenut 12. toukokuuta 2024 mennessä 763 yritystä, joista 506 hakemusta oli loppuun käsitelty ja näistä 295 hyväksytty. Määrärahasta oli näille yrityksille annettu yhteensä 5,7 miljoonaa euroa, eli 95 % koko määrärahasta. (Kyberturvallisuuskeskus 2024.)

5 Kvalitatiivinen sisällönanalyysi

Tutkimusmenetelmäksi valitsin kvalitatiivisen sisällönanalyysin. Kvalitatiivisessa sisällönanalyysissä tutkitaan aineiston sisältöä sen sisältämien asioiden, aiheiden ja teemojen näkökulmasta. Tässä menetelmässä keskeistä on koodaus, jossa aineistosta tunnistetaan ja nimetään sisällöllisiä ominaisuuksia. Aineistoa vertaillaan sisäisesti ja siitä löydetään yhtäläisyyksiä ja eroavaisuuksia. (Vuori 2021.)

Sisällönanalyysin tavoitteena on luoda selkeä sanallinen kuvaus tutkitusta ilmiöstä. Aineistona voivat toimia miltei mikä tahansa kirjalliseen muotoon saatettu dokumentti. Näitä dokumentteja voivat olla esimerkiksi artikkelit, kirjat, haastattelu, puhe ja raportit. (Tuomi & Sarajärvi 2018.)

Kvalitatiivinen sisällönanalyysi on menetelmänä samankaltainen teemoittelun kanssa ja niitä monesti käytetään toisilleen vaihtoehtoisina nimityksinä (Vuori 2021). Teemoittelussa aineistosta eritellään ja ryhmitellään aihepiirit eli teemat tutkimusongelman mukaisesti. Aineistosta etsitään tällöin näkemyksiä, jotka kuvaavat tiettyjä teemoja. (Tuomi & Sarajärvi 2018.)

Aineistoksi valitsin dokumenttiaineiston. Dokumenttiaineisto sopii tutkimusaineistoksi silloin, kun tutkimuskohdetta ei kykene tutkimaan riittävästi esimerkiksi vain kyselyiden tai haastatteluiden avulla. Dokumenteilla tarkoitetaan kaikenlaisia ilmiötä dokumentoivaa aineistoa. Tätä aineistoa voivat olla arkistomateriaali, julkaistut tekstit, valokuvat ja kertomukset. (Anttila 2014.)

Dokumenttiaineiston voi jakaa primääri- ja sekundääriaineistoon. Primääriaineisto on suoraan alkuperäisestä lähteestä saatua tietoa, kuten esimerkiksi kirjeet, päiväkirjat ja yrityksen raportit. Sekundääriaineisto on esimerkiksi artikkeleita, kirjoja ja raportteja, joissa on toisen henkilön selostusta havainnoistaan, haastattelun tuloksista tai omista käsityksistään. Sekundäärilähteiden käytössä tulee pitää mielessä lähdekritiikki. (Alastalo & Vuori 2021; Anttila 2014.)

Tutkimuksen aineistona käytin uutissivustojen uutisartikkeleita. Dokumenttiaineistoni on sekundääristä. Uutissivustoiksi valitsin Yle Uutiset, Helsingin Sanomat ja MTV Uutiset, sillä Kunnallisalan kehittämissäätiön tutkimuksessa Ylen TV- ja radiouutiset, Helsingin Sanomat ja MTV3:n uutiset oli arvioitu yksiksi Suomen luotettavimmista uutislähteistä (Kunnallisalan kehittämissäätiö 2021). Tutkimuksessa ei ollut Yle Uutisia tai MTV Uutisia erikseen, minkä perusteella arvioin niiden luotettavuutta yhtiön perusteella.

Hain uutisia aikaväliltä 21.10.-2020–21.10.2023, sillä Vastaamon tietomurto tuli julkisuuteen 21.10.2020 ja tavoitteena oli tarkastella Vastaamon tietomurtotapauksen

jälkeistä keskustelua yritysten tietoturvan ympärillä sekä mahdollisia tietoturvaloukkaustapahtumia.

Uutissivustoilla käytin artikkelihaussa hakusanoja ”tietoturva”, ”yritys tietoturva”, ”tietomurto”, ”yritys tietosuoja”, ”kyberturvallisuus”, ”tietoturvaloukkaus” ja ”kyberhyökkäys”. Tuloksien kokonaismäärää on vaikea arvioida sen vuoksi, että hauissa tuli tuloksena myös samoja artikkeleita eri hakusanoilla. Yle Uutisten artikkelihaussa arvioin haun tuloksien kokonaismääräksi noin 1000, Helsingin Sanomien artikkelihaun tuloksien kokonaismääräksi noin 1500 ja MTV Uutisten artikkelihaun tuloksien kokonaismääräksi noin 500. Kriteerinä aineiston valinnassa käytin sitä, miten hyvin uutisartikkeli vastasi toiseen tutkimuskysymykseeni, ”Miten yritysten tietoturva ja mahdolliset tietomurrot ovat olleet esillä mediassa Vastaamon tietomurtotapauksen jälkeen?”. Tämän perusteella aineistoksi valikoitui artikkeleista ne, joissa käsiteltiin Suomessa esiintyneitä yritysten tietoturvaloukkauksia sekä suomalaisten yritysten tietoturvaan liittyä yritysten omia tai asiantuntijoiden lausuntoja. Aineistoksi valikoitui lopulta 40 uutisartikkelia (Liite 1).

Tämän lisäksi käytin aineistona Suomen yrittäjien suorittamaa Yrittäjägallupia, jossa selvitettiin pienten ja keskisuurten yritysten mielipiteitä ja näkemyksiä tietomurroista. Tutkimus toteutustapana oli tiedonkeruu, ja kyselyyn vastasi yhteensä 1049 pk-yrityksen edustajaa. Tutkimuksen tiedonkeruu tehtiin 9. – 15.2.2022 välisenä aikana ja tutkimuksen luottamusväli on kokonaistuloksen osalta +- 3,1 prosenttiyksikköä. (Suomen Yrittäjät 2022.)

Käsittelen aineiston siinä esiintyneiden teemojen perusteella. Teemoina ovat suomalaisyrityksiin kohdistuneet palvelunestohyökkäykset, suomalaisyrityksiin kohdistuneet tietomurrot, muut suomalaisyrityksiin kohdistuneet tietoturvaongelmat sekä asiantuntijoiden ja suomalaisyritysten yleisnäkemys suomalaisyritysten tietoturvan tasosta.

