TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MIKA KARSIKAS

TARKOITUKSENMUKAISET TIETOTURVARATKAISUT PIENYRITYKSILLE TIETOMURTOJEN HAVAITSEMISEEN JA TUTKINTAAN

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
1. helmikuuta 2017

TIIVISTELMÄ

MIKA KARSIKAS: Tarkoituksenmukaiset tietoturvaratkaisut pienyrityksille tietomurtojen havaitsemiseen ja tutkintaan
Tampereen teknillinen yliopisto
Diplomityö, 53 sivua
Kesäkuu 2017
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietoturvallisuus
Tarkastaja: professori Jarmo Harju

Avainsanat: pienyritys, tietomurto, rikos, tutkinta, havaitseminen

Tietoturvan merkitys on lisääntymässä myös yritystoiminnassa. Tässä työssä keskitytään tietomurtojen havaitsemiseen ja tutkintaan soveltuviin ratkaisuihin pienten yritysten näkökulmasta. Koska pienillä yrityksillä on usein käytettävissä rajalliset resurssit tietoturvan toteuttamiseen, on tärkeää kohdistaa nämä tarkoituksenmukaisella tavalla vastaamaan todennäköisempien tietomurtojen tekotapojen muodostamia uhkia. Työn tavoitteena on hakea tietoa ensisijaisesti poliisin rikosilmoitustiedoista ja muista julkisesti saatavilla olevista raporteista tietomurtojen yleisimmistä tekotavoista. Haettujen tietojen perusteella tavoitteena on muodostaa periaatteet tietomurtojen havaitsemiseen ja selvittämisen edesauttamiseen kykenevien ratkaisujen toteuttamiseksi.

Työ jakaantuu kolmeen eri osaan. Ensimmäisessä osiossa esitellään tietomurron käsite ja siihen liittyvä lainsäädäntö sekä poliisin rikosilmoitustietojen perusteella muodostettu taulukko yleisimmistä tekotavoista. Yleisimmiksi tekotavoiksi osoittautuvat käyttäjätunnusten luvaton hyödyntäminen, fyysinen pääsy kohdelaitteelle ja kalastelu. Muiltakin osin rikosilmoitustietojen perusteella korostuu inhimillisen tekijän merkitys tietomurtojen mahdollistajana. Kirjatuista rikosilmoituksista yli 70 % olisi nimittäin saatu ehkäistyä huolellisilla ja tietoturvallisilla toimintatavoilla. Toinen osio sen sijaan käsittelee erilaisia ratkaisuvaihtoja tietomurtojen havaitsemiseen ja selvittämisen edesauttamiseen. Osiossa tuodaan esille erilaisia pienyrityksillekin käytettävissä olevia kaupallisia ja avoimen lähdekoodin ratkaisuvaihtoehtoja.

Viimeisessä osiossa esitellään työn tuloksena muodostettu yleisimmistä tekotavoista ratkaisujen suuntaamista varten luotu portaikko. Yrityksen on tarkoitus hyödyntää portaikkoa ratkaisujen toteuttamisessa aloittaen toteutus alimmalta portaalta eli yleisimmästä tekotavasta ja toteuttaa aluksi sen havaitsemiseen kykenevä ratkaisu. Tämän jälkeen tarkoituksena on siirtyä seuraavalla portaalle ja siitä sitten taas eteenpäin. Näin edeten yritys tulee askeleittain toteuttaneeksi sellaisia havaitsemisratkaisuja, jotka keskittyvät niihin uhkiin, jotka todennäköisesti heitä kohtaisivat. Tietomurtojen tutkintaan liittyen tarkoituksenmukaisimpana ratkaisuna pienelle yritykselle tuodaan esille turvautuminen ulkopuoliseen apuun. Tätä varten kuitenkin yritykselle olisi tärkeää, että tietomurron havaitsemisen jälkeen kaikki siihen liittyvät jäljet ja todistusaineisto kyetään dokumentoimaan ja säilyttämään muuttumattomana jälkiselvitystä varten.

ABSTRACT

MIKA KARSIKAS: Appropriate information security solutions for small-scale companies to detect and investigate security breaches
Tampere University of Technology
Master of Science Thesis, 53 pages
June 2017
Master's Degree Program in Information Technology
Major: Information security
Examiner: Professor Jarmo Harju

Keywords: small-scale business, security breach, investigation, detection, crime

The importance of information security is increasing also in the business world. In this thesis, the focus is on detection and investigation of security breaches from the perspective of a small-scale business. Small-scale businesses often have limited resources available for information security, which is why it is vital to use them appropriately to counter at least the most common forms of security breaches. The main goal of this work is to acquire information from the police's criminal reports database about the different forms of security breaches and use that information to form principles for implementing appropriate solutions for detection and investigation of security breaches.

The thesis is divided into three parts. The first part includes the definition of a security breach and the presentation of the legislation behind it. In addition, the most common forms of security breaches based on the information from the criminal reports are presented. It will be shown that the most frequent methods used in security breaches are unlawful use of user credentials, unlawful physical access to the target device and phishing. The significance of the human factor is emphasized in the successful security breaches. Over 70 % of the criminal cases could have been prevented by proper and careful procedures. In the second part, several solutions for detecting and investigating security breaches are presented. Both commercial and open source solutions suitable for small businesses are included.

The last part of the thesis includes a staircase for implementing security solutions. The staircase is formed based on the information gathered on the most popular forms of security breaches and it is meant to be used so that a company should begin from the first step, in other words from the most probable case of a security breach, and implement a solution for its detection. Next, the purpose is to move one step up and implement a solution for the detection of the form of security breach included in that step. This way the goal is to climb the staircase systematically and end up implementing security solutions to detect the most common forms of security breaches. On the other hand, the most appropriate solution for small-scale companies to investigate security breaches is determined to be the use of outside help. However, it is essential for the company to be able to document and preserve intact all the traces and information about the security breach in order for the investigation to be successful.

ALKUSANAT

Tämä diplomityö on tehty osana tietotekniikan diplomi-insinöörin tutkintoon tähtääviä opintoja Tampereen teknillisessä yliopistossa. Työn tekijänä haluan kiittää aluksi yhtäläisesti kaikki työn tekemisessä avustaneita ja tukeaan antaneita. Kiitos kuuluu myös Poliisihallitukselle tutkimusluvan myöntämisestä, mitä ilman työn toteuttaminen nykyisessä muodossa ei olisi ollut mahdollista.

Aiheen valintaan ja alussa tehtyyn työn suuntaamiseen liittyvästä opastuksesta haluan kiittää Timo Piiroista keskusrikospoliisista sekä Suvi Kaartista ja muita prosessiin osallistuneita Intopalo Oy:n työntekijöitä. Työn tekniseen puoleen liittyvästä opastuksesta kiitän lisäksi Juha Leivoa Nixu Oyj:stä. Lisäksi tuesta ja opastuksessa koko työn prosessin keston ajan haluan kiittää erityisesti kihlattuani Katja Mäenpäätä, Poliisiammattikorkeakoulun erityisasiantuntijaa Tero Toiviaista sekä työni ohjaajaa professori Jarmo Harjua.

Tampereella, 12.5.2017

Mika Karsikas

SISÄLLYSLUETTELO

KUVALUETTELO

LYHENTEET JA MERKINNÄT

CERT	engl. Computer Emergency Response Team, asiantuntijoista koostuva ryhmä tietoturvaloukkausten ennaltaehkäisyyn, havainnointiin ja ratkaisemiseen
ENISA	Euroopan unionin verkko- ja tietoturvavirasto
IDS-järjestelmä	engl. Intrusion Detection System, tunkeutumisen havaitsemisjärjestelmä
IP-osoite	internetin protokollan käyttämä osoite, joka yksilöi internetiin kytketyn laitteen ja mahdollistaa sen kanssa kommunikoinnin
IPS-järjestelmä	engl. Intrusion Prevention System, tunkeutumisen estojärjestelmä
IoT	engl. Internet of Things, esineiden internet eli internetin yli ohjattavat, mitattavat ja muuten hallittavat ympäristöään aistivat laitteet
NAT-osoite	engl. network address translation, osoitteenmuunnoksen kautta muodostettu IP-osoite julkisesti liikennöitävien IP-osoitteiden piilottamiseksi tai säästämiseksi
SIEM-järjestelmä	security information and event management -järjestelmä
TTY	Tampereen teknillinen yliopisto
TCP	engl. Transmission Control Protocol, internet-yhteyksien luomisessa käytetty tietoliikenneprotokolla
TCP SYN -paketti	TCP-protokollalla tehtävän yhteyden avaamisessa lähetettävä ensimmäinen paketti
URL	engl. Uniform Resource Locator, verkkosivun osoite
VAHTI	valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä

.

1. JOHDANTO

Tietoturvallisuus on nykypäivänä muodostunut hyvin keskeiseksi tekijäksi yhteiskunnassa ja erityisesti yritystoiminnassa. Lähes päivittäin saamme lukea uutisista uusista palvelunestohyökkäyksistä ja erilaisista hakkerointitapauksista. Kohonneen uhkatason myötä myös yritystoiminnassa on lisätty resursseja erilaisiin tietoturvaratkaisuihin. Suurimmaksi osaksi nämä ratkaisut vaikuttavat painottuvan tietoturvan parantamiseen ennalta estävästi. Sen sijaan jo tapahtuneiden hyökkäysten havaitsemiseen ja tutkintaan panostetaan vielä selvästi vähemmän.

Vaikka poliisille ilmoitettujen tietomurtojen määrä on lisääntynyt, voidaan silti olettaa, että merkittävä osa tapahtuvista tietomurroista jää joko kokonaan havaitsematta tai niistä ei haluta ilmoittaa esimerkiksi maineen menetyksen pelossa. Asiassa olisi siten kehitettävää. Tässä työssä tarkoituksena on pyrkiä selvittämään keinoja, joiden avulla erityisesti pienet yritykset pystyisivät parantamaan kykyään ensinnäkin havaita heihin kohdistuvia tietomurtoja sekä mahdollisesti sellaisen uhriksi joutuessaan edesauttamaan rikoksen selvittämisessä.

Työssä tarkastelu on rajattu pieniin yrityksiin, joilla ei ole omaa päätoimista tietoturvahenkilöstöä. Heillä tietoturvan toteutuminen on joko puhtaasti ostettujen tai oman henkilöstön sivutyönä toteuttamien ratkaisujen varassa. Ostettavien ratkaisujen kohdalla niiden hankkimisen kynnykseksi muodostuu usein niiden hinta. Lisäksi usein joutuu ostamaan erikseen tietoturvatason kartoituksen ja korjaamisen. Vastaavasti itse toteutettujen ratkaisujen osalta haasteeksi saattavat muodostua henkilöstön osaaminen ja motivaatio, koska kyseessä ei ole heidän niin sanottu päätyönsä. Työssä on tarkoituksena pyrkiä löytämään menetelmiä, jotka olisivat tarkoituksenmukaisia pienikokoisille yrityksille eli joissa muun muassa kustannukset ja tehokkuus olisivat sellaisella tasolla, että niiden hankkimisen tai toteuttamisen kynnys olisi mahdollisimman matala.

Tietoturvatuotteita ja niiden tarjoajia alkaa markkinoilla olla lukuisia erilaisia. Lisäksi muun muassa teleoperaattorit tarjoavat yrityksille tietoturvaratkaisuja eri muodoissa. Teleoperaattorien tietoturvaratkaisut ovat yrityksille helppo valinta, koska pääosa yrityksistä on jo tietoliikenneyhteyksien kautta niiden asiakkaita. Toinen vaihtoehto on hankkia ratkaisuja suurilta ja tunnetuilta tietoturvaa tarjoavilta yrityksiltä. Näiden yritysten ja tuotteiden löytäminen on yleensä helppoa. Laajalti tunnettuihin toimijoihin on myös helpompi luottaa. Toki myös pienemmät yritykset tuottavat tietoturvaratkaisuja, mutta niiden löytäminen ja niihin luottaminen ei välttämättä ole niin luontevaa.

Tietoturvatuotteiden ostamisen vaihtoehtona on ratkaisujen toteuttaminen itse, jolloin yksi käytännöllisimmistä ratkaisuista on erilaisten avoimen lähdekoodin ratkaisujen hyödyntäminen. Tällöin tosin tarvitaan ainakin jonkin verran tietoteknistä osaamista ja ymmärrystä tuotteiden asentamisessa ja käyttöön ottamisessa. Lisäksi ymmärrystä olisi hyvä olla myös siitä, mitä käyttöön otettava tuotteet oikeasti tekevät ja mitä niillä kyetään saavuttamaan.

Oli kyseessä sitten ostettu tai ilmaiseksi hankittu tai toteutettu tietoturvaohjelmisto on sen käyttötarkoitus hyvä tiedostaa. Tietoturvaohjelmistoja on olemassa muun muassa virustorjuntaan, haittaohjelmien havaitsemiseen, verkkoliikenteen seurantaan, tunkeutumisen havaitsemiseen, jne. Osa ohjelmistoista on erikoistunut johonkin yhteen toimintoon, kun taas osalla pystytään suorittamaan useita eri toimintoja. Tässä työssä tarkoituksena on kartoittaa ratkaisuja ja ohjelmistoja, joilla pyritään havaitsemaan tietomurtoja ja tallentamaan mahdollisimman kattavasti niistä jääneet jäljet mahdollisesti seuraavia tutkintatoimia ajatellen.

