Suomessa tapahtuneet julkisen sektorin tietojärjestelmien tietomurrot lähivuosina

Essi Häyrinen

Haaga-Helia ammattikorkeakoulu
Tradenomi
AMK-opinnäytetyö
2025

Tiivistelmä

Tekijä(t)
Essi Häyrinen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Suomessa tapahtuneet julkisen sektorin tietojärjestelmien tietomurrot lähivuosina

Sivu- ja liitesivumäärä
35 + 0

Tämän opinnäytetyön tarkoituksena oli selvittää, olivatko suomalaisen julkisen sektorin tietojärjestelmät alttiita tietomurroille. Tietomurrot ovat olleet nykypäivän vakava uhka, jonka vuoksi ne ovat vaikuttaneet myös suomalaiseen julkiseen sektoriin. Tutkimuksessa keskityttiin erityisesti suomalaisen julkisen sektorin tietomurtotapauksiin case-esimerkkien muodossa. Opinnäytetyön tavoitteena oli tuoda ilmi konkreettisia tietomurtotapauksia, ja kertoa kuinka tapaukset olivat edenneet sekä millaisia toimia julkisen sektorin organisaatiot olivat tehneet tietomurtotapausten seurauksena. Työssä tuotiin ilmi myös keinoja tietoturvakäytäntöihin sekä miten julkisen sektorin organisaatiot olisivat voineet ehkäistä ja hallita näitä uhkia.

Opinnäytetyön tutkimuksen tietoperusta koostui kirjallisuuskatsauksen ympärille, jossa tarkasteltiin tietomurtojen erilaisia muotoja. Tutkimuksen tutkimusote toteutettiin laadullisena tutkimuksena, jossa aineistoa kerättiin havainnoiden sekä joukkotiedotuksen tuotteita hyödyntäen. Tutkimuksessa tarkasteltiin viittä eri julkisen sektorin organisaation tietomurto case-tapausta. Tutkimuksen tutkimusmenetelmänä käytettiin vertailevaa tutkimusta sekä aineistolähtöistä sisällönanalyysiä. Empiirisessä tutkimuksessa tarkastellut case-tapaukset tarjosivat havaintoja siitä, millaisia tietomurtoja julkiseen sektoriin oli kohdistunut viime vuosina.

Tutkimuksen tulokset esittelivät vastauksia liittyen tietojärjestelmien haavoittuvuuteen, tehtyihin tietomurtoihin, hyödynnettyihin haavoittuvuuksiin, tehokkaimpiin tietoturvakäytäntöihin sekä tietomurtojen ehkäisyyn ja hallintaan.

Tutkimuksen johtopäätöksissä todettiin, että julkisen sektorin tietojärjestelmien tietomurtoja edistävät tekijät olivat tekniset haavoittuvuudet, kuten päivittämättömät järjestelmät, tietoturvaongelmat sekä inhimilliset tekijät. Julkisen sektorin organisaatioiden tietomurtojen alttius ei kuitenkaan johtunut yksittäisistä puutteista, vaan muodostui kokonaisvaltaisesti teknisten sekä organisaattoristen toimien välille.

Lopuksi opinnäytetyö tarjosi pohdintaa liittyen julkisen sektorin kyberturvallisuuteen, organisaatioiden väliseen yhteistyöhön sekä tietoturvallisuuteen liittyviin koulutuksiin. Opinnäytetyön lopussa pohdittiin myös tutkimuksen luotettavuutta, oman oppimisen arviointia sekä jatkotutkimusideoita.

Asiasanat
Tietomurto, tietojärjestelmä, julkinen sektori, kyberrikollisuus

Sisällys

1 Johdanto

Julkisella sektorilla on tapahtunut useita ikäviä tietomurtoja lähivuosien aikana. Tietomurrot ovat yleisesti kohdistuneet organisaatioiden käytössä oleviin järjestelmiin. Tietomurrot tai niiden yritykset ovat aina rangaistava teko, jotka on määritelty laissa. Tietomurroksi luetaan tapahtuma, jossa henkilö on käyttänyt hänelle kuulumatonta käyttäjätunnusta tai murtanut turvajärjestelmän sähköisesti tai muulla vastaavalla teknisellä keinolla (Rikoslaki 38:8§). Järjestelmiä on murrettu yleisimmin varastamalla kirjautumistiedot käyttäjiltä, johon käytetään tietojenkalastelua eli phisingia (Poliisi, s.a.).

Tietoturvan merkitys näiden tapausten seurauksena onkin ensisijaisen tärkeässä roolissa. Teknologian jatkuva ja nopea kehitys tekee tietoturvan hallinnasta entistäkin haastavampaa, sillä pysyviä ratkaisuja uusiin syntyviin ongelmiin ei ole löydetty. Vaikka tietoturvallisuutta kehitetään jatkuvasti uusien teknologioiden avulla, tarjoaa se vain lyhyen aikavälin suojan tietojen sekä tietoverkkojen suojaamiseksi (KumarGoutam 2015, 14.)

Julkinen sektori onkin yksi ensisijaisimmista kohteista tietomurroille, sillä siellä säilytettävän datan ja luottamuksellisen tiedon määrä on suuri. Julkisen sektorin toimijoiden onkin erityisen tärkeää huolehtia tietoturvakäytännöistä sekä varmistettava riittävä ja luottamuksellinen tietosuoja. (KumarGoutam 2015, 14.)

Tämä opinnäytetyö tarjoaa analyysin Suomessa tapahtuneista julkisen sektorin tietomurroista tietojärjestelmiin. Tutkimus tarkastelee tietoturvan merkitystä julkisen sektorin organisaatiossa, ja pyrkii havaitsemaan sen riskejä sekä haasteita julkisella sektorilla työskennellessä. Aiheen tärkeys ja ajankohtaisuus korostuvat jatkuvasti muuttuvassa digitaalisessa maailmassa, jossa organisaatiot pyrkivät mukautumaan uusiin tietoturvakäytäntöihin sekä tietoturva haasteisiin. Tietoturvauhkien määrä ja vaikeus ovat kasvaneet jatkuvasti teknologian kehityksen mukana, mikä on lisännyt työntekijöiden tarvetta ymmärtää tietoturvankäytännöistä enemmän, sekä miten työskentely suoritetaan mahdollisimman tietoturvallisesti riskejä välttäen. Työn tavoitteena on tuottaa käytännönläheinen kokonaiskuva, joka auttaa lukijoita ymmärtämään julkisen sektorin tietoturvan haasteita ja löytämään keinoja niiden parantamiseksi sekä hallitsemiseksi julkisella sektorilla työskennellessä.

1.1 Tutkimusongelma

Opinnäytetyön aiheena on Suomessa tapahtuneet julkisen sektorin tietomurrot tietojärjestelmiin lähivuosina. Aihe on ajankohtainen ja tärkeä, sillä tietomurrot ovat yleistyneet huomattavasti lähivuosien aikana. Tämä on nostanut esiin uudenlaisia tietoturvakysymyksiä sekä -haasteita. Tämän tutkimusaiheen valintaan vaikuttavia tekijöitä olivat aiheen ajankohtaisuus sekä oma

henkilökohtainen kiinnostus aihetta kohtaan. Aiheen valinnassa minulla oli kuitenkin alkuun haasteita, mutta sain siihen tarvittavaa ohjausta, jonka perusteella päädyin tähän aiheeseen.

Tutkimus on toteutettu kvalitatiivisella eli laadullisella tutkimusotteella. Laadullisella tutkimuksella tarkoitetaan tutkimusmenetelmää, jossa tutkittavasta ilmiöstä ei ole riittävästi tietoa tai ymmärrystä. Laadullisessa tutkimuksessa on tärkeää keskittyä sen eettisyyteen ja luotettavuuteen. Teorian merkitys on laadullisessa tutkimuksessa tärkeä ja ilmeinen, ja teorian tarve onkin tutkimuksessa välttämätön. (Tuomi & Sarajärvi 2018, luku 1-1.1.1.)

Tämän opinnäytetyön tiedon analysoinnissa on käytetty kirjallisuuskatsausta sekä vertailevaa tutkimusta. Vilkka (2023, luku 4.2.2) mukaan kirjallisuuskatsauksen tavoitteena on auttaa rakentamaan teoreettista viitekehystä, joka vastaa paremmin oman tutkimuksen tarkoitusta ja asetettua tutkimusongelmaa. Katsaus perustelee paikkansa erityisesti aiempien tutkimuksien esittelyssä sekä teoreettisen viitekehyksen määrittelyssä. Vertailevan tutkimuksen avulla voidaan saada informaatiota kahdesta tai useammasta eri näkökulmasta. Kekkonen (2008, 33-34) mukaan vertailevaan tutkimukseen ei ole yhtä ja ainoaa tapaa, kuinka se tulisi toteuttaa. Vertailututkimuksen etuna on se, että sen kautta voidaan saada tietoa auki eriasteisiin yleistyksiin, mikäli saadaan esille tekijöitä, jotka toistuvat eri paikoissa ja eri aikoina.

Tutkimuksen perusteella pyritään vastaamaan kysymykseen: Ovatko julkisen sektorin tietojärjestelmät alttiita tietomurroille?

Alaongelmat:

1. Miksi julkisen sektorin tietojärjestelmät ovat olleet alttiita tietomurroille?
2. Millaisia tietomurtoja julkisen sektorin tietojärjestelmiin on tehty viime vuosina?
3. Mitä haavoittuvuuksia hyödynnettiin julkisen sektorin tietomurroissa?
4. Mitkä tietoturvakäytännöt ovat osoittautuneet tehokkaimmiksi estämään tietomurtoja?
5. Miten organisaatiot voivat tehokkaasti ehkäistä ja hallita näitä uhkia?

Opinnäytetyön alaongelmien yhteys teoreettiseen viitekehykseen ja tutkimustuloksiin on kuvattu alla olevalla peittomatriisilla (Taulukko 1).

Taulukko 1. Peittomatriisi

Opinnäytetyön alaongelmat	Teoreettinen viitekehys	Tutkimustulokset
1. Miksi julkisen sektorin tietojärjestelmät ovat olleet alttiita tietomurroille?	4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.2	5.1

2. Millaisia tietomurtoja julkisen sektorin tietojärjestelmiin on tehty viimevuosina?	4.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5	5.2
3. Mitä haavoittuvuuksia hyödynnettiin julkisen sektorin tietomurroissa?	4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5	5.3
4. Mitkä tietoturvakäytännöt ovat osoittautuneet tehokkaimmiksi estämään tietomurtoja?	4.2	5.4
5. Miten organisaatiot voivat tehokkaasti ehkäistä ja hallita näitä uhkia?	4.2	5.5

Peittomatriisissa alaongelmien yhteys teoreettiseen viitekehykseen sekä tutkimustuloksiin on esitetty kappalenumerointia hyödyntäen.

1.2 Tutkimuksen rakenne

Tämä opinnäytetyö koostuu rakenteeltaan 6 pääluvusta. Ensimmäisessä luvussa lukija johdatellaan tutkimuksen aihepiiriin sekä esitellään tutkimusongelma, tutkimuskysymykset sekä keskeiset käsitteet. Toisessa luvussa käsitellään tutkimuksen teoreettinen viitekehys, jossa käsitellään tutkimukselle olennaisia teorioita ja käsitteitä. Kolmannessa luvussa esitetään tutkimusmenetelmä sekä analysoidaan tutkimusaineiston keräämistä sekä tutkimusasetelmaa. Neljännessä luvussa perehdytään itse tutkittavaan aineistoon. Viidessä luvussa kuvataan tutkimustulokset sekä pohditaan johtopäätöksiä. Kuudessa luvussa kootaan yhteen pohdinta sekä arvioidaan tutkimuksen onnistumista. Lopussa arvioidaan myös omaa oppimista sekä jatkotutkimusideoita.

1.3 Keskeiset käsitteet

DLP: On lyhenne sanoista Data Loss Prevention. DLP tarkoittaa tietojen menettämisen estämiseksi tarkoitettua ratkaisua. Se estää organisaation sisäisiä käyttäjiä lähettämästä arkaluontoisia sekä suojattuja tietoja yrityksen ulkopuolelle. DLP keskittyy ensisijaisesti sisäisten uhkien torjuntaan, ja käyttää toiminnassaan liiketoimintasääntöjä tietojen luokittelun ja suojaamisen avuksi. (Ibrahim, Thiruvady, Schneider & Abdelrazek, 2020, 2.)

Julkinen sektori: On määritelmä, johon kuuluvat valtio ja kunnat. Julkinen sektori jaetaan valtion sektoriin sekä kuntiin ja kuntayhtymiin. Valtionsektoriin kuuluvat valtion hallinto, yliopistot, Kansaneläkelaitos, valtion liikelaitokset sekä sosiaaliturvarahastot. Kuntiin ja kuntayhtymiin luetaan

kuuluviksi kunnan hallinto, kunnallinen koululaitos, kuntien ja kuntayhtymien palvelulaitokset ja toimipaikat, jotka eivät ole yhtiömuotoisia. (Tilastokeskus, 2020.)

Kyberrikollinen: Kyberrikollinen on henkilö, joka hyödyntää tietojärjestelmiä sekä teknologiaa kyberrikollisuuteen. Kyberrikollinen hyödyntää teknologiaa varkauksiin, kiristyksiin, identiteettivarkauksiin, petoksiin sekä muun muassa vakoiluun. (Cymru, 2006, 25.)

Kyberturvallisuus: Tekniikka, jonka tavoitteena on suojata käyttäjä organisaation kyberympäristö. Se suojaa internetiin yhdistettyjen järjestelmien, kuten laitteiston, ohjelmiston ja datan kyberhyökkäyksiltä. Kyberturvallisuuden tarkoituksena on säilyttää datan luottamuksellisuus, eheys ja saatavuus. (Seemma, Nandhini & Sowmiya, 2018, 125.)