5.1 Palvelunestohyökkäyksiä

Suomalaisten yritysten palveluihin kohdistui useita palvelunestohyökkäyksiä vuosien 2022 ja 2023 aikana.

Vuoden 2022 helmi-maaliskuun vaihteessa tapahtui useita palvelunestohyökkäyksiä suomalaispankkeihin, jolloin näiden verkko- ja mobiilipankkien toiminta oli hidastunutta ja katkeilevaa. Yhteen hyökkäyksen kohteeseen, Nordeaan, tapahtunut hyökkäys oli poikkeuksellisen pitkäkestoinen ja vakava. (Laitinen 2022; Raeste 2022.)

Lokakuun ja joulukuun välillä vuonna 2022 Kyberturvallisuuskeskus sai huomattavan paljon ilmoituksia palvelunestohyökkäyksistä Suomessa. Tänä aikana uhreina olivat lokakuussa yksityisen sektorin toimijoista muun muassa Alma Media ja Uusi Suomi -julkaisu sekä useita finanssi- ja ICT-alan yrityksiä. Julkisen sektorin toimijoista uhreina

olivat olleet muun muassa Kansaneläkelaitos, terveydenhuollon Kanta-palvelu, Yle Areena -suoratoistopalvelu ja HSL-palvelut. Hyökkäys oli kohdistunut myös kouluissa käytössä olevan Wilma-järjestelmää ylläpitävän Visma-yhtiön konesalitoimittajaan. Eri palvelujen kokevat vahingot vaihtelivat pienistä käyttöhäiriöistä muutaman tunnin kestoisiin käyttökatkoihin. Kaikissa näissä tapauksissa kuitenkin vahingot jäivät minimaalisiksi. (Hurme 2022; Karhu 2022; Lukinmaa 2022; Pantzar 2022.)

Vuonna 2023 tapahtui Suomeen kohdistuvien palvelunestohyökkäysten piikki samoihin aikoihin kuin vuotta aiemmin, eli lokakuussa. Uhreina olivat muun muassa Turun Sanomat, Salon Seudun Sanomat, Aktia Pankki, varustamoyhtiö Viking Line, verkkosivut Yritystele, Rantapallo, A-Katsatus ja Expat-Finland sekä julkiselta sektorilta Verohallinto, Kybeturvallisuuskeskus ja Suomen Pankki. Hyökkäysten vaikutukset olivat olleet hyvin vähäiset. (Kallunki, Joukanen & Bogdanov 2023; Kossila & Bogdanov 2023; Lehtola 2023; STT 2023a.)

Palvelunestohyökkäykset eivät ole yleensä vaarallisia eikä useista niistä edes ilmoiteta, jos varsinaista vahinkoa ei ole tapahtunut. Yritysten ilmoituskynnys palvelunestohyökkäyksistä on saattanut kuitenkin madaltua, kun vertaa palvelunestoilmoitusten huomattavasti pienempään määrään syksyllä 2021. (Pantzar 2022.)

5.2 Yrityksiin kohdistuneita tietomurtoja

Suomalaisyrityksiin on kohdistunut useita tietomurtoja varsinkin vuoden 2022 aikana, mutta myös yksi suuri tietomurtotapaus vuonna 2023. Lisäksi oli yksi tietomurtotapaus vuodelta 2021.

Henkilöstöpalveluyritys Eilakaisla joutui kiristyshaittaohjelmahyökkäyksen kohteeksi tammikuussa 2021. Hyökkäyksen yhteydessä yhtiön palvelin lakkasi toimimasta, mutta henkilötietoja ei tietomurrossa vaarantunut. Eilakaisla ilmoitti asiasta asianmukaisesti tietosuojavaltuutetulle. (STT 2021a; STT 2021b.)

Konepajateollisuusyhtiö Wärtsilä havaitsi huhtikuussa 2022 verkkohyökkäyksen Voyage-liiketoimintayksikössään, joka kehittää laivaliikennettä ja satamien toimintaa. Hyökkääjä pääsi käsiksi Wärtsilän laskutuksessa ja ostoissa käyttämiin tietoihin ja dataa vietiin yhteensä kaksi terabittiä. Yhtiön mukaan tapahtuneen jälkeen aloitettiin asianmukaiset toimenpiteet nykyisten turvatoimien vahvistamiseksi ja tapauksen mahdollisen vaikutusten lieventämiseksi. Wärtsilä ilmoitti tietomurrosta asianmukaisesti tietosuojavaltuutetulle. (Parviala 2022.)

Savonia-ammattikorkeakouluun kohdistui tietoturvahyökkäys helmikuussa 2022. Tietoturvahyökkäyksen tekokeinona oli kiristysohjelma. Savonia ilmoitti alun perin, ettei opiskelijoiden henkilötietoja vuotanut, mutta myöhemmin Savonian opiskelijoiden

vuodettuja henkilötietoja, kuten nimiä ja henkilötunnuksia, löytyi pimeästä verkosta. Savonia oli ilmoittanut tietoturvahyökkäyksen tapahtuessa asiasta viranomaisille. (Parviala 2022; Rytkönen 2022.)

Uutistoimisto STT oli tietomurron kohteena heinäkuussa 2022, jolloin heidän tietojärjestelmäänsä kohdistui kiristysohjelmahyökkäys. Tietomurrossa hyökkääjä sai haltuunsa ainakin osoitetietoja ja henkilötunnuksia. STT:n mukaan se oli varautunut ennakkoon tietojärjestelmiin kohdistuvien hyökkäysten varalle. STT ilmoitti asiasta heti tietosuojavaltuutetulle sekä myöhemmin asianomaisille. (Rimpiläinen 2022; Strömberg 2022.)

Hissiyhtiö Koneeseen kohdistui verkkohyökkäys syyskuun lopussa 2022. Verkkohyökkäyksessä hyökkääjä murtautui tietojärjestelmään ja vei sieltä Koneen työntekijöiden työhön liittyviä dokumentteja. Dokumenteissa ei ollut arkaluonteisia tietoja. Koneen viestintäpäällikön mukaan tietomurto ei johtunut tietojärjestelmä haavoittuvuudesta vaan monivaiheisesta hyökkäyksestä ja että tietomurto saatiin pysäytettyä nopeasti ja haitat rajattua. Kone ilmoitti tietomurrosta tietosuoja-asetuksen mukaisesti tietosuojavaltuutetulle. (STT 2022; Hirvonen 2022.)