Tutkimuskysymyksinä työhön lähdettäessä ovat:

1. Minkälaisilla ratkaisuilla olisi mahdollista saada pienten yritysten tietoturvallisuutta parannettua tietomurtojen havaitsemiseksi ja niiden selvittämiseksi?
2. Missä määrin edellä mainitut ratkaisut olisivat pienyrityksille toteutettavissa ilman merkittävää haittaa liiketoiminnalle?

Ennen varsinaisten tietoturvaratkaisujen kartoittamista on olennaista määritellä, mitä tietomurrolla käytännössä tarkoitetaan. Tällöin saadaan käsitys siitä, mitä hankittavilla tai itse toteutettavilla ratkaisuilla tulisi pyrkiä havaitsemaan. Kuten myöhemmin alaluvuissa 2.2 ja 2.3 nähdään, tietomurto voi lain mukaan periaatteessa toteutua lukuisilla eri tavoilla. Tätä mahdollisten tapojen joukkoa on tarkoitus pyrkiä supistamaan hankkimalla ajankohtaista tietoa poliisin rikosilmoitustiedoista tietomurtojen yleisimmistä tekotavoista. Rikosilmoitustietojen lisäksi tilastotietoa yleisimmistä tekotavoista haetaan myös muista lähteistä, kuten kansainvälisten tietoturvayritysten vuosiraporteista.

Koska yritykselle voi resurssien ja osaamisen osalta olla hankalaa toteuttaa kaikkien eri tekotapojen kattavaan havaitsemiseen kykenevä järjestelmä ja ylläpitää sitä, auttaa yleisimpien tekotapojen tiedostaminen keskittämään käytettävissä olevat resurssit ja toimet todennäköisimpien tekojen havaitsemiseen. Vastaavasti yleisimpien tekotapojen tiedostaminen auttaa lisäksi yrityksiä tietoturvaohjelmistojen hankinnassa, kun osataan paremmin arvioida niiden tuottamia etuja tietomurroista aiheutuvien riskien vaikutuksia ja todennäköisyyksiä vastaan.

Tarkoituksenmukaisten ratkaisujen kartoittamiseksi on lähdetty liikkeelle ajatuksesta, että niiden tulisi ensisijaisesti kyetä havaitsemaan yleisimmät ja siten todennäköisimmät tietomurrot. Useat eri organisaatiot laativat vuosittain raportteja heidän mukaansa ylei-

simmistä tietomurtojen tekotavoista. Raportit perustuvat täten organisaatiolle toimitetuista ja sen itsensä hankkimista ja/tai havaitsemista tiedoista, minkä johdosta raporttien pohjana käytetyissä tiedoissa on omat rajansa. Tässä työssä on sen sijaan pyritty hakemaan erilaista näkökulmaa hyödyntämällä ensisijaisena tietolähteenä Suomen poliisin rikosilmoitustietoja tietomurroista. Tavoitteena on siten saada paremmin kuvaa nimenomaan Suomen olosuhteissa yleisimmistä tekotavoista. Näitä tietoja on myös verrattu kansainvälisiin raportteihin, jotka on siten otettu huomioon varsinaisia ratkaisuja pohdittaessa.

Työ on jaettu kolmeen eri kokonaisuuteen. Luvussa kaksi käydään läpi työn lähtökohdat, tietomurtoihin liittyvä lainsäädäntö sekä esitellään tietomurtojen yleisimmät tekotavat poliisin tietojärjestelmistä ja muista lähteistä saatujen tietojen perusteella. Luku kolme sen sijaan keskittyy erilaisten pienyrityksille mahdollisten tietomurtojen havaitsemiseen soveltuvien tietoturvaratkaisujen esittelyyn. Luvussa neljä sitten tarkastellaan esiteltyjä tietoturvaratkaisuja yleisimpien tekotapojen kannalta ja rakennetaan portaittain toteutettava menetelmä tietomurtojen havaitsemiskyvyn parantamiseksi.

2. TIETOMURTORIKOKSET

Erilaisia tietoturvauhkia ja -loukkauksia on monenlaisia, ja tietomurrot muodostavat niistä yhden osan. Ennen kuin voidaan aloittaa varsinaisten ratkaisujen pohtiminen tietomurtojen varalle, on syytä tuoda esille, miksi niitä ylipäänsä tarvitaan. Tarve tietomurtojen havaitsemiselle tulee ensinnäkin lainsäädännön sekä erilaisten asetusten, ohjeiden ja suositusten kautta, mutta myös yrityksen omien liiketoimintaan liittyvien intressien pohjalta.

Toinen ratkaisujen pohtimisen kannalta olennainen seikka on kartoittaa ne toimet ja tekotavat, joiden varalle niitä ollaan toteuttamassa. Kun kyetään mahdollisimman tarkasti määrittelemään, mitä toteutettavilta ratkaisuilta edellytetään, on niiden kartoittaminen suoraviivaisempaa ja vertailu helpompaa. Esimerkiksi tietomurtojen havaitsemisen osalta on keskeistä ymmärtää, minkälaisilla tavoilla tietomurto voidaan toteuttaa, jotta ne kyetään ottamaan huomioon havaitsemisratkaisuja pohdittaessa. Tässä työssä tietomurtojen määrittelyn lähtökohdaksi on otettu Suomen lainsäädäntö ja siihen liittyvät valmisteluasiakirjat.

2.1 Pienyritysten tarve tietomurtojen havaitsemiseen

Kuten edellä on tuotu esille, tarve tietomurtojen torjuntaan, havaitsemiseen ja selvittämisen on korostunut niiden yleistymisen myötä. Tämän lisäksi yritysten tietoturvan tasoon on myös valtionhallinnon ja Euroopan unionin tasolla alettu kiinnittää huomiota. Euroopan unioni on huhtikuussa 2016 säätänyt tietosuoja-asetuksen uudistuksesta, jota aletaan soveltaa 25.5.2018 alkaen [34, s. 6].

Tietosuoja-asetuksen uudistuksessa yrityksille ja organisaatioille asetetaan velvollisuus muun muassa ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista 72 tunnin sisällä loukkauksen tapahtumisesta niille henkilöille, joiden tietoja tietoturvaloukkaus koskee [34, s. 17]. Velvollisuus tulee siis koskemaan kaikkia niitä yrityksiä, jotka pitävät yllä jonkinasteista henkilötietoja sisältävää rekisteriä. Toisin sanoen ilmoitusvelvollisuus tulee kattamaan tapaukset, joissa yritykseen tietojärjestelmiin kohdistunut tietomurto kohdistuu sellaiseen osaan tietojärjestelmää, johon on tallennettu henkilötietoja. Ilmoitusvelvollisuuteen on säädetty poikkeuksena tilanne, jossa henkilötiedot on salattu eivätkä salausavaimet ole vaarantuneet.

Valtionvarainministeriön VAHTI-työryhmä on ohjeistanut, että tietosuoja-asetuksen seurauksena yritysten tulee pyrkiä suojaamaan tietojärjestelmänsä. Järjestelmien tekninen toteutus tulisi olla sellainen, että se vastaa tietojen käsittelyyn liittyviä riskejä. Mahdollisia käytettäviä teknisiä keinoja tiedon suojaamiseen ovat muun muassa tiedon salaaminen,

pääsynhallinnan toteuttaminen ja tietojen anonymisointi. Lisäksi VAHTI-ohjeessa tuodaan esille, että yritysten tulee kyetä lokitiedostoista todentamaan, mitä henkilötietoja järjestelmästä on katsottu, muutettu, lisätty tai poistettu ja milloin toimenpide on suoritettu. Lokien seuranta tulisi suorittaa automatisoidusti lokitietojen suuren määrän johdosta. [34, s. 25–26]

EU:n tietosuoja-asetuksen määrittelemän ilmoitusvelvollisuuden johdosta henkilötietoja sisältäviä rekisterejä ylläpitävillä yrityksillä ja organisaatioilla tulee olla kyky havaita tietoturvapoikkeamat ympäristössään. Havaitsemista varten olisi hyvä olla käytössä tietoturvatapahtumien havainnointiin tarkoitettu ohjelmisto eli SIEM-järjestelmä. Lisäksi velvollisuutena on omata kyky selvittää havaitun poikkeaman syyt ja seuraukset sekä vaikutukset yksityisyyden suojaan sekä eristää poikkeaman leviäminen. Selvittämistä ajatellen tulee kaikki tutkintaan liittyvät toimet dokumentoida ja huolehtia tutkinnan kannalta tarvittavan todistusaineiston säilyttämisestä ja eheydestä. [34, s. 26–27] Todistusaineiston säilyttämisen osalta on muun muassa tapahtumaa seuraavan rikosprosessin kannalta elintärkeää, että aineisto säilyy muuttumatta. Kaikenlainen aineiston käsittely heikentää sen todistusarvoa.

Käytännössä valtaosa yrityksistä ylläpitää jonkinlaista asiakasrekisteriä, johon on tallennettu henkilötietoja jossain muodossa. Toki myös muunlaisia henkilörekisterejä saattaa yrityksillä olla. Tämän vuoksi edellä mainittu EU:n tietosuoja-asetus tulee koskemaan valtaosaa suomalaisistakin yrityksistä ja velvoittamaan heitä suojaamaan henkilötietoja ja toteuttamaan niihin kohdistuvien loukkauksien havaitsemiseen kykenevät ja selvittämistä edesauttavat järjestelmät.

Pohdittaessa tietoturvaloukkausten havaitsemiseen kykenevien järjestelmien toteuttamista on hyvä kiinnittää huomiota järjestelmän laatuun. Laadussa tulee huomioitavaksi järjestelmän ominaisuuksien lisäksi yrityksen koko, tarpeet ja muu toiminta, sillä niiden toteutus on tarkoitus suhteuttaa yrityksen toimintaan ja suojattaviin tietoihin. VAHTI-ohjeessa puhutaan asianmukaisista teknisistä ja organisatorisista ratkaisuista. [34, s. 24] Kun pohditaan havaitsemis- ja selvittämiskykyä tietomurtoja vastaan pienten yritysten näkökulmasta, voitaisiin ajatella ainakin alkuun, että yleisimmät tietomurtojen tekotavat tulisi kyetä ottamaan huomioon.

Tietoa yleisimmistä tietomurtojen tekotavoista kerätään tämän työn yhteydessä poliisin tietojärjestelmistä. Näistä on edelleen tavoitteena rajata ne, jotka muun muassa kustannuksien ja käytettävyyden perusteella soveltuvat parhaiten pienyritysten käyttöön. Vaikka Euroopan unionin tietosuoja-asetuksen soveltaminen odottaa vielä tämän työn kirjoitushetkellä tarkempia kansallisia kannanottoja ja linjauksia, voidaan tietosuoja-asetuksen sisällön perusteella jo ennakoida ja suunnitella ratkaisuja, joilla pienyritykset kykenisivät tehokkaimmin täyttämään asetuksen heille asettamat velvollisuudet.

Ratkaisujen pohdinnassa on tehty yhteistyötä noin 10 työntekijästä muodostuvan pienyritykseksi laskettavan elektroniikka-alan yrityksen kanssa, johon jatkossa viitataan Y-malli Oy:nä. Kyseisen yrityksen tietoturva oli tätä työtä aloitettaessa hyvin pitkälle teleoperaattoreilta hankittujen tietoturvaratkaisujen varassa. Nyt muun muassa Euroopan unionin tietosuoja-asetuksen voimaantulon myötä yrityksessä on herätty pohtimaan, miten tietoturvaan olisi syytä panostaa. Haasteen muodostavat yrityksen pieni koko, tietoturvaan liittyvän erikoisosaamisen puute, käytettävissä olevat resurssit sekä haasteellinen taloudellinen tilanne. Tavoitteena on tämän työn puitteissa pyrkiä parantamaan yrityksen tietoturvaa tietomurtojen havaitsemisen ja selvittämisvalmiuksien osalta.

2.2 Rikoslain 38 luku

Tietomurto rikoksena on määritelty rikoslain 38 luvun 8 §:ssä [29]. Pykälän mukaan tietomurrolla tarkoitetaan ensinnäkin oikeudetonta tunkeutumista tietojärjestelmään tai sellaisen erikseen suojattuun osaan joko tekijälle kuulumatonta käyttäjätunnusta käyttämällä tai muuten turvajärjestely murtamalla. Tietomurroksi lasketaan edellä mainitun lisäksi myös teknisen erikoislaitteen tai muuten teknisin keinoin turvajärjestelyn ohittaen, haavoittuvuutta hyväksikäyttäen tai muuten vilpillisin keinoin oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta tai datasta.

Tietojärjestelmällä tarkoitetaan tässä yhteydessä järjestelmää, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa. Rikoslain 38 luvun 13 § [29] täydentää tietojärjestelmän määritelmää vielä sisällyttämällä siihen myös laitteet tai toisiinsa kytkettyjen tai liitettyjen laitteiden kokonaisuudet, joissa yksi tai useampi on ohjelmoitu automaattista käsittelyä varten. Sama koskee myös dataa, jota varastoidaan, käsitellään, haetaan tai välitetään edellä mainituissa laitteissa tai niiden yhdistelmissä niiden toimintaa, käyttöä, suojausta tai huoltoa varten. Datalla tarkoitetaan edelleen tietojärjestelmässä käsiteltäväksi soveltuvaa tosiseikkojen, tietojen ja käsitteiden esitystä sekä ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

Tietomurron osalta on myös huomioitava sen toissijainen luonne ankarammin rangaistaviin rikosnimikkeisiin nähden. Käytännössä tämä tarkoittaa sitä, että tietomurroksi laskettava teko saattaa toisinaan tulla rangaistavaksi jonain muuna rikoksena, mikäli tästä toisesta rikoksesta seuraisi ankarampi rangaistus. [29] Esimerkkinä voisi ajatella tekoa, jossa tekijä murtautuu henkilöauton tietojärjestelmään aiheuttaen auton suistumisen tieltä ja kuljettajan menehtymisen. Tällöin asiaa käsiteltäisiin henkirikoksena, vaikka teko sinänsä täyttäisi myös tietomurron tunnusmerkistön.