Kyberuhka: Laaja kirjo haitallista toimintaa, joita tapahtuu kyberympäristössä. Kyberuhkien tarkoituksena on vahingoittaa tai häiritä yrityksien tietoverkkoja tai tietojärjestelmiä. Kyberuhkia ovat muun muassa verkkosivujen turmeleminen, vakoilu, immateriaalioikeuksien varastaminen, palvelunestohyökkäykset sekä haittaohjelmat. (Abu, Ariffin, Selamat & Yusof, 2018, 373.)

Tietojärjestelmä: Järjestelmä, jonka tarkoituksena on tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Järjestelmä koostuu tiedostoista, tiedoista käsittelevistä ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista sekä tietoja käsittelevistä ohjelmista. Tietojärjestelmällä operoidaan myös tietovarantoja. (Finto.fi)

Tietomurto: Tietomurto tarkoittaa luvatonta tunkeutumista tietojärjestelmään, palveluun, laitteeseen tai sovellukseen. Tietomurto on rangaistava teko, joka on määritelty rikoslaissa, myös tietomurron yritys on rangaistavaa. Luvaton järjestelmään tunkeutuminen täyttää rikoksen tunnusmerkit. Tietomurron taustalla on yleensä taloudellisen hyödyn tavoittelu. Tietomurrossa saatuja materiaaleja voidaan käyttää haitallisen materiaalin jakamiseen tai murretun ympäristön toiminta voidaan lamauttaa kiristyshaittaohjelmilla. (Kyberturvallisuuskeskus, 2024.)

Tietosuoja: Tietosuoja tarkoittaa käytäntöjä ja toimintatapoja, joilla pyritään turvaamaan arkaluontoiset tiedot vaarantumiselta ja vahingoittumiselta. Tietosuoja on myös tärkeä ja olennainen osa organisaation turvallisuutta. Tietosuojan toteuttaminen edellyttää tietosuojasäädösten mukaisia toimintamalleja, jotka paitsi suojaavat organisaation tiedot, myös turvaavat organisaation mainetta sekä luotettavuutta. (Microsoft, s.a.).

Tietoturva: Tarkoittaa toimia, joilla pyritään varmistamaan tietojen luottamuksellisuus, eheys ja saatavuus. Tietoturvalla pyritään varmistamaan se, että ainoastaan asianmukaiset tahot pääsevät käsiksi tarvitsemiinsa tietoihin. (Digi- ja väestötietovirasto, 2022.)

2 Tietomurtojen yleisimmät muodot

Tietomurrot ja kyberuhat ovat eksponentiaalisesti lisääntyneet nykypäivänä niin yksityisten henkilöiden kuin isompien organisaatioiden osalta. Tietomurrot ovat nykypäivän vakava ja jatkuva uhka. Tietomurrot ovat luvattomia pääsyjä suojattuihin, arkaluontoisiin ja luottamuksellisiin tietoihin. Nykyään myös julkisen sektorin organisaatiot voivat olla alttiita tietomurroille sekä kyberhyökkäyksille, kuten muutkin pienemmät organisaatiot. Tietomurron uhriksi joutuvat yleisimmin organisaatiot sekä sen asiakkaat tai sidosryhmät. Nämä tapaukset johtavat yleensä kielteisiin seurauksiin. Tietomurrot ovatkin organisaatioille kriisinomainen tilanne, jolla on vaikutusta myös organisaation muihin sidosryhmiin, kuten asiakkaisiin ja julkisella sektorilla yksittäiseen kansaan. (Joseph, 2017, 57-59.) Tietomurrot ovatkin aina rangaistava teko, joka on määritelty laissa niiden vakavuuden perusteella. Tietomurtojen teko tapoja on myös useita, ja hyökkääjät keksivätkin jatkuvasti uusia tapoja hyödyntää tietoturva-aukkoja ja -puutoksia hyökkäyksiinsä.

Tässä luvussa käsitellään tietomurtojen yleisimpiä muotoja hyödyntäen kirjallisuutta ja tutkimuksia. Tietomurtojen yleisimmät muodot on valittu kyberturvallisuutta käsittelevän kirjallisuuden sekä tutkimusten pohjalta. Tavoitteena on esitellä ne muodot, jotka esiintyvät usein alan tutkimuksissa, ja jotka aiheuttavat merkittäviä riskejä organisaatiolle. Valitut muodot ovat haittaohjelmat, tietojenkalastelu sekä tietovuodot. Ne edustavat tämän hetken vakavimpia ja yleisimpiä tietomurto muotoja.

2.1 Haittaohjelmat

Haittaohjelmat (Malware) on lyhenne sanoista Malicious Software, joka tarkoittaa haittaohjelmistoa. Sen päätarkoituksena on vahingoittaa tietokoneita tai niiden käyttäjiä. Haittaohjelmien avulla voidaan varastaa henkilökohtaisia tietoja, vioittaa tiedostoja tai tehdä muuta haitallista ja häiritsevää toimintaa, jolla voidaan vaikuttaa käyttäjän toimintaa häiritsevästi (Tahir, 2018, 20-21). Haittaohjelmien kirjo on laaja ja niitä on useita erilaisiin käyttötarkoituksiin. Haittaohjelmien muodot voivat kuitenkin vaihdella ja ne lisääntyvät jatkuvasti yhä haitallisimmiksi. AV-Test instituutin tekemän tutkimuksen mukaan vuonna 2020 joka päivä raportoitiin 350 000 uutta vaarallista sovellusta tai ohjelmaa (Pachhala, Jothilakshmi & Battula, 2021, 1207).

Haittaohjelmien leviämistapoja on useita, ja ne voivat pahimmassa tapauksessa myös levittää itse itseään ”tartuntataudin” lailla. Kyberhyökkääjät käyttävät, luovat ja myyvät haittaohjelmia yleisimmin henkilökohtaisten- tai taloudellistentietojen varastamiseen. Haittaohjelmat voivat levitä sähköpostitse, jolloin käyttäjälle lähetetty viesti voi sisältää liitteitä tai linkkejä, jotka avaamalla haittaohjelma asentuu laitteeseen. Liitteet ja linkit näyttävät useimmiten luotettavilta ja uskottavilta, mutta käyttäjän tietämättä ne levittävät haittaohjelmaa. Haittaohjelmat leviävät nopeasti myös tiedostopalvelimen kautta. Yleisimmät internet tiedostojärjestelmät (SMB/CIFS) ja

verkkotiedostojärjestelmät (NFS) kautta haittaohjelmat voivat levitä nopeasti, kun käyttäjät lataavat laitteilleen tiedostoja. Tämä voi johtaa haittaohjelmien monistumiseen siirrettävälle tallennusvälineelle ja siten koko tietokoneeseen sekä -verkkoihin (Kadari ym. 2024, 482-484.)

Haittaohjelmien toiminta on usein saman kaavan mukaista, ja haittaohjelmat hyödyntävät usein haavoittuvuuksia päästäkseen tietojärjestelmiin. Kun haittaohjelma on asennettu järjestelmään Kadari ja kumppanit (2024, 482) mukaan haittaohjelman voi kuitenkin tunnistaa useimmiten seuraavista merkeistä:

- Järjestelmän hitaampi suorituskyky
- Tuntemattomat sovellukset ja ohjelmat asentuvat laitteelle
- Epätavallinen laitteiston käyttäytyminen ja ylikuumentuminen
- Satunnaiset ponnahdusikkunat
- Vähenevä kovalevyn tila

Haittaohjelmien määrän lisääntymisen myötä, myös niiden eri muodot vaihtelevat laajasti. (Kadari ym. 2024, 483.) Seuraavaksi selitetään yleisimpien haittaohjelmien määritelmät.

2.1.1 Virukset

Viruksilla tarkoitetaan haittaohjelmaa, joka kulkee toisen ohjelman esimerkiksi asiakirjan mukana. Se pystyy leviämään itsestään sen jälkeen, kun se on käynnistetty laitteella. Virus voi levitä laitteelle esimerkiksi vaarallisen sähköposti liitteen kautta. Virukset voivat aiheuttaa tiedostojen vaurioitumista, järjestelmän hidastumista sekä esimerkiksi näppäinpainallusten tallentamista, mikä johtaa pahimmassa tapauksessa vakaviin lisäuhkiin. (Chandy, J. 2022, 387).

2.1.2 Vakoiluohjelmat

Vakoiluohjelmilla tarkoitetaan haittaohjelmaa, jonka tarkoituksena on tunkeutua laitteeseen, kerätä käyttäjästä tietoja ja lähettää ne eteenpäin. Vakoiluohjelmat pyrkivät hyötymään käyttäjästä esimerkiksi varastetuilla tiedostoilla. Vakoiluohjelmat voivat hidastaa tavallista käyttäjäntoimintaa laitteella sekä se voi vaikuttaa laitteen suorituskykyyn. Vakoiluohjelman iskiessä laitteeseen sen käyttäjä on vaarassa tietoturvaloukkauksille sekä henkilötietojen väärinkäytölle. (Chandy, J. 2022, 387.)

2.1.3 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat yksi yleistyvimmistä haittaohjelmatyypeistä. Niiden tarkoituksena on vahingoittaa tietokonetta sekä päästä käsiksi salattuihin tiedostoihin. Kyberrikolliset hyödyntävät kiristyshaittaohjelmia nykyään yleistyvästi. Kyberrikolliset pystyvät estämään ja salaamaan luvallisten

käyttäjien pääsyn hyökätyn koneen tiedostoihin, ja näin he voivat kiristää luvallisia käyttäjiä. Useimmiten hyökkääjät vaativat suuria summia lunnaita vastineeksi salauksen purusta, jotta luvalliset käyttäjät saisivat tiedostonsa takaisin. Useimmiten vaikka lunnaat olisi maksettu kyberrikollisille, he eivät kuitenkaan palauta pääsyä tiedostoihin enää luvallisille käyttäjille. (Temara, 2024, 2.)

2.1.4 Kryptojacking

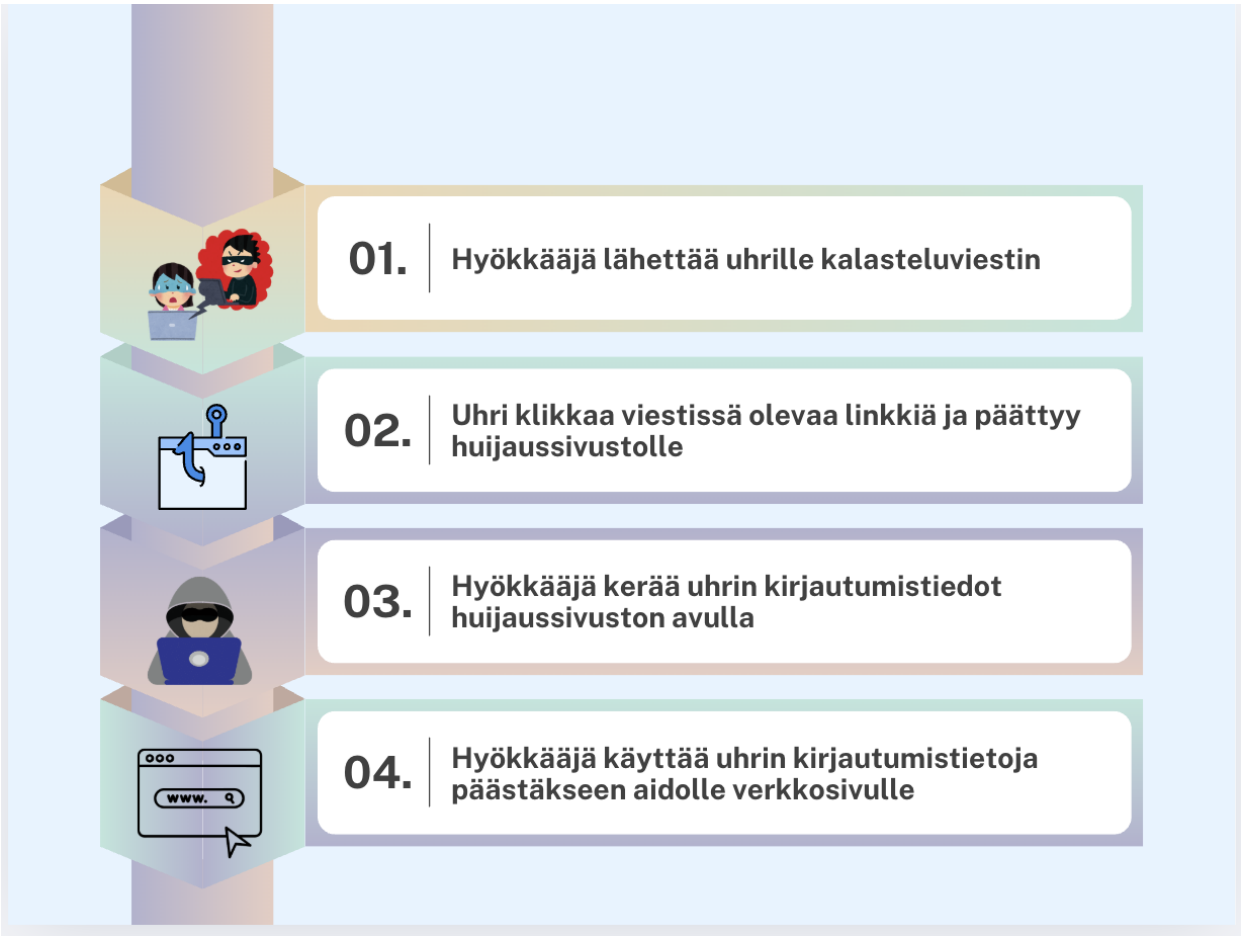
Kryptojacking on salaista selainkäyttäjän tietokoneen resurssien hyödyntämistä louhintaan voittojen saavuttamiseksi. Se on hyökkäystyyppi, joka hyödyntää ja kuluttaa käyttäjän laskentatehoa ilman hänen lupaansa. Tämä toiminta saa aikaan käyttäjän tietokoneen hidastumisen, mikä voi vaikuttaa laitteen normaaliin käyttöön. Kryptojackingissä verkkosivuille upotetaan louhintaskriptejä, jonka avulla rikolliset louhivat kryptovaluuttaa. (Wu, Lai, Hwang, Chang & Hsu, 2022, 5.)