Lihanjalostusyritys Snellman joutui tietomurron kohteeksi lokakuussa 2022. Yhtiön tuottajien tietojärjestelmän tietovuodon huomasi ulkopuolinen palveluntarjoaja, jonka serverillä järjestelmä pyöri. Tietomurrossa vuotaneen tiedon määrä oli hyvin vähäinen eikä sen mukana ollut henkilötietoja. Snellman ilmoitti asiasta tietosuojavaltuutetulle ja tuottajille, joiden tietoja oli mahdollisesti vuotanut. (Björklund & Tekoniemi 2022; Kuivasmäki 2022.)

Talotekniikkayhtiö Uponoriin kohdistui kiristysohjelmahyökkäys ja tietomurto marraskuussa 2022. Tietomurrossa vuosi Uponorin työntekijöiden, asiakkaiden ja kumppanien tietoja. Uponor kertoi hyökkäyksen jälkeen tehneensä välittömät toimet selvittääkseen ja korjatakseen tilanteen. Yhtiö ilmoitti asiasta asianmukaisesti tietotuojavaltuutetulle. (Kukkonen 2022a; Kukkonen 2022b; STT 2022.)

Inkontinenssi- ja diabeteshoitotuotteita kuljettava logistiikka-alan yritys Westlog Oy joutui tietomurron kohteeksi elokuussa 2023. Tietomurrossa yhtiön tilausjärjestelmästä oli ladattu suuri määrä asiakkaiden henkilötietoja. Palvelimelle oli myös jätetty kiristysviesti. Henkilötietoihin kuuluivat asiakkaiden nimet, yhteistiedot, tiedot tehdyistä tilauksista ja osalla myös henkilötunnus. Tietomurron tullessa ilmi palvelimen ylläpitäjä sammutti palvelimen. Tietovuoto kosketti kokonaisuudessaan yli 116 000 henkilöä. Westlog Oy ilmoitti asiasta tietosuoja-asetuksen mukaisesti tietosuojavaltuutetulle. (Pukkila 2023; Uhari 2022.)

5.3 Muita yrityksiin kohdistuneita tietoturvaongelmia

Myös muita tietoturvaongelmia kuin suomalaisyrityksiin suoraan kohdistuneita tietomurtoja esiintyi. Sen lisäksi oli useita tietojenkalastelutapauksia ja järjestelmän tietoturvan heikkous.

Maaliskuussa 2021 Microsoftin Exchange -palvelimeen kohdistui tietomurto, jonka seurauksena kymmeniin suomalaisyritysten tietojärjestelmiin oli päästy. (STT-YLE 2021.)

Osuuspankin verkkosivuihin kohdistui kyberhyökkäys tammikuussa 2022. Hyökkäyksen seurauksena yhtiön verkkosivusto oli toimintahäiriöinen usean tunnin ajan. Yhtiö otti asian heti tutkintaan, eikä hyökkäyksessä vaarantunut asiakkaiden tietoja. (Karhu & STT 2022.)

Helmikuussa 2022 useiden suomalaisten hotellien käyttämään teknologiayritys Sabren hotellivarausjärjestelmään kohdistui tietomurto. Varausjärjestelmää käytti ainakin kaksi Nordic Choice Hotels -ketjun hotellia sekä kolme muuta hotellia Suomessa. Tietovuodon kohteena olivat sisäänkirjautumistiedot, joita olivat muun muassa nimi, osoite, puhelinnumero ja sähköposti. Yhteensä yli 20 000 asiakkaan tiedot vuosivat tietovuodossa. Nordic Choice Hotels -ketjun hotellit ilmoittivat asiasta tietosuojavaltuutetulle. (Loula 2022; Seppälä 2022.)

Pankkiyhtiö S-Pankin verkkopankissa oli tietoturvaongelma huhtikuun ja elokuun välisenä aikana vuonna 2022. Tietoturvaongelman aikana osa asiakkaista oli pystynyt kirjautumaan toisten asiakkaiden verkkopankkitileille ja tekemään väärinkäytöksiä. Tietoturvaongelman aiheuttaja oli ohjelmistossa ollut virhetoiminta. Pankki ei itse huomannut ongelmaa, vaan siitä kertoi heille ulkopuolinen henkilö. S-Pankki teki ilmoituksen viranomaisille saatuaan tiedon asiasta. (Näveri & Uusitalo 2022.)

Maaliskuussa 2023 tiedotettiin, ettei useiden suomalaisten laboratorioiden käyttämän, ohjelmistoyritys Mylab Oy:n luoman tietojärjestelmän tietoturva vastaa sosiaali- ja terveysalan lupa- ja valvontavirasto Valviran vaatimuksia. Mylab ilmoitti tähän korjaavansa puutteet. (Hankaniemi 2022.)

Lokakuussa 2023 uutisoitiin tietomurtoaallosta, jossa useiden suomalaisten organisaatioiden sähköpostitileille oli murtauduttu. Sähköpostitunnuksia ja salasanoja oli saatu sähköpostitse huijauksen kohteena olevien sähköpostien kautta sekä ja huijaussivujen avulla. (STT 2023b.)

Pienten yritysten kokemat huijaus- ja sometilikaappausteot oli olleet myös uutisoinnissa esillä. Esimerkiksi vaatesuunnittelijan Instagram-tili oli kaapattu hänen laitettuaan tilin tiedot linkissä olleeseen hämäävään lomakkeeseen, autoyrittäjän puhelin sekosi

viestillä tullutta linkkiä klikattuaan ja donitsikahvilan Facebook-tilille oli päästy kirjautumaan siellä olleen vanhan sähköpostin takia ja käyttämään yrityksen rahoja Facebook-markkinointiin. (Ikävalko 2022a; Mäkelä 2023; Möller & Paavola 2021.)

5.4 Tietoturvan taso Suomessa

Psykoterapiakeskus Vastaamon tietomurtotapauksen seurauksena sosiaali- ja terveysalan tietoturva nousi pinnalle. Sosiaali- ja terveydenhuoltopalveluita tuottavan yrityksen Pihlajalinnan toimitusjohtaja kertoi sotealan olevan hyvin keskittynyt tietojärjestelmien käytössä eli suurta määrää operatiivisia järjestelmiä ei ole ja näillä vakiintuneilla järjestelmillä tietoturva oli kunnossa. (Jaskari 2020.)

Vastaamon tietomurtotapauksen seurauksena oli myös tietoturvayhtiöissä lisääntyneet yhteydenotot ja verkkosivujen kävijämäärät. Yhteydenottoja tuli erityisesti sairaanhoitopiireiltä sekä pieniltä ja keskisuurilta yrityksiltä. Tietoturvayritys SSH Communications Securityn talousjohtajan mukaan Vastaamon tietoturvakriisi nosti tietoturvan ajantasaisuuden varmistamisen välttämättömästä pahasta yritysten ylimmän johdon tärkeisiin asioihin. Tietoturvayhtiö Nixu sai lisääntyneitä kyselyitä pienistä ja keskisuurista yrityksistä, ja sen mukaan suuremmat yhtiöt ovat johtaneet tietoturvallisuuttaan järjestelmällisemmin jo pitkään. (Keski-Heikkilä 2020.)