Tietomurrolle on rikoslain 38 luvun 9 §:ssä [29] säädetty myös törkeä tekomuoto. Tietomurron voidaan katsoa olevan törkeä, mikäli se on tehty osana järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallisesti ja sitä voidaan pitää myös kokonaisuutena arvostellen törkeänä. Järjestäytynyt rikollisryhmä on määritelty rikoslain 6 luvun 5

§:n 2 momentissa [29], jonka mukaan sellaiseksi lasketaan vähintään kolmen henkilön muodostama tietyn ajan koossa pysyvä rakenteeltaan jäsentynyt yhteenliittymä, joka toimii yhteistuumin tehdäkseen rikoksia, joista säädetty enimmäisrangaistus on vähintään neljä vuotta vankeutta. Koska törkeän tietomurron rangaistusmaksimi on ainoastaan kolme vuotta vankeutta, tulee järjestäytynyttä rikollisryhmää koskeva kvalifiointiperuste sovellettavaksi ainoastaan tilanteissa, joissa ryhmä toimii tehdäkseen tietomurtojen lisäksi myös muita ankarammin rangaistavia rikoksia.

2.3 Tietomurto rikoksena

Jotta tietomurtorikoksia on mahdollista ylipäänsä havaita, pitää kyetä ainakin jossain määrin ymmärtämään, minkälainen toiminta täyttää tietomurron tunnusmerkistön. Edellä esitetty rikoslain 38 luvun 8 § [29] antaa pohjan tälle, mutta säädösteksti jättää usein merkittävästi varaa erilaisille lain tulkinnoille, joten tarkempia linjauksia on syytä hakea muun muassa lain valmisteluasiakirjoista ja oikeuskäytännöstä. Hallituksen esityksessä 94/1993 [9, s. 155] ilmaistaan, että tietomurtoa koskevilla säännöksillä pyritään turvaamaan tietojärjestelmien koskemattomuutta ulkopuolista tunkeutumista vastaan ja tietokonetyöskentelyn yksityisyyttä ulkopuolista tarkkailua vastaan.

Teon motiivin osalta tietomurron rangaistavuus ei edellytä tiedonhankkimis- tai vahingontekotarkoitusta, vaan pelkkä tunkeutuminen riittää [9, s. 145]. Yritysten ja muiden organisaatioiden kannalta tämä tarkoittaa sitä, että rikoksen toteutumista pohdittaessa riittää tunkeutumisen havaitseminen. Sillä onko kyseessä syynä uteliaisuus, kokeilu, vahingoittaminen tai tiedon hankkiminen, ei ole merkitystä rangaistavuuden kannalta. Eri asia on, voiko tietomurtoon syyllistyä vahingossa, mutta sen pohtiminen ei ole yksittäisen yrityksen kannalta tarkoituksenmukaista, vaan se on hyvä jättää esitutkintaviranomaisen selvitettäväksi.

Teon kohteena voivat olla yrityksen tietojärjestelmät, joilla tarkoitetaan tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa eli käytännössä yrityksen omia sisäverkkoja kaikkine niihin kuuluvine laitteineen. Tietojärjestelmiin lasketaan tässä yhteydessä myös erikseen suojatut toiminnalliset kokonaisuudet, millä tarkoitetaan esimerkiksi sisäverkossa olevia laitteita, jotka on erikseen suojattu pääsyä vastaan. Lisäksi on huomioitava, ettei tietomurto tule kyseeseen käsin pidettyjen tietojärjestelmien kohdalla, vaan vaatimuksena on tiedon käsittely, varastointi tai siirto sähköisesti tai muulla vastaavalla teknisellä keinolla. [9, s. 155] Käytännössä tämä tarkoittaa sitä, että pelkkä luvallinen pääsy yrityksen verkkoon esimerkiksi vieraille tarjottavan langattoman verkon kautta ei oikeuta pääsyä verkossa oleville suojatuille palvelimille. Huomionarvoista on, että mikäli verkon laitteita tai sen osia ole eroteltu esimerkiksi juuri suojauksien avulla, ei langatonta verkkoa luvallisesti käyttävä syyllistyisi tämän kohdan perusteella tietomurtoon, vaikka hän verkon kautta tutkisi yrityksen palvelinten sisältöä. Tällainen käyttäytyminen on periaatteessa säädetty rangaistavaksi tietomurtoa koskevan lakipykälän 2 momentin perusteella,

kun rangaistavaksi määritellään oikeudeton selon ottaminen vilpillisin keinoin tietojärjestelmässä olevasta tiedosta tai datasta. Tällöin tekijältä edellytetään ilmeistä vilpillistä tarkoitusta sisällön selvittämiseen. Jos kuitenkaan tietoon tai dataan pääsy ei edellytä erityistä tietoteknistä osaamista tai niitä ei ole suojattu turvajärjestelyllä, ei tietomurto useimmista tapauksissa tulisi tämänkään kohdan perusteella kuitenkaan kysymykseen [10, s. 35].

Joka tapauksessa verkkoa suunniteltaessa ja rakennettaessa on kiinnitettävä huomiota verkon jakamiseen fyysisiin ja loogisiin osioihin, joiden välillä on jonkinlainen kontrollipiste, kuten palomuuri. Lisäksi on huomioitava, että myönnettäessä pääsy johonkin verkon laitteeseen ja osaan, voidaan samalla periaatteessa sallia pääsy kaikkiin niihin laitteisiin, jotka lasketaan kuuluvaksi samaan laitteiden verkostoon ja joita ei ole erikseen suojattu pääsyä vastaan tai suojauksien avulla eroteltu.

Ongelma nousee esille erityisesti yrityksissä ja organisaatiossa, joiden verkko on rakennettu kova kuori pehmeä sisältä -periaatteen pohjalta eli jolloin verkon suojaukset on toteutettu ainoastaan sen ulkoreunoilla ja verkon sisällä on vapaa pääsy ja liikkuvuus kaikkialle. Tällöin voisi käydä siten, että henkilö tai organisaatio, joka luvallisesti tuo laitteensa yrityksen sisäverkkoon voi sen kautta tarkastella vapaasti verkossa olevia laitteita ja niiden tietoja, jolloin tietomurron toteutumisen osoittaminen tulee vaatimaan tekijän vilpillisen tarkoituksen sekä teon oikeudettomuuden osoittamista [10, s. 35].

Tietomurto voi tulla kysymykseen usealla eri tavalla tehtynä. Laissa tarkoitetulla tunkeutumisella tarkoitetaan pääsyn hankkimista järjestelmässä käsiteltyihin, varastoituihin tai siirrettyihin tietoihin, mikä tarkoittaa siis sekä muistissa olevaa tai tiedonsiirtolinjaa pitkin siirrettävää tietoa. Tietomurron rangaistavuus edellyttää jonkinlaisen turvajärjestelyn, kuten tunnistuskontrollin, ohittamista murtamalla. Murtaminen sen sijaan tarkoittaa rikoksen tekijän aktiivisesti tekemää turvajärjestelyn ohittamista eikä se sisältäisi esimerkiksi järjestelmän satunnaisesta epäkuntoisuudesta mahdollistunutta pääsyä. [9, s. 155] Tämä korostaa siten yritysten tarvetta pitää järjestelmiensä suojaukset ajan tasalla ja toiminnassa.

Useissa tapauksissa järjestelmään pääsy edellyttää oikean ja voimassaolevan käyttäjätunnuksen ja/tai salasanan syöttämistä. Tällaisen tunnistuskontrollin ohittamiseen kelpaavien tunnusten keksimisen tai saamisen tavalla ei sen sijaan ole merkitystä. Tietomurron katsotaan täyttyneen riippumatta tavasta, jolla kelvolliset tunnukset on saatu. Tekotavaksi lasketaan siten muun muassa salasananmurto-ohjelmiston käyttö, onnekas arvaus ja toiselta käyttäjältä urkkiminen. [9, s. 155–156] Tietomurtojen havaitsemisen kannalta tämä tarkoittaa muun muassa sitä, että epäonnistuneiden kirjautumisten lisäksi myös laillisten tunnusten käyttöä olisi syytä seurata. On kuitenkin muistettava, että tietomurron täyttyminen edellyttää teolta tahallisuutta eikä siten esimerkiksi vahingossa tietojärjestelmään pääseminen tai joutuminen syöttämällä virheelliset tunnistetiedot johonkin toiseen tietojärjestelmään, johon käyttäjällä on oikeus, täytä tietomurron tunnusmerkistöä [9, s. 156].

Tässä korostuu jälleen yritysten vastuu järjestelmien pääsyhallinnan ja käyttöoikeuksien valvonnan toimivuudesta. Lain henki vaikuttaisi olevan, että tekijän saaminen rangaistusvastuuseen ei onnistu, mikäli tietojärjestelmien suojauksissa ja turvajärjestelyissä on tehty laiminlyöntejä.

Tietojärjestelmään tunkeutumisen ohella tietomurto voi toteutua myös, kun tietojärjestelmästä hankitaan tietoa teknisen erikoislaitteen avulla. Tiedon hankkiminen tehdään siis ilman tunkeutumista kyseessä olevaan järjestelmään. Kyseeseen voisi tulla esimerkiksi tilanne, jossa teknistä laitetta käytetään selvittämään tietojärjestelmästä lähtevän säteilyn perusteella järjestelmässä käsiteltävän tiedon sisältöä. Tämä tekotavan muoto tulisi kysymykseen myös silloin, kun kysymyksessä on siirrettävänä olevan viestin sieppaaminen muualta kuin televerkosta. [9, s. 156] Esimerkiksi tiedon selvittäminen yrityksen sisäverkossa olevan liikenteen sisällöstä sitä seuraamalla täyttäisi tietomurron tunnusmerkistön tämän kohdan perusteella. Mikäli kysymyksessä on luvallisesti verkossa oleva laite, voi liikennettä seuraamalla tapahtuvan tietomurron toteutumisen havaitseminen olla hankalaa, jos liikenteen seuraaminen tapahtuu passiivisesti. Tilannetta voisi kuitenkin ennaltaehkäistä suunnittelemalla sisäverkon reititys siten, että esimerkiksi kytkimien avulla verkossa liikkuvat paketit eivät välity automaattisesti kuin tarkoitetulle vastaanottajalle. Tällöin liikenteen seuraaminen vaatisi todennäköisemmin hyökkääjältä aktiivisia toimia, jotka sitten taas olisi helpompia havaita.

Tietojärjestelmään tunkeutumatta tapahtuva tietomurto voi toteutua lisäksi syöttämällä järjestelmään dataa siten, että järjestelmä virheellisen toiminnan seurauksena antaa ulos sen sisältämää suojattua tietoa. Muun muassa SQL-injektio ja haittaohjelman hyödyntäminen tulevat rangaistavaksi tämän kohdan perusteella. [10, s. 35]

Tietomurto rikoksena täyttyy heti, kun tunkeutuminen tietojärjestelmään on tapahtunut tai siirrettävä tieto siepattu. Täyttyminen ei siis edellytä tiedon sisällön selvittämistä. Tämän lisäksi myös tietomurron yritys on laissa kriminalisoitu. Yritykseksi laskettaisiin muun muassa tietojärjestelmää suojaavan käyttäjätunnuksen selvittämisen yritys tai tunkeutumisen yritys. Tällaisiksi voitaisiin laskea muun muassa järjestelmässä olevien aukkojen ja haavoittuvuuksien tarkoituksenmukainen etsiminen ja kokeileminen. [9, s. 156]

Tietomurron yrityksen rangaistavuudessa on tekijän tarkoituksella suuri merkitys. On muistettava, että tietomurron yrityskin on rangaistavaa ainoastaan tahallisena tekona. Täten esimerkiksi virheellisen käyttäjätunnuksen syöttäminen vahingossa järjestelmään, johon tekijällä ei ole oikeutta, ei täytä tietomurron tunnusmerkistöä [9, s. 156].

2.4 Oikeustapauksia

Tietomurtoja koskevia korkeimman oikeuden ratkaisuja on Suomessa vähän. Käytännössä ainoa tietomurtorikosta koskeva ennakkopäätös on KKO:2003:36 [16], jossa on käsitelty tietomurron yrityksen tunnusmerkistön täyttymistä. Tapauksessa syytetty oli

suorittanut porttiskannausta kohdeyrityksen internetiin yhteydessä oleviin osoitteisiin. Syytetyn itsensä mukaan kyseessä ei ollut tietomurto, sillä skannauksella itsellään eri yritetä murtautua kohdeyrityksen järjestelmään, vaan todeta mahdollisesti avoimet palvelut.