Kaikki edellä mainitut haittaohjelmat ovat vaarallisia ja niiden avulla pyritään vahingoittamaan käyttäjän tietokonetta tai esimerkiksi varastamaan henkilökohtaisia tietoja. Julkisella sektorilla nämä edellä mainitut haittaohjelma tyypit ovat yleisimmin käytettyjä ja hyödynnettyjä organisaatioita kohtaan.

2.2 Tietojenkalastelu

Tietojenkalastelu on yhä jatkuvaan kasvava ja yleistyvä uhka. Tietojenkalastelussa kyberrikolliset yrittävät varastaa arkaluonteisia tietoja, kuten pankkitunnuksia, luottokorttitietoja ja salasanoja yksityishenkilöiltä ja organisaatioilta. Näissä tietojenkalastelun yrityksissä kyberrikolliset esiintyvät yleensä jonkin luotettavan tahon tai viranomaisen roolissa, käyttäen esimerkiksi väärennettyjä mutta aidolta näyttäviä verkkosivuja tai sähköposteja. Näin tietojenkalastelun uhri on helpompi saada uskomaan verkkosivun tai sähköpostin uskottavuus. Uhri saattaa tällöin syöttää tietojaan suoraan hakkereiden käsiin. (Trisolvena & Saputra, 2024, 38–40.) Bhavsar, Kadlak & Sharma (2018, 27) mukaan tietojenkalastelu vaiheet ovat yleisesti saman kaavan mukaisia, ja seuraavaksi käydään läpi tietojenkalastelun vaiheet:

- Hakkeri lähettää aidon näköisen sähköpostin tai tekstiviestin uhrille
- Uhri klikkaan viestissä olevaa linkkiä ja päätyy hakkereiden luomalle tietojenkalastelusivulle
- Hakkerit keräävät uhrin tunnistautumistiedot
- Hakkerit käyttävät uhrin tunnistautumistietoja päästäkseen aidolle verkkosivulle, esimerkiksi verkkopankkiin

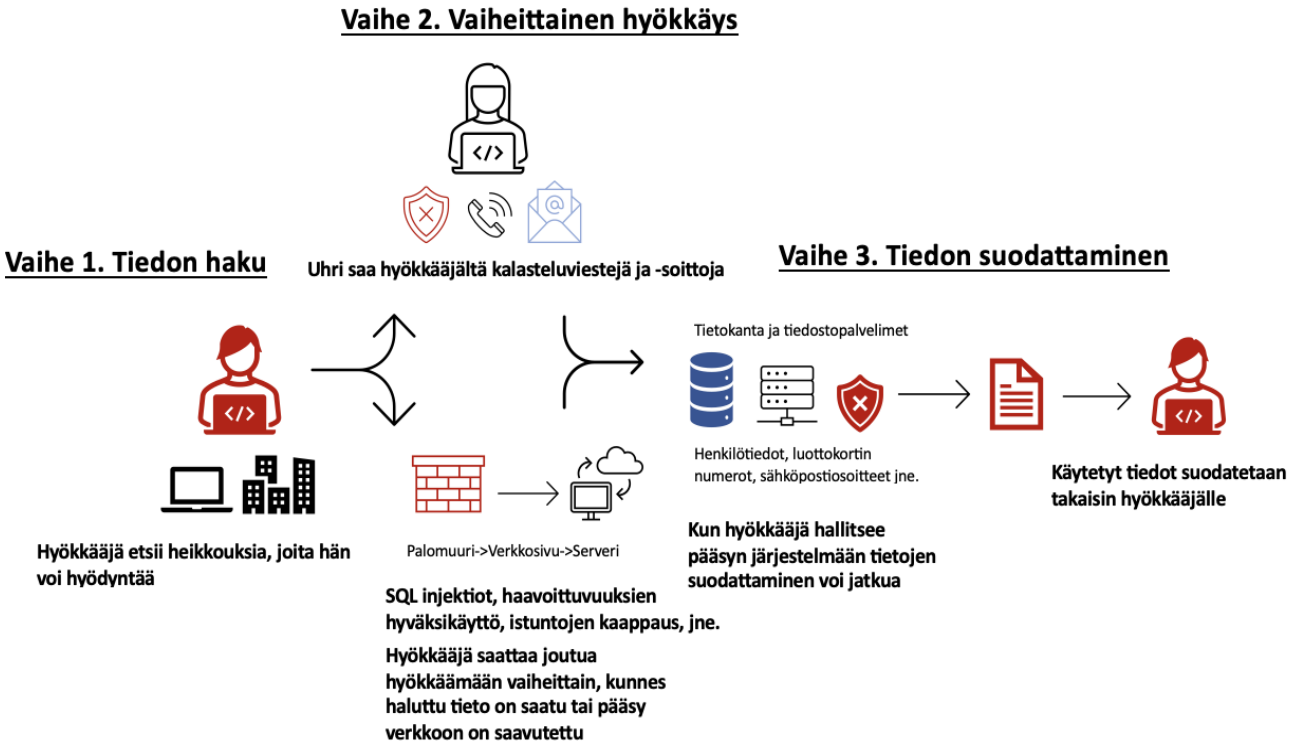


Kuva 1. Tietojenkalastelun toimintaperiaate vaiheittain. (mukaillen Bhavsar, Kadlak & Shama, 2018, 27.)

Tietojenkalastelun tunnusmerkkien perusteella käyttäjä voi helposti suojautua tehokkaasti omilla toimillaan tietojenkalastelua vastaan. Käyttäjän on tärkeää suojautua roskapostilta, sillä tietojenkalastelu yritykset tulevat tuntemattomilta lähettäjiltä, jotka ovat tekeytyneet aidonnäköisiksi. Aidonnäköisten viestin kanssa täytyy myös huomioida, ettei klikkaa tuntemattomista lähteistä tulleita linkkejä tai avaa liitteitä, mikäli ei odota kyseistä viestiä tai käyttäjä ei ole varma sen sisällöstä. Käyttäjän on siis tärkeää huomioida, ettei vastaa epäilyttäviin viesteihin tai jaa arkaluontoisia tietojaan. Myös verkkosivuja käyttäessä tulee varmistaa, että verkon yhteys on suojattu, varsinkin verkkomaksuja tehtäessä. Tämän käyttäjä voi helposti selvittää verkon url-osoitteesta. Mikäli url-osoitteessa lukee http eikä https, ei verkkoyhteys tällöin ole suojattu. Verkkosivujen url-osoitteiden kirjotusasua on myös tärkeä tarkastella. On tärkeää tarkastaa, ettei kirjotusasussa ole ylimääräisiä merkkejä tai kirjaimia, esimerkiksi paypall.com on väärin, kun taas paypal.com on oikein. Käyttäjän tulee olla huolellinen verkkosivujen url-osoitteiden kanssa, etteivät tiedot ajaudu hakkereiden hyväksikäytettäviksi. Näillä tekniikoilla käyttäjä voi helposti varmistaa, ettei joudu tietojenkalastelun uhriksi. (Bhavsar, Kadlak & Sharma, 2018, 28-29).

2.3 Tietovuoto

Tietovuodot tarkoittavat luotettavan tiedon tahallista tai tahatonta paljastumista ulkopuolisille henkilöille. Tietovuodot ovat nykypäivänä vakava uhka, joiden määrä on kasvanut eksponentiaalisesti lähivuosien aikana. Etenkin arkaluontoisten tietojen menettäminen voi aiheuttaa yrityksille vakavia ongelmia, taloudellisia tappioita sekä mainehaittaa. Yleisimmin vuotaneita tietotyyppejä ovat työntekijöiden- tai asiakkaidentiedot, potilas- ja sairaustiedot sekä immateriaalioikeuksiin viittaavat tiedot. Näiden tietojen vuotaminen on vaarallista ja aiheuttaa yrityksille paljon haittaa. Tietovuodot voivat johtua joko sisäisestä tai ulkoisesta tietoturvaloukkauksesta. Tietoturvaloukkaus voi olla myös joko tahallinen tai tahaton. Tietovuodot ovat kuitenkin lähes aina tahallinen teko, jossa organisaatio asetetaan merkittävään vaaraan. Tahallisia tietovuotoja ovat esimerkiksi hakkerin aiheuttama tietojen varastaminen. Näiden tietovuotojen motiivina on yleensä yritysvakoilu tai taloudellinen palkkio sisäisestä hyökkäyksestä. Tahatonta on taas esimerkiksi, jos työntekijä paljastaa vahingossa arkaluontoista tietoa. Tahattomien tietovuotojen motiivina toimii yleensä työntekijän huolimattomuus tai soveltuvien tietoturvallisuus käytäntöjen soveltamatta jättäminen. (Cheng, Liu & Yao, 2017, 1-2.)



Kuva 2. Tietovuotojen toimintaperiaate vaiheittain (mukaillen Streicher, 2022.)

Tietovuodot ovat valtava ongelma, ja usein tietovuotoja pidetään muiden tietoturvaongelmien, kuten ohjelmistovirheiden seurauksena. Tietoturvavaikutusten lisäksi tietovuodot aiheuttavat ongelmia yksityisyyden kanssa, sillä useimmat tietovuodot paljastavat arkaluontoisia tietoja hyökkääjille. Nämä paljastuneet tiedot päätyvätkin usein myyntiin pimeään verkkoon ja hyökkääjät voivat julkaista niitä myös julkisesti. Nämä tietojen julkaisut ja myynnit voivat johtaa yksityishenkilön vakaviin seurauksiin sekä pahantahtoisiin ajatuksiin. (Saleem & Naveed, 2020, 153.)

Tietovuotojen estämiseksi on kehitetty DLP-ratkaisu. DLP:n tarkoituksena on varmistaa, etteivät yrityksen sisäiset käyttäjät lähetä arkaluontoisia tietoja yrityksen verkon ulkopuolelle. DLP käyttää toimiakseen liiketoimintasääntöjä luokitellakseen sekä suojatakseen arkaluontoisia tietoja, jotta sisäiset käyttäjät eivät tahattomasti tai tahallisesti jaa tietoja. DLP-ratkaisut on kehitetty pääosin keskittymään yrityksen sisäisien tietovuotojen havaitsemiseksi. (Ibrahim, Thiruvady, Schneider & Abdelrazek, 2020, 2.)

3 Tutkimusasetelma

Tässä luvussa kuvataan opinnäytetyön tutkimusasetelmaa. Aluksi käydään läpi tutkimusote, jonka jälkeen syvennetään ymmärrystä tutkimuksesta aineiston keruu menetelmiin sekä tutkimusmenetelmien valintaan.

3.1 Tutkimusote

Tämän opinnäytetyön tutkimusotteeksi valittiin kvalitatiivinen eli laadullinen tutkimus. Laadullisen tutkimuksen tavoitteena on antaa tulkintoja ja syventää ymmärrystä tutkittavasta ilmiöstä. Laadullisessa tutkimuksessa teorian rooli on merkittävä, sillä teoria muodostaa perustan tutkimukselle, jossa käsitellään niiden välisiä suhteita, sekä teoria tarjoaa viitekehyksen ja ohjaa tutkimusta. (Tuomi & Sarajärvi, 2018, luku 1.1.1.) Laadullisessa tutkimuksessa tarkastellaan teorian ja käytännön välisiä suhteita. Laadullisen tutkimuksen piirteet eroavat tutkimusprosesseiltaan määrällisen tutkimuksen prosesseista, joten tutkijan tulee perehtyä hyvin laadullisen tutkimuksen perusteisiin sekä sen ominaispiirteisiin, jotta pystytään vastaamaan tutkimuksen asettamiin vaatimuksiin. (Puusa & Juuti, 2020, luku 2.)

Laadullisessa tutkimuksessa on tärkeää tarkastella myös tulkintaan sekä ymmärtämiseen liittyviä prosesseja. Tällöin tutkijan täytyy pohtia miten hänen omat näkemyksensä vaikuttavat havaintoihin ja millaisen osa se saa tutkimuksesta. (Puusa & Juuti, 2020, luku 2.) Laadullinen tutkimus kannattaa valita, kun tutkimuksen tavoitteena on ymmärtää ilmiöiden syvällisiä merkityksiä ja niiden taustalla olevia tekijöitä.

3.2 Aineiston keruu

Laadullisessa tutkimuksessa aineiston kerääminen on tavoitteellista toimintaa, jota ohjaavat tutkimuksen päämäärät. Päämäärät vaikuttavat siihen millaisia aineistoja tutkija hankkii ja miten hän niitä tulkitsee. Aineistonkeruumenetelmän hyvä tuntemus auttaa tutkijaa valitsemaan optimaalisen keruu menetelmän tutkimuksen tarpeisiin nähden. (Puusa & Juuti, 2020, luku 3.)