Liikenne- ja viestintävirasto Traficomin webinaarissa lokakuussa 2020 eri aloilla sanottiin olevan kyberturvallisuuden tasossa eroja: finanssialalla se oli hallussa, mutta varsinkin media- ja energiatarvikealalla se oli kehityksen alla. (Heiskanen 2020.)

Poliisiammattikorkeakoulun tutkijan Anna Leppäsen mukaan kyberrikoksista ilmoitetaan heikosti. Syyksi hän antoi mahdollisen maineriskin, rikostutkinnan synnyttämän yrityksen kuormittamisen ja sen, ettei poliisin luoteta saamaan kiinni ulkomailla toimivaa rikollista. (Huhtanen 2021.)

Elokuussa 2022 uutistoimisto STT:n ja konepajayhtiö Wärtsilän tietomurtojen yhteydessä aiheeksi nousi yritysmaailman kyberturvallisuus. Loihde Trust -yhtiön kybertiedustelun johtajan, tietoturva-asiantuntijan Benjamin Särkän mukaan tietomurtojen yleisyyden tarkasteleminen on vaikeaa sen vuoksi, etteivät kyberhyökkäysten kohteeksi joutuneet yritykset usein ilmoita asiasta esimerkiksi liikenne- ja viestintävirasto Traficomille. (Ikävalko 2022b.)

Vuoden 2023 helmikuussa Jyväskylässä järjestetyn kyberturvaharjoituksen yhteydessä haastatellun Traficomin kyberturvallisuusjohtaja Rauli Paanasen mukaan suomalaisten kyberhäirinnän varautumisen tasosta kertoo se, kuinka vähän havaittu kyberhäirintä lopulta näkyy julkisuudessa. Hänen mukaansa kyberturvaosaajien tarve on kuitenkin noussut ja että ala koulutetuista ammattilaisista on huutava pula. (Hytönen 2023.)

Suomen yrittäjät ry:n tuottaman Yrittäjägallup-kyselyn mukaan 84 % vastanneista yrityksistä kertoivat, etteivät ne olleet joutuneet tietomurron kohteeksi, kun taas 9 % kertoi joutuneensa tietomurron kohteeksi. Tietomurron tapahtuessa 59 % yrityksistä kertoi tietävänsä kuinka tulisi toimia ja 25 % kertoi, ettei tiedä. Tietoturvan tärkeydestä 58 % sanoi sen olevan erittäin tärkeää, 31 % melko tärkeää, 8 % vähän tärkeää ja 2 % ei lainkaan tärkeää. Yleiseksi arvioksi oman yrityksen tietoturvan tasosta 15 % yrityksistä arvioi sen erinomaiseksi, 56 % hyväksi, 23 % tyydyttäväksi, 3 % välttäväksi ja 1 % huonoksi. Mahdollisen tietomurron aiheuttamasta riskistä yrityksen liiketoiminnalle 8 % vastanneista kertoi riskin olevan suuri, 26 % kertoi riskin olevan melko suuri, 55 % kertoi riskin olevan vähäinen ja 7 % mukaan riskiä ei ollut lainkaan. Yrityksen tietoturvan toteuttamisen estämisen tekijöiksi 35 % vastanneista antoi osaamisen puutteen, 22 % tietoturvan kustannukset, 18 % ajan puutteen, 11 % digitaalisten ratkaisujen tietoturvan puutteen, 4 % digitaalisten ratkaisujen puutteen ja 4 % jonkun muun syyn. 39 % vastanneista yrityksistä kertoi, ettei tietoturvan toteutumiselle ollut esteitä. (Suomen Yrittäjät 2022.)

5.5 Johtopäätökset

Suomessa on ollut paljon palvelunestohyökkäyksiä ja nämä hyökkäykset keskittyivät samoihin aikoihin useisiin yrityksiin. Palvelunestohyökkäykset ovat useimmiten suhteellisen vaarattomia ja niistä ei usein ilmoiteta, joten niiden laaja esiintyminen mediassa on suurimmalta osin siksi, että yritykset ovat halunneet ilmoittaa palveluidensa käyttäjille palvelun käyttöongelmista palvelunestohyökkäyksen aikana.

Yrityksiin kohdistui useita tietomurtoja. Yleiset tietomurtojen tekotavat olivat verkkohyökkäys ja kiristysohjelmahyökkäys. Nämä tietomurrot vaihtelivat vakavuuden tason mukaan: osassa tietomurroista joko mitään tietoja ei viety tai viedyt tiedot eivät olleet henkilötietoja. Tämä kertoo siitä, että näissä yrityksissä oli osattu suorittaa tietoturvatoimet joko erittäin hyvin tai ainakin melko hyvin, sillä tärkeimmät tiedot oli turvattu riittävästi. Osassa tietomurtotapauksista kuitenkin myös vietiin henkilötietoja, joista osa olivat myös arkaluonteisia.

Tietomurtojen lisäksi yrityksillä esiintyi muita tietoturvaongelmia. Osa tietoturvaongelmista johtui siitä, että suomalaisyrityksen käyttämään palveluun oli tehty tietomurto, minkä vuoksi myös yrityksen tietoturva oli vaarantunut. Näissä tapauksissa tietoturvan pettäminen ei siis ollut suoranaisesti yrityksen omalla vastuulla. Sähköpostien ja muun viestien kautta tehdyt tietojenkalasteluhuijaukset olivat myös esillä jonkin verran. Tämän lisäksi esiintyi yrityksen palvelun ohjelmistossa ollut virhetoiminta, jonka seurauksena asiakkaat olivat päässeet muiden asiakkaiden tileille.

Tietomurtojen määrää on vaikea arvioida, sillä kaikista tietomurroista ei ilmoiteta viranomaisille monien syiden takia, joita ovat muun muassa mahdollinen maineriski ja rikostutkinnan synnyttämä yrityksen kuormittaminen. Toisaalta kuitenkin myös mainittiin se, että mediassa näkyvän kyberhäirinnän vähäisyys on merkki suomalaisten valmistautumisesta.