Korkein oikeus on kuitenkin tapauksessa katsonut, että porttiskannaus on toimenpide, jonka avulla pyritään selvittämään tietojärjestelmän eri tietoliikenneporteissa toimivia ohjelmia ja käyttöjärjestelmiä sekä niiden haavoittuvuutta. Porttiskannausohjelmalla on täten mahdollista selvittää tietojärjestelmän mahdollisia aukkoja ja sen heikkoja kohtia. Kyseessä on tällöin toimenpide, jonka avulla kyetään saamaan tietoja luvattoman pääsyn mahdollistamiseksi kohteena olevaan järjestelmään. Vaikka syytetty oli kiistänyt, että hänen tarkoituksenaan olisi ollut tunkeutua kohteena olevaan tietojärjestelmään, korkein oikeus ei pitänyt tätä uskottavana. Korkein oikeus perusteli kantaansa sillä, ettei luvallisesti avoimien palvelinten tai palvelujen etsintään tarvita tällaista ohjelmaa. Korkein oikeus jatkoi vielä, että skannausohjelman ominaisuuksien vuoksi ei muutoinkaan ollut uskottavaa, että sitä olisi käytetty avoimen välityspalvelimen etsintään. Loppupäätöksenään korkein oikeus katsoin syytetyn syyllistyneen tietomurron yritykseen. [16]

Tietomurtojen havaitsemiseen liittyen edellä mainitusta korkeimman oikeuden ratkaisusta on opittavissa, että järjestelmällisesti tehty porttiskannaus tätä varten suunnitellulla ohjelmistolla toteuttaa helposti tietomurron yrityksen. Verkon tapahtumien valvonta tulisikin suunnitella siten, että organisaation tai yrityksen verkon internetiin avoimien osoitteisiin kohdistuva porttiskannaus kyettäisiin havaitsemaan ja siihen liittyvät toimet tallentamaan. Sama luonnollisesti koskee vastaavanlaisen toiminnan havainnointikykyä ja tallentamista organisaation sisäverkossa.

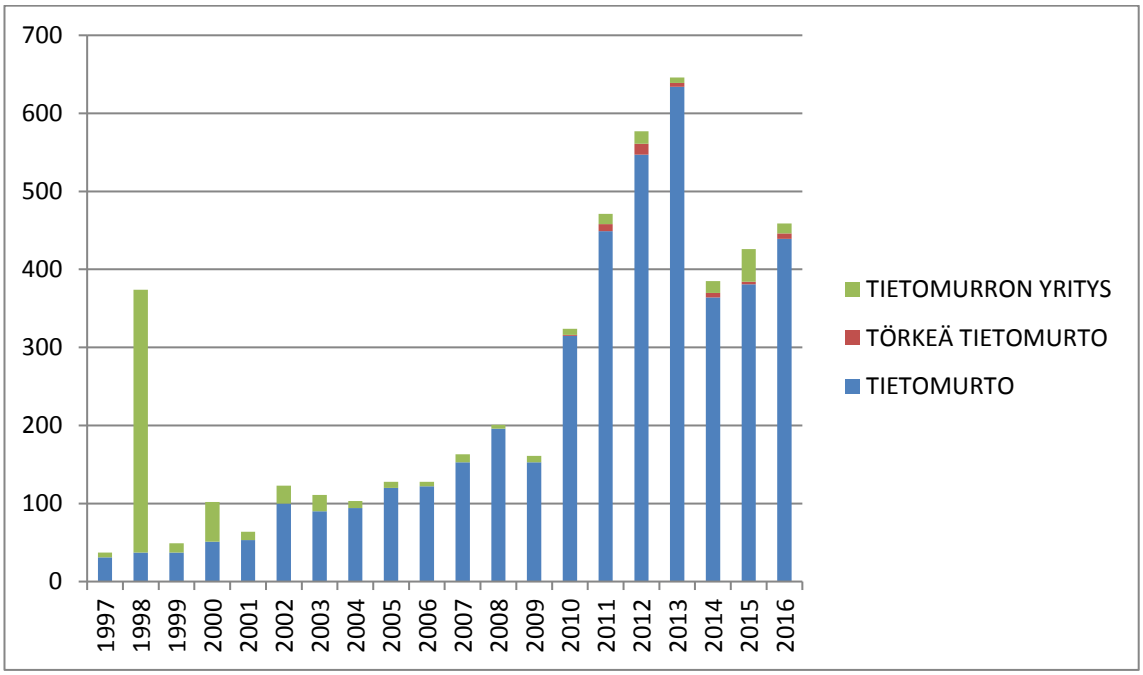
Tietomurtorikoksiin liittyen on hyvä huomioida sen yhteys yritysvakoiluun. Yksi kysymykseen tuleva rikosnimike on rikoslain 30 luvun 4 §:ssä [29] määritetty yritysvakoilu, joka toteutuu muun muassa tapauksissa, joissa hankitaan tieto toiselle kuuluvasta yritys-salaisuudesta tunkeutumalla ulkopuolisilta suljettuun tietojärjestelmään tai käyttämällä teknistä erikoislaitetta. Yritysvakoilun täyttyminen edellyttää lisäksi tarkoituksen salaisuuden oikeudettomaan ilmaisuun tai käyttöön. Pykälän perusteella huomataan, että yritysvakoilun edellä mainitut tekotavat toteuttaisivat samalla myös tietomurron tunnusmerkistön, jonka täyttymisen edellytykset eivät ole yhtä rajatut. Erityisesti yritysten tapauksessa tietomurron toteuttavat teot voivat tulla tietomurron sijasta tulla käsiteltäväksi yritysvakoiluna. Käytännössä tietomurtoa pidetään tällaisessa tapauksessa yritysvakoilun rankaisemattomana esitekona [6, s. 517]. Täten rikosnimikkeiden osalta on syytä huomioida, että pidemmälle edennyt tietomurto muuttuu tietyn kynnyksen jälkeen yritysvakoiluksi. Kaikissa yritysvakoilutapauksissa ei kuitenkaan ole kyse tietomurrosta, sillä yritysvakoilu voi toteutua muutoinkin kuin tietomurron tunnusmerkistön täyttävällä teolla.

Yritysvakoilun osalta korkein oikeus on antanut kaksi ennakkoratkaisua KKO 2013:20 [17] ja KKO 2015:42 [18], joissa kummassakin tapauksessa työnantajan palveluksesta lähtenyt työntekijä oli kopioinut yrityssalaisuuksia ennen työpaikan vaihtoa kilpailijan

palvelukseen. Tapauksissa työntekijällä on ollut luvallinen pääsy kopioinnin kohteena oleviin tiedostoihin, minkä vuoksi niitä ei ole käsitelty tietomurtoina. Kummassakaan tapauksessa korkein oikeus ei katsonut tekojen täyttävän yritysvakoilun tunnusmerkistöä, vaan tuomitsi tekijät yrityssalaisuuden rikkomisesta. Tämän työn rajauksen kannalta keskeisintä on kiinnittää huomiota tietomurtojen täyttävien tekotapojen rajoihin. Luvallisesti yrityksen tietoihin käsiksi pääsevät työntekijät eivät syyllisty tietomurtoon, vaikka heidän tarkoituksenaan olisikin luovuttaa tiedot eteenpäin. Yritysten ja organisaatioiden on ehdottomasti syytä varautua tämänlaisten tilanteiden varalle muun muassa vähimpien oikeuksien periaatetta noudattamalla, mutta koska toiminta ei sellaisenaan täytä tietomurron tunnusmerkistöä, jätetään se tässä työssä tarkastelun ulkopuolelle.

2.5 Tietomurtojen yleisyys

Kuvassa 1 on esitetty poliisille vuosittain ilmoitettujen tietomurtojen lukumäärät. Kuvasta on nähtävissä, kuinka tietomurtojen määrä on lisääntynyt selkeästi vuoden 2010 jälkeen. Kokonaismääriä tarkasteltaessa on hyvä huomioida, että yksittäinen tekijä on samassa yhteydessä saattanut aiheuttaa kymmenien rikosten kirjaamisen. Tämä saattaa toteutua esimerkiksi tapauksissa, joissa porttiskannausta on tehty lukuisiin eri kohteisiin ja jokaisen kohteen osalta kirjataan oma rikoksensa. Kaiken kaikkiaan poliisille ilmoitettuja tietomurtoja näyttäisi kuvan 1 mukaan olevan muutama sata vuodessa.



Kuva 1. *Poliisille ilmoitettujen tietomurtojen vuosittaiset määrät [26]*

Edellä tuotiin esille, että osa tietomurroista voi poliisin tietojärjestelmissä esiintyä yritysvakoiluna. Yritysvakoilutapauksia on kuitenkin vuosittain poliisille ilmoitettu vain muutamia eikä tapauksia ole yhtenäkään yksittäisenä vuonna vuosina 2000–2016 ollut kymmentä enempää [26]. Tämän vuoksi yritysvakoilutapausten huomiotta jättäminen tietojärjestelmistä kerätystä tiedossa ei aiheuta merkittävää eroa pelkästään tietomurroista kerättävien tietojen kautta saatuihin tuloksiin.

Kaikkiaan vuosittaisista tietomurroista vain osaan liittyy jokin yritys tai organisaatio joko asianomistajana tai muuten asianosaisena. Käytännössä tällaisia tapauksia on noin 15–25 % kokonaismäärästä eli keskimäärin 50–100 rikosta vuodessa [25].

Tietomurroista kirjattujen rikosilmoitusten tarkemmasta tarkastelusta käy ilmi, että läheskään kaikki ilmoituksissa kuvaillut teot eivät täytä tietomurron tunnusmerkistöä [25]. Tähän liittyen on myös tärkeää huomioida rikosilmoitusten kirjaamisen kynnys, joka esitutkintalain 3 luvun 1 §:n [4] mukaan on teon kohteena olevan henkilön oma epäily rikoksesta. Eli käytännössä lain mukaan poliisin on kirjattava rikosilmoitus kaikista sellaisista teoista, joita ilmoituksen tekijä itse pitää rikoksena riippumatta siitä, täyttääkö teko todellisuudessa ilmoitetun rikoksen tunnusmerkistöä vai ei. Useissa näistä tapauksista on kuitenkin kysymys ennemminkin identiteettivarkaudesta kuin tietomurrosta [25].

Toinen useista ilmoituksista esiin tuleva epäily tietomurrosta liittyy tilanteeseen, jossa on lähetetty sähköpostia asianomistajan sähköpostiosoitetta muistuttavasta väärennetystä sähköpostiosoitteesta. Tällöin rikoksen tekijä siis muokkaa lähettämänsä sähköpostin otsikkotietoja siten, että sähköposti näyttää saapuneen vastaanottajalle asianomistajan sähköpostista, vaikka näin ei todellisuudessa olekaan. Asianomistaja on kuitenkin tulkinnut tilanteen useissa tapauksissa siten, että hänen sähköpostitililleen on murtauduttu. Vaikka kyseessä on rikos, teko ei kuitenkaan täytä tietomurron tunnusmerkistöä. Tätä tekotapaa on käytetty muun muassa niin kutsuttujen toimitusjohtajahuijausten yhteydessä, jolloin yrityksen talousasioista vastaavalle on toimitusjohtajan väärennetystä sähköpostiosoitteesta lähetetty pyyntö siirtää tietty rahasumma tekijän tilille. [25]

Kolmas yleinen rikosilmoitusten syy on muun muassa Googlen ja Facebookin käyttämät ilmoitukset uusista kirjautumisista tileille. Näihin ilmoituksiin sisältyy usein myös paikkatieto, jonka käyttäjät ovat tulkinneet olevan tarkka, vaikka todellisuudessa sen sisältämä tieto voi vaihdella merkittävästi. Esimerkiksi helsinkiläinen käyttäjä voi saada ilmoituksen, että hänen tililleen on kirjauduttu paikkakunnalta Lappeenranta, vaikka todellisuudessa useassa tapauksessa asiaa selvitettäessä kyseessä on käyttäjän oma useimmiten matkapuhelimen kautta tekemä kirjautuminen. Lisäksi teleoperaattorien käyttämät muuttuvat NAT-osoitteet ovat saaneet osan käyttäjistä epäilemään tietomurtoa, vaikka näissäkin tapauksissa kyseessä on usein heidän oma mobiililaitteensa. [25]

Edellä mainittujen lisäksi palvelujen toimimattomuus, liikennekatkokset ja vastaavat tekniset häiriöt ovat saaneet joitakin ihmisiä epäilemään ensisijaisesti tietomurtoa [25]. Mikään edellä mainituista tekomuodoista ei kuitenkaan toteuta tietomurron tunnusmerkistöä, minkä vuoksi tämänkaltaiset rikosilmoitukset eivät ole johtaneet varsinaisen esitutkinnan aloittamiseen tietomurtoon liittyen. Tietomurtojen kokonaismäärän osalta tämä tarkoittaa sitä, että todellisten tietomurtojen määrä on jonkin verran pienempi kuin puhtaasti tietomurroista kirjattujen rikosilmoitusten kokonaismäärä antaa ymmärtää.