Yleisimpiä laadullisen tutkimuksen aineistonkeruumenetelmiä ovat haastattelut, kyselyt, havainnointi sekä erilaisista dokumenteista koottu tieto (Tuomi & Sarajärvi, 2018, luku 3.) Tässä opinnäytetyössä aineistoa kerättiin havainnoiden sekä hyödyntäen joukkotiedotuksen tuotteita, kuten uutisartikkeleja (Tuomi & Sarajärvi, 2018, luku 3.3.) Opinnäytetyössä tutkitaan case organisaatioiden tietomurtotapauksia, jonka vuoksi kyseiset aineistonkeruumenetelmät valittiin. Joukkotiedotus tuotteiden avulla saadaankin kerättyä aineistoa tapahtuneista tietomurtotapauksista, jotta tapausten analysointi on mahdollista. Joukkotiedotus tuotteita voidaan käyttää myös sisällönanalyysin tukena (Tuomi & Sarajärvi, 2018, luku 3.3.)

Joukkotiedotus tuotteiden lisäksi aineistoa kerättiin havainnoiden. Havainnointi on aineiston keruun perusmenetelmä, jota jokainen tutkija tekee. Havainnoinnin etuna on etenkin sen autenttisuus sekä kokonaisvaltaisuus, jonka avulla saatu tieto voidaan kytkeä suoraan asianyhteyteen. (Puusa & Juuti, 2020, luku 3.8.) Havainnoinnin sekä toisen aineistonkeruumenetelmän yhdistäminen on usein tehokas aineiston keruu tapa (Tuomi & Sarajärvi, 2018, luku 3.2.) Puusa & Juuti (2020, luku 3.8.) mukaan tutkijan on havainnoinnin avulla mahdollista todentaa, miten dokumenttien kautta ilmaistu asia toteutuu käytännössä. Nämä aineistonkeruumenetelmät yhdistettynä tutkimuksen tekeminen, sekä tutkimuskysymyksiin vastauksien saaminen on mahdollista.

3.3 Tutkimusmenetelmän valinta

Tämän opinnäytetyön tutkimuksen tutkimusmenetelmänä käytettiin vertailevaa tutkimusta sekä sisällönanalyysiä. Vertailevan tutkimuksen avulla saadaan avattua uusia kysymyksiä sekä mahdollisuuksia. Vertailevan tutkimuksen etuna on myös, että sen kautta saadaan eriasteisia yleistyksiä auki tekijöistä, jotka toistuvat eri paikoissa ja eri aikoina. Vertaileva tutkimus voi siis toimia myös teorian perustana. Vertailuja voidaan tehdä usealla eri tavalla, niin historian suunasta kuin vertaillen nykyhetken tapahtumia. Myös vertailujen kohdealue ja vertailtavien kohteiden määrä voivat olla hyvin vaihtelevia. Vertailevalle tutkimukselle ei olekaan yhtä ja ainoaa oikeaa tapaa toteuttaa. (Kekkonen, 2008, 33-34.)

Vertailevan tutkimuksen ansiosta pystytäänkin etsimään vastauksia tutkimuskysymykseeni. Vertailevan tutkimuksen avulla pyritään vertaamaan ja selvittämään case organisaatioiden tietomurtojen syitä, seurauksia sekä niiden ehkäisyä ja hallintaa. Se antaa kattavan ymmärryksen siitä, miten tilanteissa tulee toimia ja kuinka vastaavia uhkia voidaan ehkäistä tulevaisuudessa. Vertailu auttaa myös tunnistamaan ja ymmärtämään tietomurtojen yhtäläisyyksiä ja eroja, mikä antaa laajemman kokonaiskuvan.

Tutkimuksessa käytetiin tutkimusmenetelmänä myös aineistolähtöistä sisällönanalyysiä. Sisällönanalyysia käytetään kirjallisuuskatsauksen tukena, riippumatta onko tieto kvalitatiivista vai kvantitatiivista. Sisällönanalyysi koostuu kolmesta vaiheesta: analyysin valmistelu, organisointi ja raportointi. Valmistelu vaiheessa tiedot jaetaan muotoon, jossa niitä voidaan tutkia. Siinä myös määritetään tutkimuksen aihe, teoria ja menetelmät. Toisessa vaiheessa pohditaan aineistosta löytyneitä havaintoja, joita hyödynnetään havaintoihin, tuloksiin sekä päätelmiin. Kolmannessa vaiheessa tutkimuksen analyysi ja tulokset havainnollistetaan kirjallisuuden avulla raportiksi. (Vilkka, 2023, luku 3.1.) Aineistolähtöisessä sisällönanalyysissa pyritään yhdistelemään käsitteitä ja saada vastauksia tutkimukseen. Sisällönanalyysi perustuu tulkintaan ja päättelyyn, jossa edetään teoria osuudesta kohti empiiristä osuutta, jossa saadaan käsitteellisempää näkemystä tutkittavasta ilmiöstä. Sisällönanalyysin ansiosta teoriaa ja johtopäätöksiä verrataan alkuperäisaineistoon uutta tietoa

muodostaen. (Tuomi & Sarajärvi, 2018, luku 4.4.3.) Näin pystytään tuottamaan vastauksia tutkimuskysymyksiin. Analyysin tarkoituksena on luoda sanallinen ja selkä kuvaus tutkittavasta ilmiöstä tiiviiseen ja selkään muotoon, ilman että sen sisältämät informaatio katoaa (Tuomi & Sarajärvi, 2018, luku 4.2.)

4 Suomalaisen julkisen sektorin tietomurrot lähivuosina

Suomalaisen julkisen sektorin tietomurtojen määrät ovat lisääntyneet lähivuosien aikana, ja niitä tapahtuu linjakkaasti joka vuosi. Yleisesti vuonna 2024 todettiin yli 18 000 tietoturvapoikkeama ilmoitusta, sekä 185 000 automaattisesti käsiteltyä ilmoitusta. Tietomurtoyritysten määrä onkin tasaisessa nousussa, vaikka varsinaisesti toteutuneiden tietomurtojen määrä on hieman laskenut. (Traficom, 2025). Tässä luvussa käsitellään suomessa tapahtuneita julkisen sektorin tietomurtoja kirjallisuuden ja tapahtuneiden tietomurto tapausten sekä tietomurtoyritysten näkökulmasta. Ensin käydään läpi tietomurtotapausten esittely, jonka jälkeen siirrytään pohtimaan syitä sekä organisaatioiden reaktioita tapauksiin. Esiteltävät tietomurtotapaukset on valittu satunnaisesti, ja tarkasteluun on valittu viisi satunnaisesti ensimmäiseksi valikoitunutta tapausta.

4.1 Tietomurtotapaukset

Julkiset sektorit ovat altis kohde hakkereille sillä ne käyttävät tieto- ja viestintäteknologiaa, jotka tarjoavat mahdollisuuksia tietomurroille. Erilaiset julkisen sektorin toimijat keräävät, tallentavat ja analysoivat tietoja eri julkisen sektorin toimijoilta, kuten koulutuksesta sekä julkisesta terveydenhuollosta, ja nämä tiedot ovatkin houkuttelevia kyberrikollisille, jotka jatkuvasti etsivät keinoja hyödyntää näitä tietoja laittomasti. (Joseph, 2017, 58.) Suomessa tapahtuneet tietomurto yritykset ovat olleet yleisesti tahallisia ja tietomurtojen muodot ovat vaihdelleet monipuolisesti. Lähivuosien aikana Suomessa onkin tapahtunut lukuisia uutiskynnyksen ylittäneitä tietomurto tapauksia.

4.1.1 Case 1: Helsingin kaupungin kasvatuksen ja koulutuksen toimialan tietomurto

Yksi suurimmista lähivuosien tietomurto tapauksista kohdistui vuonna 2024 Helsingin kaupungin kasvatuksen ja koulutuksen toimialaan. Tietomurto kohdistui kaupungin käyttämään taustajärjestelmään, jonka kautta hallinnoidaan oppilaiden ja huoltajien henkilötietoja. Järjestelmän nimeä ei ole tuotu julkisuuteen. Tietomurron seurauksena hyökkääjä sai käsiinsä arkaluontoisia tietoja kaikista helsinkiläisistä vuonna 2005–2018 syntyneistä oppivelvollisista sekä heidän huoltajistaan. Hyökkääjä sai haltuunsa muun muassa henkilötunnuksia, osoitteita, oppijoiden kansalaisuuksien, äidinkieliä sekä uskontokunnan. Tietomurron vaikutusalue kattoi mahdollisesti myös yksityisiä varhaiskasvatuksenyksiöitä, kouluja, lukioita sekä ammattioppilaitoksia. Tietomurto ei rajoittunut pelkästään oppijoihin ja huoltajiin, vaan se koski myös Helsingin kaupungin työntekijöitä sekä vuokratyöntekijöitä, jotka ovat toimineet sijaisina kaupungin kasvatuksen ja koulutuksen toimialalla. Lisäksi vuotaneet tiedot sisälsivät muun muassa työnhakijoiden rekrytointitietoja, toimeksiantosopimuksia sekä hankintasopimuksia. (Helsingin kaupunki, 2025a.) Arvion mukaan tietomurto koski ainakin 150 000 henkilöä, mutta henkilömäärästä ei ole varmuutta ja uhrien kokonaismäärä voi olla jopa

kaksinkertainen eli noin 300 000. Kokonaisuudessaan kovalevyllä ollut tietoa on ollut A4-kokoisia asiakirjoja yli 17 Olympiastadionin tornin verran (Rita, 2025).

F-Securen (2024) artikkelin mukaan tietomurrossa hyödynnettiin etäkäyttöpalvelimen haavoittuvuutta. Haavoittuvuuteen oli saatavilla korjauspäivitys, mutta sen saatavuudesta huolimatta päivitystä ei tehty. Tämä osoittaa, että tietomurron taustalla oli tekninen haavoittuvuus, joka olisi voitu estää ajantasaisella järjestelmänylläpidolla. Kyseinen tapaus on hyvä esimerkki siitä, miten yksittäinen päivityksen laiminlyönti voi johtaa mittaviin tietoturvaloukkauksiin. Helsingin kaupungin It-infrastruktuuri on laaja, ja tapaus osoittaa, kuinka kriittistä on, että tietoturvaprosessit ovat ajantasaiset ja tarkat. (F-Secure, 2024.)

Tietomurroista aiheutuu organisaatioille taloudellisia kustannuksia sekä muuta negatiivista haittaa, kuten huonoa mainetta, luottamusongelmia sekä tietomurrot voivat vaarantaa organisaation pitkän ajan vakauden. (Cheng, Liu & Yao, 2017, 1.) Helsingin kaupungin kasvatuksen ja koulutuksen tapauksessa seuraukset ja vaikutukset ovat laajat. Tapauksen seurauksen rikolliset pystyvät hyödyntämään saamiaan henkilötietoja väärinkäyttöön sekä esimerkiksi kalastelu ja -huijausviesteihin sekä identiteettivarkauksiin. (Helsingin kaupunki, 2025a.) Tietomurrolla on myös taloudellisia vaikutuksia kaupungin toimintaan. Tietomurron seurauksena kaupungin tietoteknisiin toimiin tuli merkittävä kustannus. Lisäkustannuksen hinta kertaluontoisena on arviolta 7,5 miljoonaa euroa vuosien 2025–2029 aikana. Lisäkustannus tapahtui luovutetun liiketoiminnon johdosto, kun kasvatuksen ja koulutuksen toimialan infrapalveluiden yksikön ict-toiminnot luovutettiin DigiHelsingin haltuun. Näin Helsingin kaupunki haluaa varmistaa kasvatuksen ja koulutuksen toimialan tietoturvalliset ja kattavat ict-palvelu jatkossa. (Helsingin kaupunki, 2025b.) Tietomurron seurauksena Helsingin kaupunki on tehnyt asiasta ilmoituksen tietosuojavaltuutetulle, kyberturvallisuuskeskukselle sekä poliisille. Tätä tietomurtoa tutkitaankin törkeänä tietomurtona, ja tutkintatyöt ovat edelleen kesken. (Helsingin kaupunki, 2025a.)

4.1.2 Case 2: Turun kaupungin opetuksen OPAS-ympäristön tietomurtoyritys

Vuonna 2021 Turun kaupungin opetuksen käyttöön tarkoitetun OPAS-verkkopalvelun järjestelmään kohdistui tietomurtoyritys. OPAS-järjestelmä toimii opettajien ja opiskelijoiden välisen yhteydenpidon ja opetuksen järjestämisen alustana. Kyseinen hyökkäys oli osa laajempaa kiristyshaittaohjelman levitysyritystä. Vaikka hyökkäyksen tarkoituksena oli haittaohjelman asentaminen ja kiristystarkoituksessa tapahtuva tiedon salaus, onnistuttiin leviämisyritys estämään tehokkaiden järjestelmän ylläpitoprosessien ansiosta. (Hiltunen, 2021.) Tästä huolimatta hyökkääjät onnistuivat saamaan haltuunsa opettajien ja opiskelijoiden käyttäjätunnuksia.