Vastaamon tietomurtotapauksen jälkeen yrityksiä oli kiinnostanut heidän tietoturvansa taso, ja he olivat täten lisääntyvissä määrin ottaneet yhteyttä tietoturvayhtiöihin. Yrittäjät ry:n kyselyssä yrityksistä reilu puolet kertoivat kokevansa tietoturvan erittäin tärkeäksi ja oman yrityksensä tietoturvan tason hyväksi.

6 Pohdinta

Vastaamon tietomurtotapauksen jälkeen on tapahtunut useita tietoturvaloukkauksia. Niiden vakavuuden taso on vaihdellut: osa on ollut hetkellisiä palvelun käyttöhäiriöitä ja osa henkilötietoja vuotaneita tietovuotoja.

Osassa tapauksissa on myös nähtävissä yhtäläisyyksiä Vastaamon tietomurtoon. Westlog Oy:n tietovuoto on laajuudeltaan suurempi kuin Vastaamon tietovuoto, mutta toisin kuin Vastaamon kohdalla, Westlogilta vuodettuna tietoja ei löytynyt verkosta kenen tahansa saatavana. Sen sijaan Savonia-ammattikorkeakoulun vuotaneita tietoja oli löytynyt pimeästä verkosta ja joukossa oli ollut myös henkilötietoja. Datan suuressa määrässä Vastaamon tapausta vastaava oli myös Wärtsilän tietomurto, jossa tietoa vuosi peräti 2 terabitin verran.

Palvelunestohyökkäykset ovat erittäin yleisiä ja niitä raportoidaan tapahtuneeksi vuosittain yli 10 000 tapausta (Kyberturvallisuuskeskus 2022). Tämän yleisimmän verkkohyökkäyksen muodon hoitaminen kuntoon onnistui suomalaisyrityksillä hyvin. Useimmilla palvelut olivat alhaalla vain tuntien ajan ja lopuilla päivien ajan.

Eri aloilla myös mainittiin olevan tietoturvassa eroja. Aloilla, joilla tietoturva on elintärkeää liiketoiminnan kannalta, kuten finanssialalla, tietoturva on otettu jo pitkään erittäin vakavasti, mutta aloilla, joilla tietoturva voidaan nähdä vain ”välttämättömänä pahana”, on siinä vielä kehittämisen varaa. Vastaamon tietomurto herätti erityisesti sosiaali- ja terveysalan yritykset huolehtimaan tietoturvansa tasosta, sillä tämän tietomurron ollessa omalla alalla he näkivät heikon tietoturvan todellisen vaikutuksen.

Tietosuoja-asetuksessa olevan ilmoitusvelvollisuuden tuntuvat yritykset osaavan. Ilmoitusvelvollisuus koskee vain sellaisia tietoturvatapauksia, joissa luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuu riski, mistä voi päätellä aineistosta siten jääneen pois monet sellaiset tietoturvaloukkaukset, joissa riskiä ei kohdistunut eikä yritys kokenut tarpeelliseksi ilmoittaa asiasta. Ei ole myös tietoa siitä, kuinka moni ilmoitusvelvollisuuden alainen tietoturvaloukkaus jää ilmoittamatta, eli tästä on vaikea tehdä lopullisia johtopäätöksiä.

Yleisesti ottaen tietoturva vaikuttaa olevan Vastaamon tapauksen jälkeen Suomessa kohtalaisella tasolla. Vastaamon tietomurron kaltaisia tapauksia on ollut useita: yritysten tietojärjestelmiin on hyökätty ja tietoja on viety. Tästä katsauksesta kuitenkin puuttuvat ne kaikki monet yritykset, joihin ei ole kohdistunut tietomurtoja. Tämä on tietenkin siitä selkeästä syystä, ettei onnistuneista tietoturvatoimista uutisoida ainakaan yhtä paljon kuin tietomurroista. Lopullisia johtopäätöksiä on siis tästä vaikea tehdä.

Moni yritys ei ole vielä kokenut tietomurtoja eivätkä he koe mahdollisen tietomurron riskejä suuriksi, mikä yhdistelmänä voi saada osan yrityksistä olemaan keskittymättä tietoturvaan erityisen tarkasti. Parannettavaa tietoturvan osalta löytyy monista kohdista, ja yritykset sen itsekin tiedostavat ja tahtovat parannusta asiaan, mutta esteeksi nousee pula tietoturvan osaajista ja tietoturvan parantamisen kustannukset. Tähän vastauksena Suomen valtio onkin tarjonnut taloudellista tukea tietoturvan parantamiseen.

Vastauksena tutkimuskysymykseeni koskien mediassa esiintynyttä yritysten tietoturvaan ja mahdollisia tietomurtoja, voidaan sanoa yritysten tietoturvan olleen esillä mediassa melko paljon ja kohteena on tietenkin ollut niihin kohdistuneet tietomurrot ja muut tietoturvaloukkaukset ja -ongelmat. Tietoturvan onnistuminen on ollut esillä vähemmän moninaisista syistä, joista yksi on se, että aiheeseen kiinnitetään kunnolla huomiota vain silloin kun se ei ole toiminut.

Kaiken kaikkiaan Vastaamon tapaus toimi kuitenkin säikähdyksenä monille yrityksille tietoturvan tärkeydestä ja miten tietoturvaa ei tulisi suorittaa.

6.1 Yhteenveto

Tämän opinnäytetyön tuloksena syntyi katsaus suomalaisten yritysten tietoturvan ja valmistautumisen tasoon kyberhyökkäyksiä vastaan. Tietoturva on tärkeä aihe verkkoon muuttavassa maailmassa ja kyberhyökkäysten keinojen tehostuessa. Tämä opinnäytetyö antaa katsauksen tietoturvaan liittyvään lainsäädäntöön Vastaamon tietomurtotapauksen kautta sekä tarkastelee ammattikirjallisuuden avulla sitä, miten tietoturvatoimet voi suorittaa hyvin. Tämän tutkimuksen aineisto on kerätty luotettavimmiksi arvioiduilta uutissivustoilta ja Suomen yrittäjien järjestön kyselytutkimuksesta. Jatkotutkimuksena voisi tutkia eri tietosuoja-asetuksen kohtien toteutusta yrityksissä vielä tarkemmin esimerkiksi tekemällä kyselyn suoraan yrityksiin aiheesta.