2.6 Tietomurtojen tekotavat rikosilmoitustietojen perusteella

Valtaosa ilmoitetuista tietomurroista liittyy voimassa olevien käyttäjätunnusten väärinkäyttöön. Käyttäjätunnuksia on saatu käyttöön muun muassa läheiseen suhteeseen perustuvan luottamuksen, luvattoman urkkimisen, sähköpostitse toteutetun kalastelun tai asianomistajan tietokoneelle tapahtuneen pääsyn kautta. [25]

Kuvassa 2 ja taulukossa 1 on eritelty tarkemmin eri tietomurtojen eri tekotapoja vuosilta 2014–2016. Kuvassa 2 on eritelty seitsemän yleisintä tekotapaa ja loput harvinaisemmat tekotavat on sisällytetty kohdan "Muu syy" alle. Seuraavalla sivulla esitettävässä taulukossa 1 on nähtävissä kaikkien eri tekotapojen prosentuaaliset osuudet. [25]

Kuva 2. *Tietomurtojen yleisimmät tekotavat vuosina 2014–2016 [25]*

Taulukko 1. *Tietomurtojen tekotavat Suomessa vuosina 2014–2016 [25]*

TEKOTAVAN KUVAUS	%
Käyttäjätunnusten luvaton hyödyntäminen	24,8 %
Fyysinen pääsy kohdelaitteelle	16,3 %
Kalastelu sähköpostin ja/tai valesivuston avulla	14,8 %
Verkkosivustolle tunkeutuminen	10,4 %
Haittaohjelma	10,2 %
Murto- ja/tai etäkäyttöohjelman avulla	4,4 %
Tietokoneen muu hallintaan otto	2,9 %
Lukitsematon tietokone	2,2 %
WLAN-tukiaseman murtautuminen	1,9 %
Entisen työntekijän ongelma	1,9 %
Käyttäjätunnus arvaamalla	1,7 %
Puhelinpalvelimeen murtautuminen	1,7 %
SQL-injektio	1,5 %
Palveluntuottajan ohjelmistoon murtautuminen	1,2 %
Käyttöoikeuksien laajentaminen	1,0 %
Käyttäjän manipulointi	0,7 %
IOT-laitteen haltuunotto	0,7 %
Etäkäyttötunnusten väärinkäyttö	0,7 %
Tilin sulkeminen	0,5 %
Ohjelmiston haavoittuvuuden hyödyntäminen	0,2 %
Porttiskannaus	0,2 %

Kaikkiaan tietomurroista kirjattuja rikosilmoituksia oli vuosina 2014–2016 toista tuhatta, mutta merkittävä osa näistä ei täyttänyt tietomurron tunnusmerkistöä lainkaan tai oli muuten virheellisesti kirjattu. Rikosilmoituksia, joiden mukaan tietomurron voidaan pitää todennäköisesti tapahtuneen tai sen mahdollisuutta ei ainakaan voida poissulkea, oli kaikkiaan 807 kpl. Tästä määrästä on edelleen analysointia varten jätetty pois tapaukset, joista tietomurron tekotapa ei käy ilmi. Lisäksi määrään sisältyvät kaikki ne ilmoitukset, joissa ilmoituksen todenmukaisuutta on ainakin todennäköisiä syitä epäillä. Lopulta kuvassa 2 ja taulukossa 1 esitettävän aineiston pohjaksi jäi yhteensä 412 rikosilmoitusta. [25]

Käytännössä edellä mainittuun määrään sisältyy myös todennäköisesti merkittävä määrä kalastelun kautta toteutettuja tietomurtoja, sillä usein asianomistaja ei ole itse huomannut joutuneensa kalastelun uhriksi tai sitten ei kehtaa sitä myöntää. Rikosilmoituksista tulee esimerkiksi ilmi lukuisia tapauksia, joissa asianomistajan sähköpostitilin tunnukset on saatu haltuun lähettämällä asianomistajalle sähköpostia, joka on vaikuttanut tulevan sähköpostipalvelun ylläpidolta ja jossa on pyydetty vahvistamaan sähköpostitunnukset syöttämällä ne sähköpostissa olevan linkin kautta aukeavalle internet-sivulle. Teko on toteutettu sen verran ammattitaitoisesti, etteivät asianomistajat ole osanneet edes jälkikäteen

tiedostaa joutuneensa kalastelun uhriksi. Asianomistajat ovat huomanneet tietomurron siinä vaiheessa, kun heidän tilinsä väärinkäyttö on alkanut eivätkä he ole osanneet kertoa, miten heidän tunnuksensa ovat päätyneet tietomurron tekijöiden haltuun. [25] Tämä tarkoittaa sitä, että kalastelun liittyvät osuudet kuvassa 2 ja taulukossa 1 ovat todennäköisesti todellisuutta jonkin verran pienemmät.

Yleisimpänä tekotapana on mainittu käyttäjätunnusten luvaton hyödyntäminen. Tässä yhteydessä tällä tarkoitetaan kaikkia sellaisia tekotapoja, joissa rikoksen tekijä on käyttänyt asianomistajan omia voimassa olevia käyttäjätunnuksia, jotka on saanut haltuunsa muuten kuin teknisin keinoin. Näissä tapauksissa asianomistaja on usein kirjoittanut tunnuksensa johonkin ylös, jolloin tekijä on päässyt tunnukset esimerkiksi läheisen suhteen kautta näkemään. Jossain tapauksessa asianomistaja on jopa vapaaehtoisesti antanut tunnuksensa tilapäisesti jonkun toisen käyttöön ja jättänyt salasanansa muuttamatta, mikä on sitten myöhemmässä vaiheessa mahdollistanut tunnusten väärinkäytön. [25]

Fyysiseen pääsyyn liittyvä tekotapa muistuttaa vahvasti edellistä. Tässä kohtaa tekijällä on ollut joko luvallinen tai luvaton pääsy asianomistajan tietokoneelle, tabletille tai älypuhelimelle. Tämä tekomuoto kattaa siten läheisen suhteen, työsuhteen, laitteen hukkaamisen tai sen anastuksen mahdollistaman fyysisen pääsyn laitteelle, joka ei ole ollut siinä määrin lukittuna tai muuten suojattuna, että tietokoneelle tai siinä tallennettuna olleelle tilille tunkeutuminen oli mahdollista. [25]

Kalastelu nimensä mukaisesti tarkoittaa tässä yhteydessä nimensä mukaisesti käyttäjätunnusten kalastelua sähköpostin tai muun viestintäkanavan avulla. Käytännössä tekotapoina on suoraan käyttäjätunnusten pyytäminen vastausviestinä erilaisten syiden perusteella tai käyttäjän ohjaaminen sähköpostin kautta toimitetun linkin kautta sivustolle, jonne käyttäjätunnukset pyydetään syöttämään. Yleisimpiä tällaisia onnistuneita kalastussivustoja ovat olleet muun muassa palvelujen ylläpitäjien, kuten Microsoftin tai Googlen, nimissä esiintyvät sivustot sekä eri pankkien sivustoiksi naamioidut sivustot. Esimerkiksi Microsoftina esiinnyttäessä on käyttäjää uhattu Hotmail-tilin sulkemisella tai tilin voimassaolon päättymisellä, mikäli käyttäjä ei vahvista tiliään erillisellä sivustolla. [25]

Huomionarvoista on, että edellä mainitut kolme tekotapaa muodostavat jo yli puolet kaikista niistä tietomurtojen tekotavoista, jotka ilmoitustietojen perusteella oli mahdollista selvittää. Näiden torjumisen osalta on hyvä myös huomata, ettei näiden tekotapojen muodostamia riskejä voida kokonaan poistaa tai vaikutuksia estää puhtaasti teknisen keinoin, sillä tekotavoissa pyritään ensisijaisesti hyödyntämään niin sanotun inhimillisen elementin heikkouksia. Täten olennaisempaa näiden tekotapojen torjumisessa, havaitsemisessa ja selvittämisessä olisi käyttäjien valistaminen ja kouluttaminen tietoturvallisista toimintatavoista ja käytännöistä.

Henkilöstön tietoturvakoulutuksessa olisi ennalta ehkäisyyn ja torjuntaan liittyvien toimien lisäksi tärkeää huomioida myös havaitsemiseen ja selvittämiseen liittyvät toimet. Havaitsemiseen liittyen on hyvä saada henkilöstö tekemään ilmoitus aina vähänkään varteenotettavalta vaikuttavista tietomurron yrityksistä. Esimerkiksi kalasteluviestien osalta tiedottaminen olisi tärkeää, sillä vaikka viesti vaikuttaisi itselle melko epätoivoiselta yritykseltä, ei se välttämättä kaikille sitä ole. On osattava huomioida, että ihmisillä on hyvin erilaiset taustat ja osaaminen tietoturvaan liittyvistä asioista. Sen lisäksi muun muassa kiire, motivaation puute, hajamielisyys ja rutiinit voivat lisätä riskiä joutua tietomurron uhriksi. Tästä syystä oman yrityksen kohdalla olisi hyvä saada mahdollisimman kattavasti tietoa tietomurtoon liittyvistä yrityksistä oli kyseessä sitten kalasteluviestit, tunnusten urkkimisen yritykset tai fyysinen pääsy. Käyttäjätunnusten, tietokoneiden, puhelinten ja muiden laitteiden lainaamis- tai käyttämispyyntöihin tulisi aina osata suhtautua varauksella. Työyhteisöissä on toki usein yhteiskäytössä olevia laitteita, jolloin tilanne on luonnollisesti eri, mutta lähtökohtaisesti käyttäjätunnuksien lainaamiseen ei tulisi olla mitään perusteltua syytä.

Tietomurtojen selvittämisen osalta yksi keskeisimmistä asioista on tietomurroista ilmoittaminen. Jos tietomurto on tapahtunut jonkun henkilön inhimillisen virheen johdosta, on riskinä, että virheen tehnyt pyrkii peittämään teon välttääkseen arvostelun kohteeksi joutumisen. Tässä kohtaa on suuri merkitys yrityksessä vallitsevalla toimintakulttuurilla. Mikäli virheiden tekijä joutuu aina voimakkaan arvostelun kohteeksi tai häntä rangaistaan muuten ankarasti, on niistä ilmoittamisen kynnys helposti korkeampi. Toisena ääripäänä virheisiin suhtautumisessa on esimerkiksi toimintatapa, jossa henkilöstön palaverien yhteydessä kannustetaan erilaisten virheiden esille tuomiseen, esille ottajalle annetaan suosionosoituksia ja virheen tekemisestä jopa palkitaan.

Verkkosivuille tunkeutuminen on yksi yleisimmistä erityisesti yrityksiin kohdistuvista tietomurtojen tekotavoista. Tähän kategoriaan on sisällytetty kaikki sellaiset verkkosivustoille tunkeutumiseen liittyvät tekotavat, joita ei ole ilmoitusten tietojen perusteella mahdollista yksilöidä tarkemmin jonkun muun tarkemman tekotavan alle. Esimerkiksi erilaisten murto-ohjelmien tai SQL-injektioiden hyödyntäminen on sisällytetty omiin kohtiinsa, mikäli tieto on käynyt ilmi ilmoituksesta, eikä ensisijaisesti tämän kategorian alle. Yksi merkittävimmistä tähän kohtaan sisältyvistä tekotavoista on verkkosivuilla olleen haavoittuvuuden hyödyntäminen, mikä on useammassa tapauksessa johtunut siitä, ettei sivustoja ole päivitetty uusimpiin versioihin. [25]

Haittaohjelmat liittyvät useiden eri tekotapojen suorittamiseen. Omassa kohdassaan kysymyksessä ovat sellaiset tilanteet, jossa haittaohjelman avulla on mahdollistettu pääsy kohteena olevaan järjestelmään tai saatu sieltä tietoa. Haittaohjelman asentumisen tapa asianomistajan tietokoneelle tai muulle laitteelle jää suuressa osassa ilmoituksia mainitsematta. Esille tuotuja asentumistapoja ovat muun muassa haittaohjelman asentuminen vieraillun verkkosivuston kautta, jonkin toisen ohjelman mukana ja itsenään naamioituna

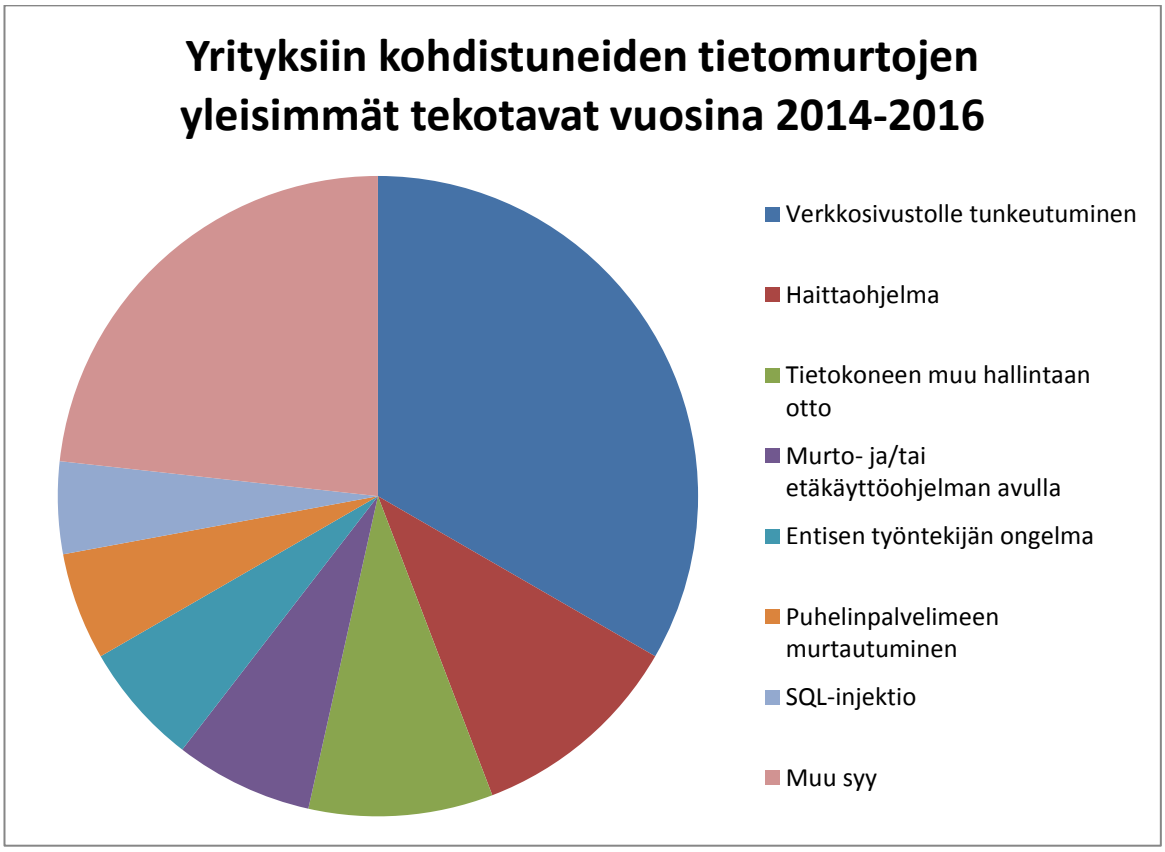
aivan muunlaiseksi ohjelmaksi. Viimeksi mainittu nousee esille erityisesti peliyhteisöissä. Tällöin ohjelma saadaan "lahjana" joltain toiselta pelaajalta, joka kertoo ohjelman antavan asentajalleen jonkun edun pelattavassa pelissä, vaikka todellisuudessa ohjelma kaappaa asianomistajan pelitilin käyttäjätunnukset ja välittää ne hyökkääjälle. [25]