Tietomurtoyrityksen seurauksena Turun kaupunki ryhtyi välittömiin varotoimenpiteisiin. Kaikkia OPAS-järjestelmän käyttäjiä ohjeistettiin vaihtamaan salasanansa. Salasanan vaihtamisen avulla pyritään minimoimaan riskit, että hyökkääjä pääsisi käyttämään saamiaan tunnuksia hyväksi. Lisäksi järjestelmän teknistä suojausta vahvistetiin, jotta tulevaisuudessa vastaavanlaiset hyökkäykset pystyttäisiin estämään. (Luhtala, 2021.) Turun kaupunki on kuitenkin tapauksen seurauksena vahvistanut tietoturvakäytäntöjään. Myöhemmin vuonna 2024 Turun kaupunki on jatkanut toimiaan tietoturvan parantamiseksi. Turun kaupunki hankki haavoittuvuuksien havainnointiin liittyvän lisäpalvelun, joka pystyy tunnistamaan myös tietoturvariskejä. Tämä viittaa siihen, että hyökkäys saattoi hyödyntää yleisiä tietoturva-aukkoa, kuten päivittämättömiä ohjelmistoja tai järjestelmiä. (Turun kaupunki, 2024.) Kyberrikolliset hyödyntävät tällaisissa kiristyshaittaohjelman levitysyrityksissä päivittämättömien tai vanhentuneiden ohjelmistojen tietoturva-aukkoja, jotta pääsevät käsiksi järjestelmään. Uusimmissa järjestelmissä onkin usein automaattinen päivitystoiminto, jonka avulla ne pysyvät ajan tasalla (Kovács, 2022, 102). Tarkkaa hyökkäyksessä hyödynnettyä haavoittuvuutta ei ole julkistettu (Turun kaupunki, 2024).

Turun kaupungin tietomurto yritys onnistuttiin kuitenkin estämään järjestelmän toimivan ylläpidon ansioista, eikä kiristyshaittaohjelma ehtinyt levitä. Mikäli kiristyshaittaohjelma olisi levinnyt pidemmälle ja haittaohjelma asentunut Turun kaupunki olisi joutunut hankaliin vaikeuksiin. Hyökkääjä olisi voinut salata kaikki OPAS-järjestelmän tiedostot tai poistaa ne, ja esittää lunnasvaatimuksia. Hyökkääjät eivät kuitenkaan yleensä anna purkuavainta järjestelmään, vaikka lunnaat olisi maksettu (Temara, 2024, 2.) Onneksi Turun kaupungilla oli käytössään toimivat järjestelmän ylläpitoprosessit.

4.1.3 Case 3: Oulun kaupungin kryptokaappaus

Vuonna 2022 Oulun kaupunki joutui kryptokaappauksen kohteeksi, jolloin kaupungin verkkosivut olivat haitallisen hyökkäyksen kohteena. Kryptokaappaus tarkoittaa tilannetta, jossa verkkosivuston kävijöiden tietämättä heidän tietokoneitaan käytetään kryptovaluutan louhintaan. Oulun kaupungin verkkosivujen koodiin oli asennettu haittaohjelma, joka aktivoitui, kun käyttäjä avasi sivuston. Tämän jälkeen kryptovaluutan louhinta alkoi. Haittaohjelma ehti olla kaupungin verkkosivuilla vain vuorokauden, ennen kuin se huomattiin epäilyttävän verkkoliikenteen vuoksi. Kyseinen hyökkäys johtui todennäköisimmin Oulun kaupungin verkkosivujen tietoturvaongelmasta, johon kryptovaluutan louhijat usein iskevät. Ongelma saatiin kuitenkin nopeasti havaittua ja verkkosivut korjattua entiselleen. (Heikinmatti, 2022.)

Oulun kaupungin verkkosivujen koodin asennettu haittaohjelma on todennäköisemmin ollut JavaScript-pohjainen louhintakoodi, joka käyttää hyväkseen sivustolla vierailleiden henkilöiden laskentatehoa salaisesti kryptolouhintaan. Tätä tekniikkaa kutsutaan myös nimellä kryptojacking.

Tämän kaltainen hyökkäys voidaan toteuttaa pelkästään verkkosivujen avaamisella ilman, että käyttäjä tekee sivulla mitään aktiivista toimintaa. Tämä on myös luvattoman taloudellisen hyödyn saavuttamista ilman käyttäjän suostumusta. (Wu, Lai, Hwang, Chang & Hsu, 2022, 4-5.) Vaikka kyseinen rikollinen ei saanut varastettua sivustoilla vierailleiden henkilöiden tietoja, heikensi tämä kuitenkin käyttäjien yleistä luottamus Oulun kaupungin verkkopalveluiden tietoturvaan. Tämä voi vaikuttaa jatkossa siihen, kuinka käyttäjät suhtautuvat kaupungin verkkopalveluihin jatkossa.

Kryptokaappaus myös heikentää käyttäjien laitteiden suorituskykyä, ja laitteet kuluttivat enemmän virtaa kryptolouhinnan seurauksena. Krytojacking on yleisesti vielä haitallisempaa organisaatioille, mikäli organisaation tietokoneklusteri saatuisi. Tämä aiheuttaisi organisaatiolle mittavia taloudellisia vahinkoja, jotka liittyisivät sähkön lisäkulutukseen sekä koko prosessoriyksikön vaihtoon, mikäli kryptojacking olisi jatkunut sivustolla pitkään. (Tanana, 2020, 543.) Ongelman nopea havainnointi estikin suurimmat menetykset sekä vahingot Oulun kaupungille sekä muille sivustoa käyttäneille uhreille. Tapaus toimi myös hyvänä esimerkkinä tietoturva ongelmien vaikutuksesta, ja niihin liittyvien nopeiden toimenpiteiden merkityksestä organisaatioille.

4.1.4 Case 4: Vanamo kirjastopalveluiden tietomurto

Vuonna 2021 Hämeenlinnan seudun Vanamon-kirjaston palvelut joutuivat tietomurron kohteeksi, kun kirjastojärjestelmään kohdistui kiristyshaittaohjelmahyökkäys. Hyökkäyksen seurauksena Vanamo-järjestelmä oli poissa käytöstä. Asiakkaat eivät päässet kirjautumaan omiin tietoihinsa tai tekemään varauksia tai uusimaan lainojaan. Myös kirjaston teosten saatavuustiedot eivät olleet näkyvissä asiakkaille. (Niskanen, 2021.) Järjestelmän toimimattomuuden vuoksi kaikki kirjaston palvelut olivat poissa noin viikon ajan. Kirjaston asiakkaiden tiedot säilyivät kuitenkin järjestelmässä, eikä kiristyshaittaohjelman hyökkäyksen seurauksena ole ilmennyt merkkejä tietojen vaarantumisesta tai vuotamisesta. Tapahtuman seurauksena kirjaston palvelut siirrettiin uuteen turvallisempaan ympäristöön, joka mahdollisti jatkossa järjestelmän käytön ilman vastaavia riskejä. (Lassheikki, 2021.)

Kiristyshaittaohjelmahyökkäys on voinut tapahtua useasta syystä Hämeenlinnan seudun Vanamo-kirjasto palveluun. Julkisuuteen ei ole tuotu millainen haittaohjelma Vanamon-kirjasto palveluiden tapauksessa oli kyseessä. Mutta yleisin syy kiristyshaittaohjelmahyökkäykselle on päivittämättömät ohjelmistot tai järjestelmät. Kyberrikolliset hyödyntävät usein vanhoissa tai päivittämättömissä käyttöjärjestelmissä olevia tietoturva-aukkoa kohteenaan. Hyökkääjät voivat näin hyödyntää useita eri tekniikoita, kuten etäkoodin suorittamista järjestelmään, jonka avulla hyökkääjät pääsevät järjestelmään. (Kovács, 2022, 101-102.) Samoin kuin Helsingin kaupungin kasvatuksen ja koulutuksen tapauksessa, myös tämä on hyvä esimerkki siitä, miten tärkeää on pitää järjestelmät ja ohjelmistot ajantasaisesti päivitettyinä, jotta vastaavia tapauksia voidaan estää tulevaisuudessa.

Tapauksen seurauksena Vanamo kirjaston palvelut olivat poissa käytössä, joka aiheutti kirjaston asiakkaille haittaa. Tämä voi vaikuttaa esimerkiksi asiakastyytyväisyyteen. Kirjasto kuitenkin ilmoitti ja viesti asiakkaitaan selkäesti, ja ohjeisti että kirjastoon voi olla myös yhteydessä puhelimitse sekä sähköpostitse. (Lassheikki, 2021.) Niin kuin Oulun kaupungin OPAS-ympäristön kiristyshaittaohjelma hyökkäyksessä, niin tässäkin todennäköisimmin hyödynnettiin tietoturva-aukkoa. Uhkan leviämisen estämiseksi organisaatioiden onkin priorisoitava kyberturvallisuuteen, kuten ohjelmistojen säännölliseen päivittämiseen sekä henkilöstön koulutukseen, jotta voidaan jatkossa estää vastaavanlaiset tapaukset (Kovács, 2022, 102-103.)

4.1.5 Case 5: Kelan kalasteluviestit

Kansaneläkelaitos (Kela) on varoittanut asiakkaitaan kalastelu- ja huijausviesteistä, joita on lähetetty rikollisten toimesta Kelan nimissä. Kalasteluviestien avulla rikolliset pyrkivät saamaan haltuunsa suomalaisten henkilötietoja, kuten pankkitunnuksia. Viesteissä on pyydetty muun muassa muuttamaan sairausvakuutustietoja Kelan kautta. Viesteihin on sisällytetty usein linkkejä, jotka ohjaavat henkilön huijaussivustolle. Sivustot saattavat näyttää erittäin uskottavilta, mikä voi hämätä henkilöä luulemaan sivustoa aidoksi. Sivustoilla on hyödynnetty Kelan logoja sekä Kelan sivuston tyypillistä värimaailmaa. Mikäli käyttäjä klikkaa viestissä olevaa linkkiä ja päätyy syöttämään henkilökohtaisia tietojaan huijaussivustolle, tiedot päätyvät suoraan rikollisten käsiin. Tämän vuoksi on myös syytä tarkastella verkkopalvelun URL-osoitetta, jotta se ei sisällä epäilyttäviä lisämerkkejä, mikä voi viitata huijaussivustoon. (Taskinen, 2025.) Tämän esimerkin myötä käyttäjän on tärkeää olla tarkkana viestien aitouden suhteen ja varmistaa, että tiedonanto ja yhteydenpito virallisten tahojen kanssa tapahtuu luotettavissa sekä oikeissa kanavissa ja ympäristössä.

Kalastelu- ja huijausviestejä lähetetään jatkuvasti, ja niitä pyritään tekemään yhä uskottavimmiksi. Kalasteluviestit ovat uhrin sosiaalista manipulointia, jonka avulla pyritään saamaan henkilökohtaista tietoa uhrilta. Rikolliset yrittävät vaikuttaa uhriin erilaisin psykologisin keinoin ja manipuloiden. Tällaisissa tapauksissa kalasteluviestien lähettäjät pyrkivät osumaan ihmisten sosiaalisiin haavoittuvuuksiin. Kalasteluviesteissä on yleisesti hyödynnetty vakuuttumistekniikkaa, jonka avulla uhri pyritään vakuuttamaan viestin oikeudesta ja kiireellisyydestä. Näin kalasteluviestien lähettäjät varmistavat, että uhri uskoisi kalasteluviestin sisällön. Kalasteluviestit ovat aina inhimillinen tekijä, eivätkä johdu teknisistä puutteista, sillä viestien lähettäjinä toimivat ulkopuoliset rikolliset. (Valecha, Mandaokar & Rao, 2021, 747-748.)

Kalasteluviestin seurauksena Kela on joutunut varoittamaan asiakkaitaan huijausviesteistä. Kela myös muistuttaa asiakkaitaan, ettei lähetä teksti- tai sähköpostiviesteissään asiakkaille linkkejä. Huijausviesteissä olevia linkkejä ei tule ikinä avata tai niitä saanut uhri voi joutua ongelmiin (Taskinen, 2025). Kelan tapauksessa ei ole tapahtunut tietojen vaarantumista, mikäli viestin saanut

henkilö ei ole antanut henkilökohtaisia tietojaan huijaussivustolle. Mikäli henkilö olisi antanut tietojaan huijaussivustolle, olisi hän joutunut todellisiin vaikeuksiin. Kalasteluhyökkäykset ovat uhrille aina taloudellinen menetys, sillä rikolliset voivat esimerkiksi hakea lainaa henkilötunnuksen perusteella henkilön niissä itselleen. Uhrille aiheutuu tästä myös henkilökohtaisia kustannuksia mukaan lukien ajan menetystä, stressiä sekä luottamuksen heikentymistä organisaatiota kohtaan (Kelley, Hong, Mayhorn & Murphy–Hill, 2012, 2108.)

4.2 Organisaatioiden reaktiot ja jälkitoimet

Tietomurto tapausten seurauksena organisaatioiden täytyy reagoida tapauksiin. Tietomurrot asettavat organisaatiolle erityisiä haasteita liittyen tietoturvaan, rikoksen tutkintaan, toiminnan palauttamiseen normaaliksi sekä mahdollisten uusien hyökkäyksien estämiseen ja ehkäisemiseen. Organisaatioiden onkin tärkeä tehdä jälkitoimia myös murtoon johtaneen perimmäisen syyn selvittämiseksi, jotta uusia hyökkäyksiä voidaan minimoida. (Gwebu, Wang & Wang, 2018, 683-684.)