6.2 Opinnäyteprosessi ja oman oppimisen arviointi

Opinnäyteprosessi oli minulle vaikea, sillä sekä aiheen keksiminen että opinnäytetyön työstäminen olivat minulle vaikeita, sillä tein sitä lopulta tiukalla aikataululla. Aikataulussa haasteiksi muodostuivat omat väärät arviot eri osuuksien laajuudesta ja teon kestosta sekä oma viivyttely sen vuoksi, että osassa osuuksia oli hankaluuksia tietää, mistä aloittaa. Tutkimusmenetelmäksi valikoitui sisällönanalyysi dokumenttiaineiston avulla. Dokumenttiaineistoa oli luontevaa hakea ja valikoida, sillä minulla oli tarkka näkökulma sen tarkoitukseen tutkimuskysymyksien avulla.

Nyt jälkeenpäin tehtynä olisin valinnut tutkimusmenetelmäksi tai sisällönanalyysin lisäksi haastattelun tai kyselytutkimuksen, jossa olisin suoraan kysynyt valikoiduilta yrityksiltä heidän tietoturvansa tasosta. Tämän menetelmän avulla saisi tietoa yritysten

tietoturvasta suoraan juuri Vastaamon tietomurtotapaukseen liittyen. Tiukan aikataulun vuoksi en kuitenkaan olisi nyt ehtinyt suorittamaan sopivan kattavia kyselyitä tai haastatteluita, vaikka ne olisivatkin ehkä sopineet tämänkaltaiseen tutkimukseen paremmin.

Aiheesta löytyi hyvin ammattikirjallisuutta eri näkökulmista, mikä auttoi aiheen prosessoimisessa. Tämän opinnäytetyöprosessin aikana tietoturvan moninaisuus ja tärkeys avautuivat minulle, minkä avulla olen saanut syvemmän tietämyksen aiheesta.

Lähteet

Alastalo M. & Vuori J. 2021. Dokumentit. Laadullisen tutkimuksen verkkokäsikirja. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/dokumentit/. Luettu: 29.4.2024.

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). Tietosanoma. Helsinki.

Anttila, P. 2014. Tutkimisen taito ja tiedon hankinta. Metodix. Luettavissa: metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/. Luettu: 29.4.2024.

Data Group 2024a. Kuinka yrityksen tietoturvaa parannetaan? Luettavissa: https://www.datagroup.fi/tietoturva. Luettu: 21.4.2024.

Data Group 2024b. Salattu sähköposti – Miksi sähköposti pitää salata ja miten se tehdään? Luettavissa: https://www.datagroup.fi/ajankohtaista/salattu-sahkoposti-miksi-sahkoposti-pitaa-salata-ja-miten-se-tehdaan. Luettu: 21.4.2024.

Euroopan komissio 2024a. Mikä on tietoturvaloukkaus ja miten sellaisen sattuessa pitää toimia? Luettavissa: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fi. Luettu: 20.3.2024.

Euroopan komissio 2024b. Mitkä henkilötiedot katsotaan arkaluonteisiksi? Luettavissa: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_fi. Luettu: 19.3.2024

Euroopan komissio 2024c. Mitkä tiedot ovat henkilötietoja? Luettavissa: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_fi. Luettu: 19.3.2024.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

F-Secure 2024. Mikä on haittaohjelma? Luettavissa: https://www.f-secure.com/fi/articles/what-is-malware. Luettu: 21.4.2024.

Hanninen, M., Laine, E., Rantala K., Rusi, M. & Varhela M. 2017. Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset. Helsingin seudun kauppakamari. Vantaa.

Hermans, J. 2022. Miten ulkoistaa yrityksen IT-palvelut – ja 5 syytä miksi se kannattaa. Rauhala. Luettavissa: https://www.rauhala.fi/blog/miten-ulkoistaa-yrityksen-it-palvelut-ja-5-syyta-miksi-se-kannattaa. Luettu: 21.4.2024.

Hyppönen, M. 2021. Internet. WSOY. Helsinki.

Hämäläinen, V. 2021. Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä – tietoturva-asiantuntija: "Älyvapaata". Yle Uutiset. Luettavissa: https://yle.fi/a/3-11750220. Luettu: 25.3.2024.

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

Järvinen, P. 2022. Yrityksen tietoturvaopas. Helsingin seudun kauppakamari. Helsinki.

Keller, M. 2023. Mitä on tietosuoja? Alma Talent. Helsinki.

Kotimaisten kielten keskus 2024. Palomuuri. Luettavissa: https://www.kielitoimistonsanakirja.fi/#/palomuuri. Luettu: 21.4.2024.

Kuluttajaliitto 2024. Yhteiskuntavastuu – Vastuullinen kuluttaminen. Luettavissa: https://www.kuluttajaliitto.fi/materiaalit/yhteiskuntavastuu/. Luettu: 12.5.2024

Kunnallisalan kehittämissäätiö 2021. Ylen ja STT:n uutisointiin luotetaan eniten. Kunnallisalan kehittämissäätiö. Luettavissa: https://kaks.fi/uutiset/ylen-ja-sttn-uutisointiin-luotetaan-eniten/. Luettu: 30.4.2024.

Kyberturvallisuuskeskus 2024. Hae tietoturvan kehittämisen tukea. Luettavissa. https://www.kyberturvallisuuskeskus.fi/fi/hae-tietoturvan-kehittamisen-tukea. Luettu: 12.5.2024.

Kyberturvallisuuskeskus 2020. Pienyritysten kyberturvallisuusopas. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. Luettu: 21.4.2024.

Kyberturvallisuuskeskus 2022. Toimintaohje –Palvelunestohyökkäys. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/PalvelunestohyökkäysToimintaohje.pdf. Luettu: 28.4.2924.

Länsi-Uudenmaan käräjäoikeus 2024. 24/119144. Tuomiolauselma.

McAfee 2024. Mikä on haittaohjelma? Luettavissa: https://www.mcafee.com/fi-fi/antivirus/malware.html. Luettu: 21.4.2024.

Mäntysalo, J, & Salumäki, T. 2023. Ehdolliseen vankeuteen tuomittu Ville Tapio pyytää anteeksi Vastaamon tietomurron uhreilta: ”Olen todella pahoillani”. Yle-Uutiset.Luettavissa: https://yle.fi/a/74-20027598. Luettu: 2.5.2024.

National Institute of Standards and Technology 2024. Root user. Luettavissa: https://csrc.nist.gov/glossary/term/root_user. Luettu: 7.4.2024.

Poliisi 2024. Tietomurrot. Luettavissa: https://poliisi.fi/tietomurrot. Luettu: 20.3.2024.

Rimpiläinen, T. 2023. Vastaamon Malmin toimipisteessä luotiin vuonna 2012 työasemille salasana ”malmi70” – sitten sitä käytettiin kaikkialla vuosien ajan. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20020562. Luettu: 25.3.2024.