Murto- ja etäkäyttöohjelmien käyttämisellä tarkoitetaan tässä yhteydessä varta vasten tietojärjestelmän suojauksen ohittamiseen tai murtamiseen taikka etäkäytön mahdollistamiseen tarkoitetun ohjelman käyttämistä. Etäkäyttöohjelmien käyttö liittyi pääsääntöisesti tilanteeseen, jossa tekijä oli saanut fyysisen pääsyn asianomistajan koneelle ja siten asentanut ohjelman tämän tietokoneelle myöhempää käyttöä varten. Näissä tilanteissa tekotapa on luokiteltu tämän kategorian alle fyysinen pääsyn sijasta. Käytetyistä murto-ohjelmista rikosilmoituksista mainittiin esimerkiksi erilaiset keylogger-ohjelmat, salasanan murto-ohjelmat, Blackshades, Sentry MBA ja haavoittuvuuksien etsintäohjelmat.

Muiden taulukossa 1 mainittujen tekotapojen osalta mainitaan vielä erikseen WLAN-verkkoon murtautuminen ja entisen työntekijän ongelma. WLAN-verkkoon murtautuminen kattaa tässä yhteydessä muun muassa oletustunnusten käyttämisen ja tukiasemassa olevan haavoittuvuuden hyväksikäytön. Entisen työntekijän ongelma liittyy tilanteeseen, jossa entiseltä työntekijältä on jäänyt käyttöoikeudet peruuttamatta ja niitä on sitten hyödynnetty tietojen hankkimiseen yrityksen tietojärjestelmistä työsuhteen päättymisen jälkeen. Näiden osalta on hyvä huomioida, että vaikkei niiden yleisyys ole kovin suuri, on niillä aiheutettu vahinko usein selkeästi suurempi kuin muilla tietomurtojen tekotavoilla. Puhelinpalveluun murtautumiset liittyvät vuonna 2014 todennäköisesti yhden tekijätahon tekemiin puhelinpalvelimissa olleiden haavoittuvuuksien hyödyntämiseen. Vastaavasti palveluntuottajan ohjelmistoon murtautuminen nousi pinnalle vuonna 2016 tehtyjen suurten yritysten, kuten Yahoo, palvelujen käyttäjätietojen vuotamisen kautta. [25]

Seuraavalla sivulla esitettävässä kuvassa 3 on eroteltu kaikista tietomurroista ne, joiden voidaan katsoa kohdistuneen yrityksiin yksittäisten henkilöiden sijasta. Tässäkin yhteydessä on jätetty pois kaikki sellaiset rikosilmoitukset, joissa tietomurron tunnusmerkistö ei ole täyttynyt tai joista tietomurron tekotapa ei selviä millään tarkkuudella rikosilmoituksen tekstistä. Kuten kuvasta 3 nähdään, eroavat yleisimmät tekotavat hieman kuvassa 2 esitetyistä. Yrityksiin kohdistuvista tietomurroista lähes puolet koostuu verkkosivustoille murtautumisista ja haittaohjelmien avulla tehdyistä teoista. Huomionarvoista kuitenkin on, että vuosina 2014–2016 yrityksiin kohdistuneista tietomurroista oli kirjattu yhteensä 129 sellaista rikosilmoitusta, josta tekotapa oli määritettävissä. Tämä tarkoittaa, että tekotapojen prosentuaaliset osuudet saattaisivat muuttua pienilläkin arvojen muutoksilla. Hieman yllättävää lienee myös, että kalastelu ei ole päässyt yrityksiin kohdistuvissa tekotavoissa listan kärkisijoille, vaikka voisi ajatella yritysten olevan nimenomaan kalastelulle yksityisiä henkilöitä houkuttelevampia kohteita. Kuitenkin kuten jo aiemminkin mainittiin, on kalastelun osuus mahdollisesti tässäkin yhteydessä todellisuudessa suurempi, sillä tietomurron tapahduttua ei sitä välttämättä ole yrityksissä onnistuttu havaitsemaan tai yhdistämään varsinaiseen murtoon. [25]

Lisäksi kuvassa 3 esiin tuotu tietokoneen muu hallintaan ottaminen sisältää tässä yhteydessä sellaiset tapaukset, joissa hyökkääjä on saanut kohteena olevan koneen tavalla tai toisella omaan hallintaansa. Rikosilmoituksista ei näissä tapauksissa kuitenkaan käy ilmi, onko hallintaan ottaminen tapahtunut esimerkiksi haittaohjelman avulla, murto-ohjelmaa käyttäen tai haavoittuvuutta hyödyntäen vai kalastelun kautta saatujen käyttäjätunnusten avulla. Nämä tekotavat siis mitä ilmeisimmän sisältyvät johonkin muuhun kategoriaan, mutta rikosilmoitustietojen perusteella sitä ei ole yksilöitävissä.



Kuva 3. *Yrityksiin kohdistuvien tietomurtojen yleisimmät tekotavat vuosina 2014–2016 [25]*

Tietomurtojen selvittämisen kannalta käy rikosilmoitustiedoista ilmi, että esimerkiksi vuonna 2014 kirjatuista tietomurtoon liittyvistä rikosilmoituksista 14,4 % ja vuonna 2015 kirjatuista 10,0 % on edennyt esitutkinnasta syyteharkintaan. Vuoden 2014 ilmoituksista enää 1 % ja vuoden 2015 ilmoituksista 8,9 % oli tutkimuksen tekohetkellä tammi-helmikuun vaihteessa 2017 vielä avoinna. Käytännössä siis ainoastaan noin joka seitsemäs tietomurrosta tehty rikosilmoitus johtaa syyteharkintaan. Suurin osa tapauksista on joko keskeytetty näytön puuttumisen vuoksi tai rajoitettu kustannusperusteisesti. Näin on toimittu etenkin tapauksissa, joissa rikoksesta epäillyn oletetaan hänen IP-osoitteensa perusteella oleskelevan ulkomailla. Tällöin on katsottu, että tutkinnan jatkamisesta aiheutuvat kustannukset olisivat epäsuhteessa tutkittavana olevan asian laatuun ja siitä mahdollisesti odotettavaan seuraamukseen. [25]

Poliisille ilmoitettuja tietomurtoja koskevat ilmoitukset koostuvat suurimmaksi osaksi tiedoista, jotka ilmoittaja on poliisille kertonut. Siitä seuraa, että tapauksissa, joissa poliisi ei ole suorittanut varsinaisia tutkintatoimia teon selvittämiseksi, ilmoituksien tiedot perustuvat ainoastaan ilmoittajan omiin havaintoihin ja näkemyksiin asiassa. Lisäksi merkittävästä osasta ilmoituksia ei käy ilmi, miten tietomurto on toteutettu, vaan ilmoituksissa keskitytään enemmälti teon ilmitulon ja seurausten selvittämiseen. Tämä on hyvä ottaa huomioon, mikäli rikosilmoitustietojen perusteella olisi tavoitteena tehdä tarkempaa analyysiä tekotapojen yleisyydestä. Tämän työn osalta tietojen keräämisen tarkoituksena oli kartoittaa niitä tekotapoja, joilla todellisuudessa tietomurtoja tehdään. Vaikka merkittävä osa rikosten tekotavoista jää ilmoitustietojen perusteella pimentoon, saadaan kuitenkin jäljellä jäävien ilmoitustietojen perusteella muodostettua kuva niistä tekotavoista, joita vastaan olisi ainakin hyvä varautua. Tuntemattomaksi jääneet tekotavat saattavat korkeintaan tuoda joitain tekotapoja lisää ja vaikuttaa kuvassa 2 listattujen tekotapojen suhteellisiin määriin toisiinsa nähden.

2.7 Tietomurtojen yleisimmät tekotavat muiden raporttien pohjalta

Erilaisia tietoturvauhkia kartoittavia raportteja laativat maailmalla useat eri tahot. Niissä tuodaan esille aina laatijan käsitys tiettyjen uhkien yleisyydestä. Yksi esimerkki näistä on Euroopan unionin verkko- ja tietoturvaviraston (ENISA) vuosittain julkaisema Threat Landscape -raportti. Vuoden 2015 raportin mukaan viisitoista yleisintä tietoturvauhkaa olivat:

1. Haittaohjelmat
2. Verkon kautta tehdyt hyökkäykset
3. Verkkosovelluksiin kohdistuvat hyökkäykset
4. Botnet-hyökkäykset
5. Palvelunestohyökkäykset
6. Fyysinen vahinko, anastus tai häviäminen
7. Sisäpiiriuhka
8. Kalastelu
9. Roskaposti
10. Exploit kit -sivustot
11. Tietojärjestelmiin tunkeutuminen
12. Identiteettivarkaus
13. Tietovuoto
14. Kiristyshaittaohjelmat
15. Kybervakoilu [5, s. 51]

Tämän työn kannalta on hyvä huomata, etteivät kaikki edellä mainituista suoraan toteuta tietomurron tunnusmerkistöä, joten on olennaisinta keskittyä niihin, jotka sen tekevät.

Esille nousevat tällöin osittain haittaohjelmat, verkon kautta tehdyt ja verkkosovelluksiin kohdistuvat hyökkäykset, laitteiden anastus, sisäpiiriuhka, kalastelu, tietojärjestelmiin tunkeutuminen ja kybervakoilu. Tietojärjestelmiin tunkeutumiseksi on tässä yhteydessä laskettu teot, joissa tietojärjestelmästä on onnistuttu hankkimaan tietoa. Määritelmä on siten hieman laissa määriteltyä tietomurtoa suppeampi [5, s. 38–41].

Kun verrataan näitä taulukossa 1 esitettyihin tekotapoihin, huomataan, että ENISA:n arvioissa kalastelu on asetettu hieman alemmas. Kaiken kaikkiaan kuitenkin ENISA:n raportti ja poliisin rikosilmoitustiedot ovat samansuuntaisia. Kybervakoiluun liittyviä tapauksia ei rikosilmoitustiedoista käy ilmi, mikä voi selittyä esimerkiksi niiden havaitsemisen vaikeutena tai haluttomuutena kirjata niistä tietoja rikosilmoitusjärjestelmään.

Yleisesti raportteja käsiteltäessä on syytä kiinnittää huomiota siihen, miten ja mistä tiedot on saatu kerättyä. ENISA:n raportissa tiedot erilaisista tekotavoista ja niiden esiintymismääristä on kerätty useista eri julkisista lähteistä vuoden 2015 ajalta. Julkisten lähteiden lisäksi raportin laadinnassa on hyödynnetty muutamia ENISA:n käytössä olevia tiedonjakofoorumeja esimerkiksi CERT-EU:n kanssa. [5, s. 8] ENISA:n raportissa voisi siten ajatella olevan kysymys eräänlaisesta useiden muiden raporttien koonnoksesta.

Eri tietoturvayritykset laativat myös omia raporttejaan yleisimmistä tietoturvauhista. Tällaisia yrityksiä ovat muun muassa Symantec ja Verizon. Kaikilla näillä on omat tapansa kerätä raporttien pohjana käytettävää tietoa.

Esimerkiksi Symantec käyttää raporttinsa pohjana tietoja ylläpitämästään haavoittuvuustietokannasta, muun muassa yli viidestä miljoonasta niin sanotusta houkutustilistä koostuvasta tiedusteluverkosta, sekä asiakkaidensa verkoista ja tuotteista [31, s. 4]. Houkutustilillä tarkoitetaan sellaista tiliä, jonka tarkoituksena on vaikuttaa mahdollisimman houkuttelevalta kohteelta roskapostille, kalastelulle ja haittaohjelmille ja siten pyrkiä keräämään kattavaa tietoa tällaisiin käyttäjätileihin kohdistuvista uhista.