Jokaisessa case tapauksessa organisaatiot onnistuivat ammattimaisessa viestinnässä tietomurron uhreille. Tiedotteen julkaiseminen ja viestintä ovat erittäin tärkeitä tällaisissa tapauksissa, jotka koskevat henkilötietoja. Helsingin kaupunki julkaisi pikimmiten tiedotteen verkkosivuilleen, jossa kerrotaan kaikki oleellinen liittyen tietomurto tapaukseen. Tiedotteessa kerrotaan, ketä tietomurto koskee ja kuinka heidän tulee toimia tilanteessa. Tiedotteessa varoitettiin tietomurron uhreja henkilötietojen väärinkäytöstä, joka on valitettava ja vakava riski tämän tasoisessa tietomurrossa. (Helsingin kaupunki, 2025a.) Myös F-Securen (2024) laatimassa tiedotteessa kerrotaan mitä uhrit voivat tehdä suojautuakseen, ja kuinka uusiin mahdollisiin tuleviin tietomurtoihin voi suojautua. Organisaation viestintä uhreille oli onnistunutta, ja sen avulla uhrit pystyvät tekemään omat parhaat toimenpiteensä tietomurron jälkeen. Helsingin kaupungin tapauksessa ryhdyttiin myös välittömiin suojaus toimenpiteisiin, jonka avulla murtautujan toiminta onnistuttiin estämään nopeasti havaitsemisen jälkeen. Tämän jälkeen murtautujasta ei ole ollut havaintoja. Helsingin kaupunki on tehostanut valvontaa kaikissa kaupungin tietoverkoissa tapauksen jälkeen. Vastaavien murtojen estämiseksi kaupunki on edistänyt myös tiedonhallinnan, tietoturvan ja tietosuojan toimenpiteitä niiden parantamiseksi. Kaupunki on myös selkeyttänyt tietoturvajohtamisen vastuualueita, jotta niiden hallinta olisi mahdollisimman tehokasta. (Helsingin kaupunki, 2025a.) Helsingin kaupungin reagointi ja jälkitoimet ovat olleet kattavia, ja tapaus onkin edelleen poliisin tutkinnassa.

Turun kaupungin OPAS-ympäristön tapauksessa organisaation nopea ja kohdennettu toiminta olivat avain hyökkäyksen leviämisen estämiseen. Turun kaupunki toimi läpinäkyvästi tapauksessa ja tiedotti käyttäjiään nopeasti viestinnällä. Teknisen suojauksen vahvistamisen sekä jatkuvan tietoturvan kehityksen avulla pystytään hallitsemaan tulevaisuuden uhkia tulevaisuudessa tehokkaasti (Turun kaupunki, 2024). Tietomurtotapaukset paljastavat kuitenkin organisaation järjestelmien ja

hallinnan heikkoudet, joten on tärkeää reagoida nopeasti tapauksiin (Gwebu, Wang & Wang, 2018, 684). Turun kaupunki tarjosi hyvän esimerkin vahinkojen hallinnasta nopean reagoinnin, tiedotuksen ja järjestelmien kehityksen avulla.

Samoin kuin Turun kaupungin tapauksessa, myös Oulun kaupungin tapauksessa organisaation nopea ja välitön reagointi auttoivat tilanteen palauttamisessa, kun tapaus havainnoitiin epäilyttävän verkkoliikenteen vuoksi. Verkkosivut saatiin myös palautettua normaaliksi ilman pysyviä vahinkoja. (Heikinmatti, 2022.) Kryptojacking tapausten estämiseksi on kehitetty mustalistasuodattimia, jonka avulla kyseisiä kryptolouhinta tapauksia voidaan estää tehokkaasti. Minerblock on lisäosa verkkoselaimeen, joka aktivoituu, kun selain lataa verkkosivun. Mikäli sivusto sisältäisi JavaScript muotoisen koodin, kuten Oulun kaupungin tapauksessa, laukaisee Minerblock estotoiminnon, joka estää käyttäjää pääsemästä käsiksi sisältöön. Tämä on tehokas keino estää kryptolouhinta tapauksia. (Wu, Lai, Hwang, Chang & Hsu, 2022, 6-8.)

Hämeenlinnan Vanamon-kirjastopalveluiden kiristyshaittaohjelmahyökkäyksessä organisaatio reagoi välittömästi sulkemalla järjestelmän, jotta haittaohjelman leviäminen saatiin estettyä. Myös palveluiden siirtäminen uuteen turvallisempaan ympäristöön oli turvallinen ja tehokas ratkaisu. Tapausten estämiseksi tulevaisuudessa Vanamon-kirjastopalveluiden organisaation on tärkeää ylläpitää ajankohtaisia päivityksiä ajan tasalla sekä kouluttaa henkilöstöä tietomurtojen varalle (Kovács, 2022, 102.) Kiristyshaittaohjelmien toteuttamisen helppous onkin yksi niiden onnistumisen edellytys. Vanamon-kirjaston tapauksessa organisaation riittämätön tietoturva voi aiheuttaa tämänkaltaisen hyökkäyksen. Kiristyshaittaohjelmien estämiseksi ja ehkäisemiseksi organisaation henkilöstön on saatava kattava koulutus näitä hyökkäyksiä vastaan. Yksikin heikosti kouluttautunut henkilö organisaatiossa voi johtaa kiristyshaittaohjelmahyökkäyksen onnistumiseen. (Temara, 2024, 6-7.)

Kelan kalasteluviestien seurauksena organisaation täytyi viestiä välittömästi asiakkaitaan ja varoittaa liikkeellä olevista huijaus- ja kalasteluviesteistä. Tapausten estäminen on haastavaa, sillä rikolliset keksivät jatkuvasti uusia keinoja huijata uhrejaan. Huijaussivustoista tehdään aidomman näköisiä ja viesteistä yritetään tehdä mahdollisimman uskottavia. Uhrit ovat kuitenkin tietoturvan heikoin lenkki tietomurron onnistumiseksi (Valecha, Mandaokar & Rao 2021, 747.)

Nämä keinot ovat tärkeitä uusien tietomurtojen ehkäisemiseksi, sillä täydellinen tietoturvariskien ehkäisy on käytännössä täysi mahdottomuus. Tehokkaiden palautumis- ja vahinkojenhallinta keinojen avulla organisaatio pystyy suojelemaan toimintaansa parhaiten. Organisaatioiden on tärkeä pystyä ennaltaehkäisemään tapauksia, sillä niiden kohteeksi joutuneena he kärsivät taloudellisesti tappiota esimerkiksi korvausten tarjoamisesta sekä oikeudellisten velvoitteiden täyttämisestä liittyen rikostutkintaa. Tietomurrot vaikuttavat kokonaisuudessa myös organisaation asiakastyytyväisyyteen sekä brändikuvaan. Organisaatioiden anteeksipyyntö tietomurtotapauksista ovat yksi

tehokkaimmista keinoista säilyttää luottamus ja maine jatkossa organisaatiota kohtaan. (Gwebu, Wang & Wang, 2018, 684.)

5 Tutkimustulokset

Tässä luvussa esitellään tutkimuksentulokset, jotka on ryhmitelty aihealueittain omiin alakappaleisiinsa. Alakappaleet on muodostettu vastaamaan tutkimuksen alaongelmiin numerojärjestyksessä. Tutkimuksessa pyritään vastaamaan kysymykseen: Ovatko julkisen sektorin tietojärjestelmät alttiita tietomurroille?

Tutkimuksen alaongelmat:

1. Miksi julkisen sektorin tietojärjestelmät ovat olleet alttiita tietomurroille?
2. Millaisia tietomurtoja julkisen sektorin tietojärjestelmiin on tehty viime vuosina?
3. Mitä haavoittuvuuksia hyödynnettiin julkisen sektorin tietomurroissa?
4. Mitkä tietoturvakäytännöt ovat osoittautuneet tehokkaimmiksi estämään tietomurtoja?
5. Miten organisaatiot voivat tehokkaasti ehkäistä ja hallita näitä uhkia?

5.1 Tulokset liittyen tietojärjestelmien haavoittuvuuteen

Q1: Miksi julkisen sektorin tietojärjestelmät ovat olleet alttiita tietomurroille?

Julkisten sektorin tietojärjestelmät ovat alttiita tietomurroille useiden teknisten ja inhimillisten tekijöiden vuoksi. Tutkimuksen perusteella yksi keskeinen syy on riittämätön varautuminen kyberuhkiin. Teknologisesta näkökulmasta järjestelmissä voi esiintyä suojaamattomia yhteyksiä, päivittämättömiä ohjelmistoja tai järjestelmiä sekä puutteellista valvontaa, jotka mahdollistavat tietomurto hyökkäysten toteutumisen. Kun järjestelmiä ei pidetä ajan tasalla päivitysten avulla, jää niihin usein haavoittuvuuksia, joita hyökkääjät voivat hyödyntää helposti tietomurtoihin. Useissa tutkimissani tapauksissani hyökkäykset onnistuivat juuri hyödyntämällä näitä teknisiä haavoittuvuuksia.

Lisäksi inhimilliset tekijät vaikuttavat tietojärjestelmien alttiuteen tietomurroille. Inhimilliset tekijät korostuvat erityisesti sosiaalisen manipuloinnin muodossa, kuten tietojenkalastelussa, jossa käyttäjää yritetään johdattaa harhaan ja näin luovuttamaan henkilökohtaisia sekä arkaluontoisia tietojaan. Inhimilliset tekijät toimivat usein tietomurron onnistumisen kriittisenä pisteenä, vaikka organisaation tekninen suojaus olisikin kunnossa. Yritysten järjestelmien haavoittuvuus ei siis johdu yksittäisistä puutteista, vaan monipuolisesta kokonaisuudesta, jossa sekä tekninen että koko organisaation osaaminen vaikuttavat suoraan tietoturvan tasoon.

Voidaan todeta, että tietojärjestelmien alttius tietomurtoihin johtuu kokonaisvaltaisesta tietoturvan puutteesta, niin teknisestä kuin organisaattorisesta näkökulmasta. Tietoturva vaatii jatkuvaa kehittämistä, valvontaa sekä ennaltaehkäisevää suunnittelua.

5.2 Tulokset liittyen tehtyihin tietomurtoihin

Q2: Millaisia tietomurtoja julkisen sektorin tietojärjestelmiin on tehty viime vuosina?

Julkisen sektorin tietojärjestelmiin on tehty viime vuosina useita erilaisia tietomurtoja. Tietomurrot ovat johtaneet muun muassa arkaluontoisten tietojen vuotamiseen, taloudellisiin menetyksiin sekä luottamuksen heikentymiseen julkisen sektorin organisaatiota kohtaan.

Tutkimuksessa analysoitiin julkisen sektorin tietomurtoja case-tapauksien avulla. Tutkimuksen perusteella tehdyt tietomurrot voidaan jakaa neljään kategoriaan: tietovuoto, kiristyshaittaohjelmahyökkäys, kryptojacking-hyökkäys sekä sosiaalisen manipulointi. Taulukossa 2. on esitetty ja havainnoitu millaisia tietomurtoja julkisen sektorin case tapauksien 1–5 tietojärjestelmiin on tehty.

Taulukko 2.

	Case 1	Case 2	Case 3	Case 4	Case 5
Tietovuoto	X				
Kiristyshaittaohjelma-hyökkäys		X		X	
Kryptojacking-hyökkäys			X		
Sosiaalinen manipulointi					X

Tutkimuksen perusteella voidaan todeta, että tietojärjestelmiin on tehty useimmiten kiristyshaittaohjelmahyökkäyksiä. Kiristyshaittaohjelma hyökkäykset ilmenivät kahdessa tapauksessa viidestä, eli 40% tapauksista. Muut tietomurtojen muodot – tietovuoto, kryptojacking ja sosiaalinen manipulointi - ilmenivät kukin vain yhdessä tapauksessa.

Tämä viittaa siihen, että kiristyshaittaohjelmahyökkäykset ovat tällä hetkellä keskinen uhka julkisen sektorin tietojärjestelmille. Muiden hyökkäystyyppien yksittäiset esiintymät osoittavat, että tietoturvauhat ovat monipuolisia ja jatkuvassa kehityksessä. Julkisen sektorin organisaatioiden tuleekin varautua monipuolisesti erilaisiin hyökkäystapoihin, jotta heillä on valmius toimia mahdollisen uhan tai hyökkäyksen alkaessa.

5.3 Tulokset liittyen hyödynnettyihin haavoittuvuuksiin

Q3: Mitä haavoittuvuuksia hyödynnettiin julkisen sektorin tietomurroissa?

Julkisen sektorin tietomurroissa hyödynnettiin useita erilaisia haavoittuvuuksia. Tietomurroissa hyödynnetyt haavoittuvuudet voidaan jakaa kolmeen pääkategoriaan niiden yleisyyden mukaan tapauksissa: järjestelmän päivittämättömyys, yleiset tietoturvaongelmat sekä inhimilliset tekijät.

Alla olevassa Taulukossa 3. on havainnoitu yleisimmin hyödynnetyt haavoittuvuudet organisaatioiden case tapauksista 1–5.

Taulukko 3.

	Case 1	Case 2	Case 3	Case 4	Case 5
Järjestelmän päivittämättömyys	X	X		X	
Tietoturvaongelmat	X	X	X		
Inhimilliset tekijät					X

Taulukon sekä tutkimuksen perusteella useissa tapauksissa hyökkäykset onnistuivat, koska järjestelmät eivät olleet ajan tasalla. Tämä ilmeni kolmessa case tapauksessa viidestä, eli prosentuaalisesti 60%. Järjestelmien päivittämättömyyden vuoksi järjestelmiin on voinut jäädä aukkoja, joita ei ole korjattu päivityksistä huolimatta. Päivittämättömät järjestelmät mahdollistavat haavoittuvuuksista hyötymisen, jolloin hyökkääjien ei tarvitse käyttää edistynyttä tekniikkaa murtautuakseen järjestelmiin onnistuneesti. Tämä mahdollistaa hyökkääjien nopean ja tehokkaan toiminnan ja näin edistää tietomurron toteutumista.

Tietoturvaongelmat ilmenivät myös kolmessa case-tapauksessa viidestä, eli 60% tutkituista tapauksista, ja muodostavat näin yhden yleisimmän hyödynnetyn haavoittuvuuden tutkimuksessa. Tietoturvaongelmien sekä tietoturvan heikkouden vuoksi hyökkääjät onnistuivat iskemään organisaatioiden järjestelmiin, jotka saattoivat ulottua syvälle organisaation toimintaan ja tietovarantoihin.