Tietosuojavaltuutettu 2021. Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen. Luettavissa: https://finlex.fi/fi/viranomaiset/tsv/2021/20211183. Luettu: 7.4.2024.

Tietosuojavaltuutetun toimisto 2024a. Henkilötietojen käsittelyn roolit ja vastuut tieteellisessä tutkimuksessa. Luettavissa: https://tietosuoja.fi/henkilotietojen-kasittelyn-roolit-ja-vastuut. Luettu: 19.3.2024.

Tietosuojavaltuutetun toimisto 2024b. Henkilötietojen käsittely. Luettavissa: https://tietosuoja.fi/henkilotietojen-kasittely. Luettu: 19.3.2024.

Tietosuojavaltuutetun toimisto 2024c. Mikä on henkilötieto? Luettavissa: https://tietosuoja.fi/mika-on-henkilotieto. Luettu: 19.3.2024.

Tietosuojavaltuutetun toimisto 2024d. Osoita noudattavasi tietosuojasäännöksiä. Luettavissa: https://tietosuoja.fi/osoitusvelvollisuus. Luettu: 1.4.2024

Tietosuojavaltuutetun toimisto 2024e. Tietosuojavastaavan nimittäminen. Luettavissa: https://tietosuoja.fi/tietosuojavastaavan-nimittaminen. Luettu: 16.4.2024.

Tietosuojavaltuutetun toimisto 2024f. Tietosuojavastaavat. Luettavissa: https://tietosuoja.fi/tietosuojavastaavat. Luettu: 16.4.2024.

Tietosuojavaltuutetun toimisto 2024g. Tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietoturvaloukkaukset. Luettu: 20.3.2024.

Tietosuojavaltuutetun toimisto 2024h. Tietosuoja. Luettavissa: https://tietosuoja.fi/tietosuoja. Luettu: 9.5.2024.

Tietosuojavaltuutetun toimisto 2024i. Tunne oikeutesi. Luettavissa: https://tietosuoja.fi/tietosuoja/tunne-oikeutesi. Luettu: 9.5.2024.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi. Helsinki.

Valtioneuvoston asetus tietoturvan kehittämisen tuesta 13.10.2022/860.

Vuori, J. 2021. Laadullinen sisällönanalyysi. Laadullisen tutkimuksen verkkokäsikirja. Luettavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/laadullinen-sisallonanalyysi/. Luettu: 12.5.2024.

Liite 1

Björklund S. & Tekoniemi S. 2022. Lihanjalostusyhtiö Snellman joutunut tietomurron kohteeksi – jopa tuhansien sopimustuottajien henkilötietoja voinut päätyä vääriin käsiin. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20003459. Luettu: 28.4.2024.

Hankaniemi, A. 2023. Useiden suomalaisten laboratorioiden tietojärjestelmä ei vastaa lakia – Valvira määräsi tamperelaisyritykselle 500 000 euron uhkasakon. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20021140. Luettu: 28.4.2024.

Heiskanen R. 2020. ”Maailma on paljon pahempi paikka kuin kuvitellaan” – osa yrityksistä on huomioinut kyberturvallisuuden hyvin, mutta osa kehittää sitä vasta nyt, sanoo asiantuntija. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000006701488.html. Luettu: 28.4.2024.

Huhtanen, J. 2021. Kyberrikoksista ilmoitetaan tutkijan mukaan heikosti poliisille – Uusi opas neuvoo yrityksiä tekemään kyberrikoksista poliisiasian matalalla kynnyksellä. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000007884172.html. Luettu: 28.4.2024.

Hurme, A. 2022. Sähköiset reseptit eivät toimi kaikkialla – syynä Kelaan ja Kantaan kohdistuva palvelunestohyökkäys. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20008024. Luettu: 28.4.2024.

Hytönen, T. 2023. Kyberturvaa harjoitellaan ennätyksellisen ahkerasti – alan asiantuntijoista on käynnissä kova kansainvälinen kilpailu. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20016760. Luettu: 28.4.2024.

Ikävalko, K. 2022a. Anni Ruuth avasi Instagramiin tulleen linkin, ja tili oli kaapattu sekunneissa – yksinäisenkin yrittäjän on muistettava somen turvatoimet. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12570551. Luettu: 28.4.2024.

Ikävalko, K. 2022b. Lunnaiden maksu rikollisille voi olla välttämätöntä tietomurroissa – tietoturva-asiantuntija: Toinen vaihtoehto on konkurssi. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12573399, Luettu: 28.4.2024.

Jaskari, K. 2020. Sote-alalla on huolta siitä, miten pienet yritykset kestävät tietoturvan parantamisen kustannukset – valtiolta toivotaan tukea. Yle Uutiset. Luettavissa: https://yle.fi/a/3-11646290. Luettu: 2024.

Kallunki E., Joukanen T. & Bogdanov J. 2023. Verohallintoon ja Aktiaan kohdistuu palvelunestohyökkäys. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20054676. Luettu: 28.4.2024.

Karhu, O. 2022. HSL:n digipalveluissa häiriöitä, maksaminen hidastuu – ongelmaa ei saada suljettua pois. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20008542. Luettu: 28.4.2024.

Karhu, O. & STT 2022. Osuuspankin verkkosivut joutuivat kyberhyökkäyksen kohteeksi – verkkopalvelun häiriö kesti useita tunteja. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12263337. Luettu: 28.4.2024.

Keski-Heikkilä, A. 2020. Vastaamon tietomurto sai sairaanhoitopiirit ja keskisuuret yritykset valpastumaan: Näin tapaus on näkynyt tietoturvayhtiöissä. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000007606598.html. Luettu: 28.4.2024.

Kossila E. & Bogdanov J. 2023. Turun Sanomat ja useita muita verkkosivuja palvelunestohyökkäyksen kohteena – venäläinen hakkeriryhmä väittää olevansa iskun takana. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20053721. Luettu: 28.4.2024.

Kuivasmäki 2022. Snellmanin tietomurrosta selvittiin säikähdyksellä – henkilötietoja ei ole vuotanut eikä päätynyt vääriin käsiin. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20007831. Luettu: 28.4.2024.

Kukkonen, L. 2022a. Uponor joutui kyber-hyökkäyksen kohteeksi. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000009183972.html. Luettu: 28.4.2024.

Kukkonen L. 2022b. Uponorin tuotanto keskeytyi kyber-hyökkäyksen takia, antoi tulos-varoituksen. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000009214984.html. Luettu: 28.4.2024.

Laitinen, J. 2022. Muutama suomalaispankki on joutunut kyberiskun kohteeksi Venäjän aloittaman sodan jälkeen – Nordea on yksi uhriksi joutuneista pankeista. Luettavissa. https://www.hs.fi/talous/art-2000008682691.html. Helsingin Sanomat. Luettu: 28.4.2024.