Symantec ei raportissaan varsinaisesti aseta eri tekotapoja järjestykseen niiden yleisyyden perusteella, mutta kertoo kuitenkin eri tekotapojen yleisyyksistä ja kehittymissuunnista. Symantecin mukaan tietomurtojen määrät ovat viimeisten parin vuoden aikana lievästi kasvaneet. Erilaisten haittaohjelmien määrä, kiristyshaittaohjelmat, sähköpostikalastelu ja verkkohyökkäysten määrä ovat olleet kasvussa. Erityisesti huomioitavaksi tulee, että Symantecin havaintojen mukaan verkkohyökkäysten määrä on yli kaksinkertaistunut vuodesta 2014 vuoteen 2015. [31, s. 8-9]

Verizon sen sijaan pohjaa oman raporttinsa lukuisilta eri organisaatioilta saamiinsa tietoihin tietomurtotapauksista. Vuoden 2015 osalta raportti pohjaa tietonsa yli 100 000 tietoturvallisuuteen liittyvään tapaukseen, joista noin 64 000 tapausta käytettiin varsinaisesti raportin tulosten pohjana. Huomionarvoista on, että näistä 2260 tapauksessa oli kysymyksessä tietojen hankkiminen onnistuneesti kohteena olevasta tietojärjestelmästä. [37, s. 1]

Verizonin laatiman vuoden 2015 tapauksia käsittelevän raportin mukaan yleisimmiksi tietomurtojen tekotavoiksi nousevat haittaohjelmien käyttäminen, anastettujen käyttäjätunnusten hyödyntäminen, haavoittuvuuksien tai takaporttien hyödyntäminen, käyttäjätunnusten kalastelu ja vakoiluohjelmien hyödyntäminen [37, s. 9]. Verizonin havainnot vastaavat niiltä osin myös poliisin rikosilmoitustietoja, sillä Verizonin tekemien havaintojen mukaan 63 % vahvistetuista tietomurroista on liittynyt joko anastettuihin, heikkoihin tai oletuksena annettuihin käyttäjätunnuksiin [37, s. 20].

Suomessa viestintävirasto on omassa vuosikatsauksessaan nostanut esille, että vuoden 2016 perusteella organisaatioihin kohdistuvat merkittävimmät tietoturvauhat ovat päivitysten laiminlyönti, kiristyshaittaohjelmat, kalastelu, ulkoistukset ja laitehankinta sekä palvelunestohyökkäykset. Yksityishenkilöiden osalta on mainittuna huijausten ja kiristyshaittaohjelmien ohella IoT-laitteiden turvallisuus, yksityisyys sosiaalisessa mediassa ja salasanojen kierrätys. [38, s. 4]

Vuonna 2013 suomalaisissa suuryrityksissä tehdyssä tutkimuksessa todettiin, että tutkimukseen osallistuneista kymmenestä yrityksestä puolessa havaittiin merkkejä käynnissä olevista tietomurroista. Yrityksien itsensä kanta oli ollut, että verkon kautta tapahtuva teollisuusvakoilu on lähinnä vain teoreettinen uhka, mikä taas johtunee ainakin osittain siitä, ettei hyökkäyksiä edes havaita. Havaituissa hyökkäyksissä pääosassa tekotapana oli ollut tietoja keräävän haittaohjelman hyödyntäminen. Haittaohjelman saamiseksi yrityksen verkkoon oli käytetty sähköpostia, haavoittuvaista internet-selainta tai USB-muistitikkua. [23, s. 100–101]

2.8 Yhteenveto yleisimmistä tekotavoista

Edellä esitettyjen tietojen perusteella huomataan, että eri tekotapojen painotuksissa on joitakin eroja lähteestä riippuen. Lisäksi on tärkeä huomioida, minkälaisia tapauksia eri lähteissä on analysoitu. Tässä työssä keskitytään Suomen lain mukaan tietomurroksi luokiteltaviin tekoihin, mutta yksityisissä raporteissa käsitellään myös useita muita tietoturvauhkia.

Poliisille tehtyjen rikosilmoitusten osalta heikkoutena on organisaatioihin kohdistuvien tietomurtojen ilmoitusten määrän vähäisyys. Tälle voisi ajatella olevan syynä esimerkiksi se, ettei tekoja todellisuudessa havaita tai ettei niitä ei haluta syystä tai toisesta ilmoittaa poliisille. Toisaalta kun ajatellaan tietomurtouhkia pienten yritysten kannalta, on hyvä huomata, etteivät ne kohteina eroa merkittävästi yksityishenkilöistä. Esimerkiksi pienten yritysten ja yksityishenkilöiden käyttämät ja hallinnoimat tietotekniset laitteet, tietojärjestelmät ja -verkot ovat usein hyvin saman tyyppisiä ominaisuuksiltaan ja rakenteeltaan. Tämän johdosta pienten yritysten tietoturvaratkaisuja pohdittaessa on hyvä pyrkiä huomioimaan yhtä lailla myös yksityishenkilöihin kohdistuvat yleisimmät uhat.

Yksityisten raporttien käytettävyyden haasteena saattaa olla niiden puolueellisuus, sillä raporttien pohjina käytetyt lähteet ovat yleensä profiloituneet tietynlaisiksi. Tietoa kerätään paljon asiakasorganisaatioista tai niin sanotun uutiskynnyksen ylittävistä tapauksista. Tämän tasoiset organisaatiot ovat usein kooltaan huomattavia ja muodostuvat siten oman asemansa ja näkyvyytensä kautta omanlaisiksi kohteiksi tietoturvahyökkäyksille. Esimerkiksi suuren monikansallisen useita satoja tuhansia asiakastietoja käsittelevän yrityksen tietojärjestelmä muodostaa houkuttelevuutensa puolesta hyvinkin erilaisen kohteen kuin korkeintaan satoja asiakastietoja käsittelevän alle kymmenen hengen elektroniikkayrityksen tietojärjestelmä. Tämä ei tosin tarkoita, etteikö kumpikin voisi joutua yhtä lailla tietomurtohyökkäysten kohteeksi, mutta hyökkäysten motiivi ja siten hyökkääjien laatu ja menetelmät saattavat hyvin erota toisistaan.

Poliisille tehtyjen rikosilmoitusten perusteella nousee hyvin keskeisesti esille inhimillisen tekijän merkitys. Selvästi yli puolet kaikista tietomurroista oli mahdollistunut jonkin käyttäjän itsensä tekemän toimen kautta. Käyttäjätunnukset on annettu toiselle käyttöön, niitä on säilytetty tai käytetty huolimattomasti, omaa laitetta ei ole suojattu ulkopuoliselta käytöltä tai on sorruttu kalastelu- tai huijausviestin uhriksi. Näiden lisäksi on syytä huomata, että haittaohjelmien kohdalla inhimillinen elementti on usein mukana mahdollistamassa ohjelman asentumisen järjestelmään. Käytännössä taulukon 1 tietojen perusteella käyttäjien huolellisilla ja tietoturvallisilla toimintatavoilla olisi saatu ehkäistyä yli 70 % kaikista tietomurroista.

Kuten kuvasta 3 käy ilmi, organisaatioiden kohdalla niistä ulospäin näkyvät verkkopalvelut, kuten internet-sivut, muodostavat todennäköisimmän kohteen tietomurrolle. Symantecin raportin mukaan vuonna 2015 78 % tarkastetuista verkkosivuista sisälsi jonkin haavoittuvuuden. Näistä 15 % oli kriittisiä haavoittuvuuksia, joiden avulla haitallisen koodin ajaminen verkkosivulla on mahdollista ja joiden kautta mahdollistuu siten myös verkkosivustolle murtautuminen. [31, s. 20]

Verizonin mukaan verkkosovelluksiin kohdistuvista tietomurroista valtaosa toteutettiin anastettujen ja kalasteltujen käyttäjätunnusten avulla, hyödyntäen ohjelmistossa olevaa takaporttia tai haavoittuvuutta taikka haittaohjelman avulla [37, s. 29]. Käytännössä tämän kautta korostuvat inhimillisen elementin lisäksi ohjelmistojen päivittäminen, toteutuksen turvallisuus sekä haittaohjelmien torjunta. Ohjelmistojen jatkuva päivittäminen ja pitäminen ajan tasalla on yksinkertaisin tapa ehkäistä haavoittuvuuksien hyödyntämistä. Ohjelmistojen toteutuksen turvallisuuden kannalta on syytä kiinnittää huomiota, mistä ja keneltä oman organisaation käyttöön tarvittava ohjelmisto hankitaan. Haittaohjelmien osalta käyttäjien ohjeistamisen lisäksi on tärkeää hyödyntää myös haittaohjelmien torjuntaan keskittyviä ohjelmistoja.

3. PIENYRITYSTEN TIETOTURVARATKAISUT

Tässä työssä tarkastellaan tietoturvaratkaisuja pienten yritysten näkökulmasta. Pieneksi yritykseksi lasketaan sellaiset yritykset, joilla ei ole päätoimista tietoturvahenkilöstöä ja jonka henkilöstön kokonaismäärä on korkeintaan kymmenen henkilöä. Toisaalta esitetyt toimintamallit ja tekniset ratkaisut ovat ainakin osittain hyödynnettävissä myös suuremmille yrityksille etenkin, mikäli niiden tietoverkon rakenne ja muut tietotekniset ratkaisut ovat pienten yritysten kaltaisia.

Kun ajatellaan alle 10 hengen yritystä, rajoittuu käytössä olevien työasemien määrä myös todennäköisesti alle kymmeneen. Näiden lisäksi yrityksellä saattaa hyvin olla oma tiedostopalvelin, www-palvelin, VPN-palvelin, WLAN-tukiasema, erilaisia IoT-laitteita sekä muita eritoten tuotantotyössä tarvittavia verkkoon liitettäviä laitteita.

Yrityksen käytössä olevien erilaisten laitteiden määrä ja laatu vaikuttavat suuresti siihen, mitä kaikkia asioita muun muassa sen tietoverkon rakenteessa tulisi tietoturvan kannalta ottaa huomioon. Sovellettavia perusperiaatteita, kuten looginen erottelu ja vähimpien oikeuksien periaate, on useita ja niistä on kerrottu tarkemmin valtionvarainministeriön VAHTI-työryhmän sisäverkon toteuttamiseen keskittyvässä ohjeessa [35].

Tässä työssä ei paneuduta puhtaasti ennaltaehkäiseviin ratkaisuihin tai tietoverkon rakenteen tietoturvalliseen suunnitteluun sen syvällisemmin, vaan tarkoituksena on keskittyä niihin ratkaisuihin, joilla kyetään ensinnäkin havaitsemaan tietomurron tunnusmerkistön täyttävää toimintaa ja toiseksi edesauttamaan niiden selvittämistä havaitsemisen jälkeen. Erilaisia ratkaisuja on pyritty pohtimaan seuraavassa esiteltävän esimerkkiyrityksen kautta.

3.1 Esimerkkiyrityksen esittely ja nykytilan kartoitus

Esimerkkiyrityksenä on tässä työssä elektroniikka-alan yritys, jolla on tasan kymmenen työntekijää ja josta tässä yhteydessä käytetään nimeä Y-malli Oy. Yritys kehittää, tuottaa ja myy erilaisia elektroniikkalaitteita. Yrityksen asiakkaat muodostuvat sekä yksityisistä henkilöistä ja yrityksistä että julkisen sektorin organisaatioista.

Yritykselle toteutettavien tarkoituksenmukaisten tietoturvaratkaisujen pohdinta aloitettiin tekemällä ensimmäiseksi yrityksen nykytilan kartoitus. Tässä kartoituksessa selvitettiin henkilöstön haastattelujen ja yrityksen tilojen tarkastelun kautta, missä ja miten tietoa yrityksessä säilytetään, miten tietoa käsitellään ja siirretään sekä miten tiedot on suojattu.