Tutkituista tapauksista yhdessä korostuivat inhimilliset tekijät, jotka liittyvät tietojenkalasteluun. Eli 20% tutkituista tapauksista. Tällöin kyse on käyttäjän toiminnasta, joka voi mahdollistaa tietomurron onnistumisen. Inhimillisiä tekijöitä on erityisen haastava torjua, sillä se vaatii jatkuvaa koulutusta ja tietoisuuden ylläpitoa koko organisaatiossa. Tämä osoittaa, että teknisten haavoittuvuuksien lisäksi myös käyttäjien toiminta voi avata reitin tietomurtoon. Näiden haavoittuvuuksien tunteminen on tärkeää ja keskeistä suunnitellessa ennaltaehkäiseviä toimenpiteitä.

Tuloksien perusteella voidaan todeta, että teknisten suojausten ohella myös organisaation toimet sekä inhimilliset tekijät ovat keskeisessä roolissa tietoturvan kokonaisvaltaisessa hallinnassa. Näiden haavoittuvuuksien tunnistaminen ja niihin puuttuminen on kriittistä ja tärkeää, mikäli vastaavia uhkia halutaan ehkäistä tehokkaasti myös tulevaisuudessa.

5.4 Tulokset liittyen tehokkaimpiin tietoturvakäytäntöihin

Q4: Mitkä tietoturvakäytännöt ovat osoittautuneet tehokkaimmiksi estämään tietomurtoja?

Tehokkaimmat tietoturvakäytännöt tietomurtojen estämiseksi perustuvat useiden toimenpiteiden yhdistelmään. Tutkituissa tapauksissa tehokkaimmiksi tietoturvakäytännöiksi osoittautuivat organisaatioiden nopea reagointi, tehokas viestintä, teknisen suojauksen kehittäminen sekä henkilöstön kouluttaminen. Organisaatioiden nopean ja johdonmukaisen reagoinnin vuoksi tietomurtotapauksia pystytään estämään tehokkaasti. Tähän kuuluvat muun muassa järjestelmien sulkeminen tarpeen mukaan ja tarvittavien suojaustoimenpiteiden käynnistäminen välittömästi, joiden avulla hyökkäysten eteneminen sekä vahinkojen tapahtuminen voidaan estää nopeasti. Samanaikaisesti avoin ja ajantasainen viestintä tietomurron uhreille on osoittautunut tärkeäksi keinoksi ylläpitää luottamusta ja ohjeistaa uhreja suojatumaan mahdollisilta väärinkäytöiltä.

Tietomurtojen estämiseksi organisaatioiden on myös jatkuvasti kehitettävä teknistä suojaustaan. Teknisen suojauksen kehittämisessä keskeisiä toimenpiteitä ovat olleet valvontajärjestelmien tehostaminen, haitallisen verkkoliikenteen estävän suodatusmekanismin käyttöönotto sekä selainlaajennusten hyödyntäminen haittakoodien torjumiseksi. Lisäksi organisaatiot ovat parantaneet tietoturvan ja tietosuojan hallintaa myös strategisesti selkeyttämällä tietoturvan vastuualueita sekä päivittämällä tietosuojakäytännöt ajan tasalle.

Henkilöstön koulutus nousi tutkimuksessa myös yhdeksi keskeisimmistä tekijöistä tietomurtojen estämiseksi. Henkilöstön säännöllinen ja ajantasainen koulutus on olennainen osa tietoturvan kokonaisuutta. Organisaation henkilöstön tulee ymmärtää ja osata tunnistaa esimerkiksi kalasteluviestien tunnusmerkit, sekä muut yleiset tietoturvauhat, jotta heidän toimintansa ei altista organisaatiota hyökkäyksille. Näiden käytäntöjen yhdistelmä muodostaa tehokkaan suojan tietomurtojen estämiseksi.

5.5 Tulokset liittyen tietomurtojen ehkäisyyn ja hallintaan

Q5: Miten organisaatiot voivat tehokkaasti ehkäistä ja hallita näitä uhkia?

Tutkimuksen perusteella organisaatioiden tehokkaimmat tavat ehkäistä ja hallita näitä uhkia perustuvat sekä ennakoiviin että reaktiivisiin toimiin. Ennakoivasti organisaatioiden tulee varmistaa järjestelmien ajantasaisuus päivittämällä käytössä olevat järjestelmät ajan tasalle. Organisaatioiden täytyy myös vahvistaa teknistä suojausta sekä selkeyttää tietoturvan eri osa-alueiden vastuunjakoa, jotta tietoturvan hallinta on mahdollisimman tehokasta. Henkilöstön säännöllinen koulutus ja tietoisuuden lisääminen ovat keskeisiä keinoja estää inhimillisten virheiden kautta tapahtuvia hyökkäyksiä. Kun tietomurto tapahtuu, täytyy organisaatioiden keskittyä reaktiivisiin toimiin. Se vaatii organisaatioilta nopeaa reagointia, kuten järjestelmien sulkemista tarvittaessa, tiedottamista tapahtuneesta sekä teknisien suojaustoimien aloittamista. Nämä toimenpiteet ovat ratkaisevia vahinkojen rajoittamisen kannalta. Organisaatioiden tulee myös analysoida ja selvittää tietomurtoon johtaneet syyt ja kehittää toimintaansa jatkuvasti estääkseen tapauksia. Viestintä uhreille ja julkinen anteeksipyyntö tapauksista voivat säilyttää luottamusta ja minimoida organisaation imagohaitat. Näiden keinojen avulla organisaatiot voivat sekä ehkäistä tulevia uhkia että hallita niiden vaikutuksia tehokkaasti.

5.6 Johtopäätökset

Tutkimustulosten perusteella voidaan tehdä useita johtopäätöksiä liittyen julkisen sektorin tietomurtoihin. Merkittävimmät tietomurtoja edistävät tekijät ovat tekniset haavoittuvuudet, kuten järjestelmien päivittämättömyys sekä tietoturvaongelmat. Myös inhimilliset tekijät, kuten sosiaalinen manipulointi altistaa tietomurroille. Tietomurrot ovat olleet monimuotoisia, ja erityisesti kiristyshaittaohjelmahyökkäykset nousivat tutkimuksessa yleisimmäksi hyökkäystyypiksi. Haavoittuvuuksien hyödyntäminen liittyi useimmiten päivittämättömiin järjestelmiin ja yleisiin tietoturvaongelmiin, joita esiintyi suurimmassa osassa tarkastelluissa case-tapauksissa. Vaikka tehokkaita tietoturvakäytäntöjä, kuten nopeaa reagointia, henkilöstön kouluttamista ja teknisen suojauksen kehittämistä, on pystytty toteuttamaan ja soveltamaan, on niiden käytössä vaihtelevuutta eri julkisen sektorin organisaatioiden välillä.

Tutkimustulosten perusteella voidaan vastata myös tutkimuksen pääkysymykseen: Ovatko julkisen sektorin tietojärjestelmät alttiita tietomurroille? Tutkimuksen perusteella voidaan todeta, että julkisen sektorin organisaatiot ovat alttiita tietomurroille. Tämä alttius ei johdu kuitenkaan yksittäisistä puutteista, vaan muodostuu kokonaisvaltaisesti tietoturvan hallinnan ja ylläpidon haasteista. Nämä haasteet vaativat sekä teknisten että organisaattoristen toimien jatkuvaa kehittämistä. Organisaatioiden tulee systemaattisesti tunnistaa, ehkäistä ja hallita tietoturvauhkia, jotta tulevaisuudessa

näihin uhkiin voidaan vastata entistä tehokkaammin sekä uhkia pystytään estämään mahdollisimman hyvin.

6 Yhteenveto ja pohdinta

Tässä luvussa esitetään tutkimuksen yhteenveto ja pohdinta. Lisäksi pohditaan tutkimuksen luotettavuutta sekä oman oppimisen arviointia opinnäytetyöprosessin ajalta. Lopussa mietitään jatkotutkimusideoita aiheelle.

6.1 Pohdinta

Tutkimuksen tulokset osoittavat, että julkisen sektorin tietojärjestelmät ovat haavoittuvaisia monipuolisille kyberuhille. Tämän tutkimuksen perusteella julkisen sektorin tietomurrot johtuvat sekä teknisistä että inhimillisistä tekijöistä. Vaikka tutkimuksessa tunnistettiin myös tehokkaita tietoturvakäytäntöjä tietomurtojen torjumiseksi, on tärkeää tarkastella organisaatioiden toimintakulttuuria sekä pitkäjänteistä kehittämistyötä osana tietoturvan kehitystä.

Yksi keskeinen pohdinnan aihe on julkisen sektorin organisaatioiden kyky tunnistaa heidän oma kyberturvallisuuden tasonsa. Useassa case-tapauksessa tekninen suojaus saattoi olla olemassa, mutta käytännön tasolla sen käytössä oli puutteita, joko osaamisen tai selkeiden tietoturvallisuuden vastuualueiden jaon vuoksi. Tämä vaikuttaa siihen, miten organisaatiot arvioivat ja mittaavat omaa tietoturvaansa. Kysymys herää myös voisivatko julkisen sektorin organisaatiot kehittää näitä mittareita luotettavammiksi sekä toimivammiksi.

Tulosten pohjalta pohdinnan aiheeksi nousi myös esiin olisiko julkisen sektorin organisaatioilla tarve laajemman strategian yhteistyölle. Julkisen sektorin organisaatiot voisivat hyötyä enemmän keskinäisistä tietoturvayhteistöistä, esimerkiksi jakamalla havaintoja uhkista tai järjestämällä yhteisiä koulutuksia liittyen tietoturvaan ja tietoturvauhkiin. Tällainen yhteistyö muiden julkisen sektorin organisaatioiden kanssa voisi lisätä kollektiivista vastuunkantoa kyberuhkia vastaan.

Pohdittavaa herätti myös koulutuksen vaikuttavuus julkisen sektorin organisaatioissa. Pelkkä koulutuksen tarjoaminen ei automaattisesti kuitenkaan takaa parempaa tietoturvakäyttäytymistä, vaan tarjoaa lisätietoa ja mahdollisuuksia oppia uutta. Julkisen sektorin organisaatioiden olisikin hyvä pohtia, miten koulutusta voidaan muotoilla motivoivammaksi, käytännönläheisemmäksi sekä jatkuvaksi oppimiseksi osana arkea ja työtä. Tämä voi auttaa muuttamaan tietoturvaa velvollisuudesta aidoksi osaksi työyhteisön kulttuuria.

6.2 Tutkimuksen luotettavuus

Tutkimuksen tavoitteena oli vastata kysymykseen ovatko julkisen sektorin tietojärjestelmät alttiita tietomurroille, sekä tavoitteena oli myös saada vastaukset pääkysymyksen viiteen eri alaongelmaan. Tutkimuksen tavoitteessa onnistuttiin ja vastaukset tutkimuskysymykseen sekä alaongelmiin

saavutettiin. Vastaukset tutkimuskysymyksiin ja sen alaongelmiin ovat selkeitä, johdonmukaisia sekä ekspliittisiä. Vastausten luotettavuudesta voidaan olla varmoja näiden case tietomurtotapausten kohdalla, mutta laajemman skaalan tutkimuksella olisi saatu luotettavampia tutkimustuloksia, kun otanta case tapauksista olisi ollut suurempi. Suurempi tapausten määrä olisi antanut luotettavammat tulokset tietomurtotapauksista julkisella sektorilla. Tämän tutkimuksen case tapauksien määrä oli 5, mutta mikäli tutkittavia tapauksia olisi ollut esimerkiksi 15, olisi saatu luotettavampia tuloksia aiheeseen liittyen. Joten voidaan todeta myös, että tämän tutkimuksen tulokset ovat osin myös suppeita.

Tutkimuksen tietoperusta antoi tukevaa tietoa tutkimuksen aihealueen tueksi, ja nojasi ajankohtaisiin sekä luotettaviin lähteisiin. Tutkimuksessa käytetyt lähteet ovat myös luotettavia ja perustuvat vertaisarvioituihin artikkeleihin sekä alan tutkimuksiin. Lähteiden käyttö oli myös monipuolista ja runsasta.

Vaikka tutkimus näistä tutkituista tapauksista oli perusteltu, pienellä tapausotannalla ei voida tehdä kovin laajoja tuloksia ja johtopäätöksiä koko julkisen sektorin tietojärjestelmien tietomurroista. Tutkimuksen luotettavuutta olisi lisännyt tapausten määrän lisääminen. Tutkimuksen tulokset kuitenkin vastaavat tutkimuskysymyksiin, ja ne antavat realistisen kuvan tutkimuksessa käsitellystä ilmiöstä. Lisäksi tutkimuksen rajaukset ja analyysimenetelmät, on esitetty realistisesti ja suoraan, mikä tukee tutkimuksen sisäistä luotettavuutta.

6.3 Opinnäytetyön ja oman oppimisen arviointi

Opinnäytetyön tekeminen oli itselleni osittain haastava oppimisprosessi. Se kuitenkin kehitti itseäni ja omaa osaamistani monella eri osa-alueella. Opinnäytetyöprosessin aikana opin erityisesti projektin hallintaa, jossa tavoitteiden asettelu, aikataulutus sekä asioiden priorisointi olivat merkittävässä roolissa. Aikatauluttaminen ja opinnäytetyön priorisointi olivat itselleni osittain haastavia, sillä viikkotasolla aikaa kului muuhunkin kuten töihin opiskelun ohella. Oli kuitenkin tärkeää osata priorisoida opinnäytetyö etusijalle, jotta työn sai tehtyä valmiiksi aikamääreeseen mennessä.