Lehtola, J. 2023. Useisiin varustamoihin kohdistuu palvelunestohyökkäys ympäri Eurooppaa – myös Viking Linen sivut kohteena. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20056204. Luettu: 28.4.2024.

Loula, P. 2022. Noin 20 000 asiakkaan varaustiedot vuosivat kahdesta suomalais-hotellista – poliisi aloitti tietomurtotutkinnan. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000008774004.html. Luettu: 28.4.2024.

Lukinmaa, T. 2022. Koulujen Wilma-järjestelmässä oli aamulla käyttökatkoja eri puolilla maata – syynä palvelunestohyökkäys. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20009745. Luettu: 28.4.2024.

Mäkelä, E. 2023. Donitsi-kahvila joutui liriin: joku kaappasi Facebook-sivun ja pääsi käsiksi yrityksen rahoihin. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kaupunki/helsinki/art-2000009720394.html. Luettu: 28.4.2024.

Möller S. & Paavola, R. 2021. Yrittäjä lankesi huijausviestiin ja sai jopa uhkaavia viestejä – "Vähän jännittää, kun siitä niin kiivastuttiin". Yle Uutiset. Luettavissa: https://yle.fi/a/3-12209385. Luettu: 28.4.2024.

Näveri, A. & Uusitalo, K. 2022. Sadat S-pankin asiakkaat pääsivät kirjautumaan toisten verkkopankkeihin – Finanssivalvonta: poikkeuksellinen ja vakava tapahtuma. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12621116. Luettu: 28.4.2024.

Pantzar, M. 2022. Palvelunestohyökkäykset ryöpsähtivät – kohteena muun muassa suosittu Yle Areena. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12665063. Luettu: 28.4.2024.

Parviala, A. 2022. Wärtsilän tietojärjestelmä hakkeroitiin Venäjältä vetäytymisen jälkeen – tietoja päätyi rikollisryhmän kauppatavaraksi. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12549885. Luettu: 28.4.2024

Pukkila, T. 2023. Tietomurto Tena-tuotteita kuljettavaan yritykseen – tuhansien asiakkaiden henkilötietoja vaarassa. Yle Uutiset. Luettavissa: https://yle.fi/a/74-20051516. Luettu: 28.4.2024.

Raeste, J. 2022. Finanssivalvonta: Palvelunesto-hyökkäys Nordeaan oli ”poikkeuksellinen ja pitkäkestoinen”. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000008653356.html. Luettu: 28.4.2024.

Rimpiläinen, T. 2022. STT:n mukaan toimittajien muistiinpanoja ei ole vuotanut eikä lähdesuoja vaarantunut verkkohyökkäyksessä – muita vahinkoja selvitetään. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12557548. Luettu: 28.4.2024.

Rytkönen A. 2022. Tietomurrossa uusi käänne: Savonian opiskelijoiden tietoja julkaistiin Tor-verkossa. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12319469. Luettu: 28.4.2024.

Seppälä, S. 2022. Suomalaishotellien jättimäinen tietovuoto laajeni kolmeen uuteen hotelliin – Poliisi: Seurauksia uhreille mahdoton arvioida. MTV Uutiset. Luettavissa: https://www.mtvuutiset.fi/artikkeli/suomalaishotellien-jattimainen-tietovuoto-laajeni-kolmeen-uuteen-hotelliin-poliisi-seurauksia-uhreille-mahdoton-arvioida/8413978#gs.yq8nyq. Luettu: 28.4.2024.

Strömberg, J. 2022. STT varoitti entisiä ja nykyisiä työntekijöitään sähköpostilla: tietomurron tekijät saivat ehkä haltuunsa henkilötunnuksia ja osoitteita. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12577406. Luettu: 28.4.2024.

STT 2021a. Kyberhyökkäyksen kohteeksi joutunut Eilakaisla sai toimintansa taas pyörimään – viitteitä tietojen varastamisesta ei ole. MTV Uutiset. Luettavissa: https://www.mtvuutiset.fi/artikkeli/kyberhyokkayksen-kohteeksi-joutunut-eilakaisla-sai-toimintansa-taas-pyorimaan-viitteita-tietojen-varastamisesta-ei-ole/8033598. Luettu: 28.4.2024.

STT 2023a. Suomen Pankki, Verohallinto ja moni media olleet torstaina palvelun-esto-hyökkäyksen kohteena. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000009903723.html. Luettu: 28.4.2024.

STT 2021b. Työnvälitysyhtiö Eilakaisla joutunut kyberhyökkäyksen kohteeksi – kymmenientuhansien henkilötietoja saattanut joutua vääriin käsiin. Yle Uutiset. Luettavissa: https://yle.fi/a/3-11730761. Luettu: 28.4.2024.

STT 2022. Uponoriin epäillään kohdistuneen tieto-murto kiristys-hyökkäyksen yhteydessä. Helsingin Sanomat. Luettavissa: https://www.hs.fi/talous/art-2000009210654.html. Luettu: 28.4.2024.

STT 2023b. Vakava varoitus suomalaisille: Tietomurto leviää yleisessä sähköposti-järjestelmässä. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000009936329.html. Luettu: 28.4.2024.

STT & Hirvonen S. 2022. Hissiyhtiö Kone on joutunut verkkohyökkäyksen kohteeksi – sama hakkeri voi olla taksipalvelu Uberin ja peliyhtiön hyökkäysten takana. Yle Uutiset. Luettavissa: https://yle.fi/a/3-12641867. Luettu: 28.4.2024.

STT-YLE 2021. Kyberturvallisuuskeskus varoittaa: Sadat organisaatiot ovat riskissä päätyä tai ovat jo päätyneet sähköpostipalvelinten tietomurron kohteeksi. Yle Uutiset. Luettavissa: https://yle.fi/a/3-11827028. Luettu: 28.4.2024.

Suomen yrittäjät 2022. Yrittäjägallup helmikuu 2022 Tietomurrot. Luettavissa: https://www.yrittajat.fi/wp-content/uploads/2022/04/Yrittajagallup-helmikuu-2022_tietoturva.pdf. Luettu: 29.4.2024-

Uhari, M. 2023. Westlog-yhtiön tietomurto vaaransi yli 116 000 ihmisen tietoturvan – Laajuus monin-kertainen Vastaamoon nähden. Helsingin Sanomat. Luettavissa: https://www.hs.fi/kotimaa/art-2000010031773.html. Luettu: 28.4.2024.