Opinnäytetyöprojekti aloitettiin helmikuussa 2025 ja sain työn valmiiksi toukokuussa 2025. Tämä aikataulu oli kuitenkin tiukka, mutta osoittaa myös hyvää projektinhallintaa sekä opinnäytetyön priorisointia etusijalle, kun työ saatiin valmiiksi aikamääreeseen mennessä.

Opinnäytetyötä oli kuitenkin myös mieluisa tehdä, sillä aihe on ajankohtainen ja itselleni mieluinen. Se opetti minulle luottamusta omaan tekemiseen sekä kehitti analyyttistä ajattelua ja kirjoittamista. Opinnäytetyön teko opetti minulle myös tulevaisuuden kannalta projektinhallintaa ja ajankäyttöä. Prosessin aikana koin myös haasteita motivaation kanssa sekä kävin läpi erilaisia tunteita, kun

tuntui ettei prosessi etene haluamallani tavalla, mutta kun sai itsensä kerättyä ja uudelleen motivoiduttua työn ääreen koki myös onnistumisen tunteita.

6.4 Jatkotutkimusidea

Opinnäytetyöprosessin aikana kehittyi myös uusia jatkotutkimusideoita. Jatkotutkimuksissa voisi perehtyä syvällisemmin ja laajemmalla skaalalla julkisen sektorin tietomurtotapauksiin. Case-tapauksien määrää voitaisiin lisätä, jolloin saataisiin kattavampia ja luotettavampia tuloksia julkisen sektorin tietomurtoihin liittyen. Tutkimuksessa voitaisiin myös vertailla eri toimialojen kuten sosiaali- ja terveydenhuollon, kasvatuksen- ja koulutuksen sekä kunnanhallinnon toimialojen välisiä tietomurtotapauksia. Tällainen tutkimus voisi paljastaa toimialakohtaisia eroja haavoittuvuuksista sekä tietoturvakäytännöistä.

Lisäksi jatkotutkimuksissa voitaisiin tutkia julkisen sektorin organisaatioiden valmiuksia palautua tietomurroista. Tällaisessa tutkimuksessa voitaisiin analysoida viestinnän sekä jälkitoimien merkitystä. Tutkimuksessa voitaisiin myös pohtia sidosryhmien luottamusta organisaatiota kohtaan tietomurtotapausten jälkeen.

Laajemmalla skaalalla ilmiötä voitaisiin tutkia myös vertailevasti kansainvälisessä kontekstissa. Silloin voitaisiin tarkastella, miten tietomurtoihin varaudutaan ja reagoidaan muissa maissa kuin Suomessa. Tällainen tutkimus antaisin myös kansainvälistä kuvaa tietomurtotapauksista ja niihin reagoinnista.

Lähteet

Abu, M.S., Ariffin, A., Selamat, S.R. & Yusof, R. 2018. Cyber Threat Intelligence – Issue and Challenges. Indonesian Journal of Electrical Engineering and Computer Science. Luettavissa: https://www.researchgate.net/profile/Md-Sahrom/publication/322939485_Cyber_Threat_Intelligence_-_Issue_and_Challenges/links/5d2d492192851cf440871da8/Cyber-Threat-Intelligence-Issue-and-Challenges.pdf. Luettu: 3.3.2025.

Bhavsar, V., Kadlak, A. & Sharma, S. 2018. Study on Phising Attacks. International Journal of Computer Applications. Luettavissa: https://www.ijcaonline.org/archives/volume182/number33/bhavsar-2018-ijca-918286.pdf. Luettu: 1.4.2025.

Chandy, J. 2022. Review on Malware, Types and its Analysis. International Journal for Research in Applied Science and Engineering Technology. Luettavissa: https://www.ijraset.com/best-journal/review-on-malware-types-and-its-analysis. Luettu: 25.3.2025.

Cheng, L., Liu, F. & Yao, D. 2017. Enterprise data breach: causes, challenges, prevention, and future directions. WIley Interdisciplinary Reviews Data Mining and Knowledge Discovery. Luettavissa: https://wires.onlinelibrary.wiley.com/doi/pdfdirect/10.1002/widm.1211. Luettu: 19.3.2025.

Cymru, T. 2006. Cybercrime: An Epidemic. Acm Queue. Luettavissa: https://dl.acm.org/doi/pdf/10.1145/1180176.1180190. Luettu: 2.5.2025.

Digi- ja väestötietovirasto 2022. Mitä on digiturva? Luettavissa: https://dvv.fi/mita-on-digiturva. Luettu: 24.2.2025.

F-Secure 2024. Helsingin kaupungin tietomurto: Mitä sinun tulee tietää. Luettavissa: https://www.f-secure.com/fi/articles/helsingin-kaupungin-tietomurto-mita-sinun-tulee-tietaa. Luettu: 6.4.2025.

Finto Suomalainen asiasanasto- ja ontologiapalvelu s.a. Tietojärjestelmä. Luettavissa: https://finto.fi/tt/fi/page/t79. Luettu: 24.2.2025.

Gwebu, K.L., Wang, J. & Wang, L. 2018. The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. Luettavissa: https://www.tandfonline.com/doi/full/10.1080/07421222.2018.1451962. Luettu: 13.4.2025.

Heikinmatti, A. 2022. Hakkeri ujutti Oulun kaupungin verkkosivuille koodin, joka valjasti sivuilla vierailleiden tietokoneet louhimaan kryptovaluuttaa. Yle. Luettavissa: https://yle.fi/a/3-12424013. Luettu: 8.4.2025.

Helsingin kaupunki 2025a. Kasvatuksen ja koulutuksen tietomurto. Luettavissa: https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto. Luettu: 6.4.2025.

Helsingin kaupunki 2025b. Esitys kaupunginhallitukselle, toimialan eräiden ICT-toimintojen luovuttaminen, kasvatus- ja koulutuslautakunta. Luettavissa: https://paatokset.hel.fi/fi/asia/hel-2025-005090/a21175cb-a99f-c835-bf7e-96150fd00002. Luettu: 12.4.2025.

Hiltunen, T. 2021. Turun opetuksen verkkopalveluihin kohdistettu tietomurto pystyttiin estämään – varotoimenpiteenä tulee vaihtaa salasana. Yle. Luettavissa: https://yle.fi/a/3-11883275. Luettu: 8.4.2025.

Ibrahim, A.S., Thiruvady, D., Schneider, J.-G. & Abdelrazek, M. 2020. The Challenges of Leveraging Threat Intelligence to Stop Data Breaches. Frontiers in Computer Science. Luettavissa: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.00036/full. Luettu: 1.4.2025.

Joseph, R.C. 2017. Data Breaches: Public Sector Perspectives. IT Professional. Luettavissa: https://ieeexplore.ieee.org/abstract/document/7950860. Luettu: 13.3.2025

Kadari, S.R., Radhika, G., Shekar, R. & Madhu, Ch. 2024. A Study on the Key Applications of Malware. International Journal of Advanced Research in Science Communication and Technology. Luettavissa: https://ijarsct.co.in/Paper19359.pdf. Luettu: 25.3.2025.

Kekkonen, J. 2008. Vertailevan tutkimuksen haasteita. Tieteessä tapahtuu. Luettavissa: https://journal.fi/tt/article/view/482. Luettu: 13.3.2025.

Kelley, C.M., Hong, K.M., Mayhorn, C.B. & Murhy-Hill, E. 2012. Something Smells Phishy: Exploring Definitions, Consequences and Reactions to Phishing. Proceeding of the Human Factors and Ergonomics Society Annual Meeting. Luettavissa: https://journals.sagepub.com/doi/10.1177/1071181312561447. Luettu: 12.4.2025.

Kovács, A. 2022. Ransomware: a cmprehensive study of the exponentially increasing cybersecurity threat. Insights into regional Development. Luettavissa: https://jssidoi.org/ird/article/102. Luettu: 11.4.2025.

KumarGoutam, R. 2015. Importance of Cyber Security. Luettavissa: https://research.ijcaonline.org/volume111/number7/pxc3901250.pdf. Luettu: 25.2.2025.

Kyberturvallisuuskeskus 2024. Tietomurrot. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/tietomurrot. Luettu: 24.2.2025.

Lassheikki, P. 2021. Haittaohjelman sulkemat Vanamo-kirjastot auki torstaina – omatoimikirjasto ei vielä toiminnassa. Yle. Luettavissa: https://yle.fi/a/3-12004004. Luettu: 10.4.2025.

Luhtala, J. 2021. Turussa tietomurto opetuksen verkkopalveluihin – tunnustietoja saattanut vuotaa. Mtv Uutiset. Luettavissa: https://www.mtvuutiset.fi/artikkeli/turussa-tietomurto-opetuksen-verkko-palveluihin-tunnustietoja-saattanut-vuotaa/8116470. Luettu: 8.4.2025.

Microsoft s.a. Mitä tietosuoja on? Luettavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-data-protection. Luettu: 2.5.2025.

Niskanen, A-M. 2021. Vanamonkirjastojen palvelut ovat tietomurron takia poissa käytöstä Hämeenlinnan seudulla. Yle. Luettavissa: https://yle.fi/a/3-11997663. Luettu: 10.4.2025.

Pachhala, N., Jothilakshmi, S. & Battula, B.P. 2021. A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques. 2nd International Conference on Smart Electronics and Communication. Luettavissa: https://ieeexplore.ieee.org/document/9591763. Luettu:19.3.2025.

Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus. Luettu: 15.4.2025.

Rita, M. 2025. KRP epäilee rikosta Helsingin kaupungin toiminnassa – poliisin arvio tietomurron uhrimäärästä ”laajassa haarukassa”. Yle. Luettavissa: https://yle.fi/a/74-20149294. Luettu: 6.4.2025.

Streicher, C. 2022. The Anatomy of a Data Breach. Blogi. Luettavissa: https://elasticito.com/the-anatomy-of-a-data-breach/. Luettu: 1.4.2025.

Tahir, R. 2018. A Study on Malware and Malware Detection Techniques. International Journal of Education and Management Engineering. Luettu: 13.3.2025.

Tanana, D. 2020. Behavior-Based Detection of Cryptojacking malware. Ural Symposium Biomedical Engineering, Radioelectronics and Information Technology. Luettavissa: https://ieeexplore.ieee.org/document/9117732. Luettu: 12.4.2025.

Taskinen, H. 2025. Kelalta varoitus kalasteluviesteistä – ”Aina syytä olla varuillaan”. Mtv Uutiset. Luettavissa: https://www.mtvuutiset.fi/artikkeli/kelalta-varoitus-kalasteluviesteista-aina-syyta-olla-varuillaan/9120218. Luettu: 8.4.2025.

Temara, S. 2024. The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. Asian Journal of Advanced Research and Reports. Luettavissa: https://journalajarr.com/index.php/AJARR/article/view/610. Luettu: 18.3.2025

Tilastokeskus 2020. Julkinen sektori. Luettavissa: https://stat.fi/meta/kas/julkinen_sektor.html. Luettu: 24.2.2025.

Traficom, 2025. Vuosi 2024 muistetaan isoista kybertapauksista. Luettavissa: https://traficom.fi/fi/ajankohtaista/vuosi-2024-muistetaan-isoista-kybertapauksista?utm_source=chatgpt.com. Luettu: 3.4.2025.

Trisolvena, M.N. & Saputra, N.H. 2024. Phishing Cyber Security Threats. Jurnal Improsci. Luettavissa: https://annpublisher.org/ojs/index.php/improsci/article/view/440. Luettu: 18.3.2025.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Tammi. Uudistettu laitos. E-kirja. Luettu: 3.3.2025.

Turun kaupunki 2024. Haavoittuvuuksien havainnointiin liittyvän lisäpalvelun hankinta NetNordic Finland Oy:ltä. Kaupunginhallituksen päätöspöytäkirja. Luettavissa: https://ah.turku.fi/kh/2024/0422010p/5041465.htm. Luettu: 11.4.2025.

Poliisi, 2025. Tietomurrot. Luettavissa: https://poliisi.fi/tietomurrot. Luettu: 25.2.2025.

Rikoslaki 38 luku 8 §, Finlex. Luettavissa: https://www.finlex.fi/fi/lainsaadanto/1889/39-001#chp_38v19950578__sec_7bv20150368__heading. Luettu: 25.2.2025.

Saleem, H. & Naveed, M. 2020. SoK: Anatomy of Data Breaches. Proceedings on Privacy Enhancing Technologies. Luettavissa: https://petsymposium.org/popets/2020/popets-2020-0067.php. Luettu: 1.4.2025.

Seemma, P.S., Nandhini, S. & Sowmiya, M. 2018. Overview of Cyber Security. International Journal of Advance Research in Computer and Communication Engineering. Luettavissa: https://www.researchgate.net/profile/Nandhini-Sundaresan/publication/329678338_Overview_of_Cyber_Security/links/5c1640b3299bf139c75c29e7/Overview-of-Cyber-Security.pdf. Luettu: 3.3.2025.

Valecha, R., Mandaokar, P. & Rao, H.R. 2021. Phising Email Detection using Persuasion Cues. IEEE Transactions on Dependable and Secure Computing. Luettavissa: https://ieeexplore.ieee.org/document/9565347. Luettu: 11.4.2025.

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Helsinki: Art House. E-kirja. Luettu: 28.2.2025.

Wu, M-H., Lai, Y-J., Hwang, Y., Chang, T-C. & Hsu, F. 2022. Mineguard: A Soulution to Detect Browser-Based Cryptocurrency Mining trhough Machine Learning. Applied Sciences. Luettavissa: https://www.mdpi.com/2076-3417/12/19/9838. Luettu: 11.4.2025.