Lähes jokaisella yrityksen työntekijälle on oma henkilökohtainen työasemansa, johon hän tallentaa omat työnsä. Työasemissa on käytössä Windows 7 -käyttöjärjestelmät. Nämä

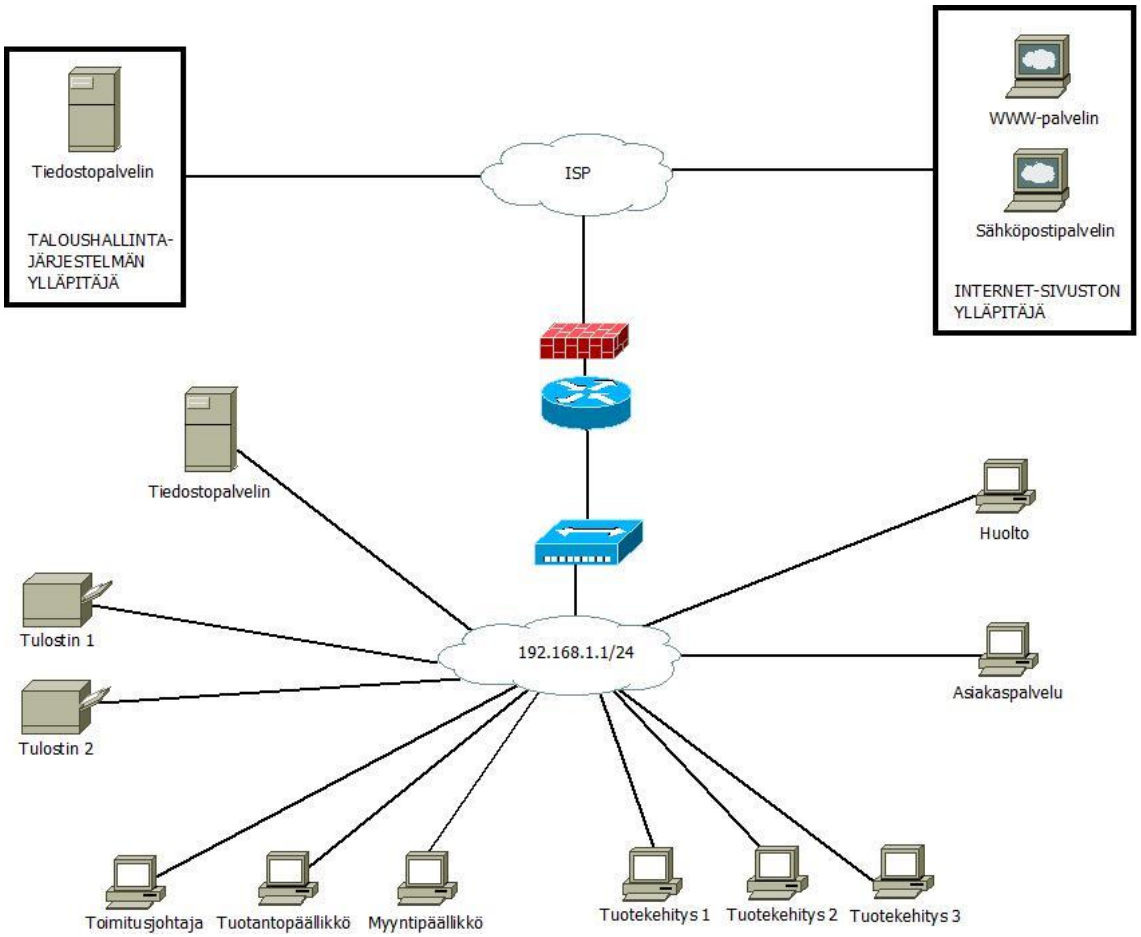
tiedot siirretään säännöllisesti yrityksen omalle tiedostopalvelimelle. Yrityksellä on lisäksi muutama erillinen tuotanto- tai mittauslaite, kuten CNC-sorvi, johon on tallennettu sen käyttöön liittyviä tietoja. Yrityksellä on tiloissaan kaksi verkon kautta käytettävää tulostinta, jotka myös säilyttävät joitain tietoja tulostetuista ja skannatuista asiakirjoista.

Yrityksellä on olemassa internet-sivut, jotka ovat ulkopuolisen palveluntarjoajan ylläpitämät. Yrityksen omalla henkilöstöllä on mahdollisuus internet-selaimen kautta muokata sivuston sisältöä haluamakseen. Sivustolla on tietoa muun muassa yrityksen tuotteista, yhteystiedoista ja henkilöstöstä. Sivustoa ylläpitävä yritys on tarjonnut Y-malli Oy:lle myös sähköpostipalvelimen, jonka kautta yrityksellä on käytössä kuusi sähköpostiosoitetta.

Yritys on lisäksi hankkinut ulkopuoliselta yritykseltä taloushallintaa varten oman ohjelmiston, johon on tallennettu yrityksen asiakkaiden tiedot muun muassa laskutusta ja kirjanpitoa varten. Asiakastietojen lisäksi ohjelmistossa on tiedot yrityksen myynneistä, tilauksista ja varastotilanteesta. Tätä järjestelmää käytetään etäyhteyden kautta yrityksen omilta pääteasemilta.

Tiedon siirrossa yrityksen omien laitteiden välillä käytetään omaa sisäverkkoa. Sisäverkko noudattaa tähtitopologiaa eli kaikki yrityksen tietokoneet ovat yhteydessä toisiinsa ja ulkoverkkoon yhden reitittimen ja siihen liitetyn kytkimen kautta. Langallisesti verkkoon on liitetty yhteensä kahdeksan työasemaa ja tiedostopalvelin. Edellä mainittu reititin toimii samalla myös langattoman WLAN-verkon tukiasemana. WLAN-verkko on yrityksen henkilöstön omassa käytössä ja siihen on työaikoina liittyneenä muutamia mobiililaitteita, joilla ei kuitenkaan säilytetä tai käsitellä yrityksen toimintaan liittyviä tietoja. Edellä mainittuja tuotanto- ja mittauslaitteita ei ole liitetty sisäverkkoon millään tavalla. Kuvassa 4 on kuvattu karkeasti tiedon säilytys- ja käsittelypaikat sekä niiden väliset yhteydet yrityksessä.

Yrityksen verkko on suojattu ulkopäin reitittimessä olevalla palomuurilla, jolla on estetty kaikki yhteydet ulkoverkosta sisäverkkoon. Vastaavasti yrityksen WLAN-verkko on suojattu WPA2-personal suojausta käyttäen ja siihen liittyminen vaatii käyttäjätunnuksen ja salasanan käyttämisen. Kaikki työkoneet on suojattu käyttäjätunnuksilla siten, että niiden käyttäminen edellyttää voimassaolevan käyttäjätunnuksen ja salasanan syöttämistä. Vastaavasti sisäverkossa oleva tiedostopalvelin on suojattu käyttäjätunnuksen ja salasanan avulla. Minkäänlaista loogista erottelua sisäverkossa ei ole tehty, vaan jokaiselta verkkoon liitetyltä työasemalta on pääsy muille työasemille ja tiedostopalvelimelle.



Kuva 4. *Y-malli Oy:n tiedon säilytyspaikat ja niiden välisten yhteyksien muodostama tietoverkko*

Vaikka yrityksen tietoturvallisuuden kokonaisvaltaiseksi parantamiseksi olisi syytä tarkastella tietoturvaratkaisuja laajemminkin, rajataan tässä yhteydessä tarkastelu koskemaan lähinnä tietomurtojen havaitsemiskyvyn ja selvittämismahdollisuuksien tehostamiseen liittyviä menetelmiä ja ratkaisuja. Kokonaisvaltaisemmassa tietoturvakartoituksessa ja tietoturvan parantamisessa kyseeseen tulisivat muun muassa riskianalyysin toteuttaminen, verkon rakenteen ja suojausten arviointi, verkon erottelu, palomuuripolitiikoiden arviointi, saatavuuden varmistaminen ja kahdennusten toteuttaminen.

3.2 Tietoturvallisuuden merkitys

Yrityksien kannalta nykypäivänä yksi tärkeimmistä ellei tärkein pääoma on tieto ja sen ylläpitämiseksi tarvitaan erilaisia tietojärjestelmiä ja tietoverkkoja. Liiketoiminta on tullut jopa niin riippuvaiseksi tiedosta ja tiedonkulusta, että esimerkiksi yhteyksien katkeaminen, tiedon saatavuusongelmat ja salassapidon pettäminen aiheuttavat valtaosalle yrityksistä merkittäviä ongelmia ja vahinkoja. Toiminnan sujuvuuden häiriintymisen ja taloudellisten vahinkojen lisäksi tietomurtojen uhriksi joutuminen muodostaa yrityksille

myös maineriskin, sillä asiakkaiden ja mahdollisten sijoittajien menettäminen muodostavat vakavan uhan yrityksen toiminnan jatkuvuudelle. [23, s. 98–99]

Y-malli Oy:llä on runsaasti sille arvokasta tietoa, jonka varassa se toimii ja jonka avulla se pyrkii erottautumaan kilpailijoistaan. Näitä tietoja ovat muun muassa yrityksen toimintaan, strategiaan ja toimintamenetelmiin liittyvät tiedot, kaikki valmistettavien laitteiden tuotantoon liittyvät tiedot, tulevien tuotteiden suunnittelu ja tuotekehitystiedot sekä asiakassuhteisiin ja -myyntiin liittyvät tiedot. Käytännössä kaikki sellainen tieto, jota ei ole varta vasten tarkoitettu julkaistavaksi on katsottu siinä määrin arvokkaaksi, että sen tulemisesta julkiseksi olisi ainakin jossain määrin haittaa yrityksen toiminnalle. Täten tietoturvallisuudella on merkitystä ensinnäkin yrityksen toiminnan mahdollistamisessa ja toiseksi mahdollisen kilpailuedun saavuttamisessa ja säilyttämisessä.

Esimerkiksi Y-malli Oy:ssä tiedon suojaamisessa on keskitytty pääasiassa ennalta ehkäisyyn, minkä varaan on laskettu paljon. Ajatuksena on ollut, että rakennetaan ja hankitaan omasta näkökulmasta riittävä suojaustaso ja luotetaan sen pitävyyteen. Y-malli Oy:ssä ei ole juurikaan huomioitu mahdollisesti tapahtuvien tietomurtojen havaitsemista. Vaikka lokitietoja kerätään tietyistä asioista, niitä ei käytännössä seurata mitenkään.

Nykyään on kuitenkin melko riskialtista laskea puhtaasti sen varaan, että oma tietojärjestelmä kestäisi kaikki mahdolliset tunkeutumisyritykset. Tämän johdosta olisi tärkeää pohtia myös ratkaisuja ja toimintamalleja siltä varalta, että tietomurto on kaikista ennalta ehkäisevistä toimista huolimatta päässyt jo tapahtumaan. Varhaisella havaitsemisella kyetään todennäköisemmin rajaamaan tietomurron laajuutta ja vähentämään siitä aiheutuvien vahinkojen suuruutta. Voidaan ajatella, että mitä kauemmin tietojärjestelmään tunkeutuminen ja sen hyväksikäyttö ovat mahdollisia, sitä enemmän vahinkoa tunkeutumisesta ehtii yritykselle aiheutua. Mahdollisten vahinkojen määrän minimoinnin voisi kuvitella olevan kaikkien yritysten intressinä. Ilman ajantasaista havaitsemisjärjestelmää pitenee tietomurroista toipumiseen kuluva aika [1, s. 232].

Havaitseminen merkitys tulee esille myös murretun tietojärjestelmän väärinkäytön seurauksien kautta. Jos esimerkiksi tunkeutuja käyttää murtamaansa tietojärjestelmää hyväksi joko muihin järjestelmiin tunkeutumiseen tai muuhun rikolliseen toimintaan, saatetaan tämän hyväksikäytetyn tietojärjestelmän omistajaa ja ylläpitäjää pitää myös osaltaan vastuullisena aiheutuneista seurauksista. [1, s. 232] Erityisesti tietojärjestelmän ylläpitäjän maine saattaa kärsiä merkittävästikin, mikä korostaa aikaisen havaitsemisen ja hyökkäystoiminnan rajaamisen merkitystä.

Havaitsemisjärjestelmän yhtenä toimintaesimerkkinä voisi olla tilanne, jossa havaitaan hyökkäysliikenne jostain tietystä IP-osoitteesta. Tällöin voidaan kyseinen osoite asettaa niin sanotulle mustalle listalle, jolla kielletään kaikki liikenne hyökkääjän IP-osoitteesta.

Näin saadaan nopeasti ja yksinkertaisesti estettyä hyökkääjän kaikki tunkeutumisyritykset kyseisestä osoitteesta. Pienten yritysten kannalta tällaisten ratkaisujen etuna on mahdollisuus niiden automatisointiin. [21, s. 195]

EU:n uuden tietosuoja-asetuksen myötä taloudellisten vahinkojen lisäksi saattaa havaitsemiskyvyn laiminlyönti jatkossa aiheuttaa huomattavan suuruisen hallinnollisen maksun. EU:n tietosuoja-asetuksen 83 artiklan [28] mukaan tietomurrosta ilmoittamatta jättämisestä saattaa tietyissä olosuhteissa seurata hallinnollinen maksu, jonka yläraja on joko 10 miljoonaa euroa tai 2 % yrityksen maailmanlaajuisesta liikevaihdosta riippuen siitä, kumpi niistä on suurempi. Täten lainsäädännön perusteella voi yritykselle aiheutua taloudellisia seuraamuksia myös varsinaisten taloudellisten vahinkojen lisäksi.

Tietoturvaan panostaminen nousee esille myös yritystoimintaa tukevien organisaatioiden kautta. Esimerkiksi kansainvälinen kauppakamari on laatinut yrityksille kuuden toimenpiteen listan tietoturvaan liittyvien riskien vähentämiseen. Listan kohta numero neljä ohjeistaa yritystä seuraamaan toimintaympäristöään siten, että se kykenee havaitsemaan mahdolliset tietoturvauhat ja -loukkaukset. Ohjeessa kehotetaan hyödyntämään tunkeutumisen havainnointi- ja estojärjestelmiä, mutta korostetaan, ettei niiden pelkkä asentaminen riitä. Järjestelmien tehokas hyödyntäminen edellyttää niiden jatkuvaa käyttöä ja analysointia. [15, s. 10–11]

Tietomurtojen selvittämisen huomiointi tietoturvaratkaisujen toteuttamisessa sen sijaan luo mahdollisuuden saada murron tekijä selville ja vaatia tältä ainakin jonkinasteista korvausta aiheutuneista vahingoista. Selvittäminen kuitenkin edellyttää, että tietomurto kyetään ylipäänsä havaitsemaan, joten selvittämisenkin kannalta tietomurtojen havaitsemiskyvyn omaaminen on keskeistä [1, s. 232]. On hyvä muistaa, että kuten luvussa 2 tuotiin esille, vain noin reilu 10 % poliisille tehdyistä rikosilmoituksista etenee syyteharkintaan. Yksi merkittävä syy tähän rikosilmoituksista ilmi käyvien tietojen perusteella on näytön puuttuminen tai sen hankkimisen kustannusten suuri määrä [25]. Vaikka ulkomailla toimivien hakkeriryhmien tekemien rikosten selvittämisen tai tekijöiden vastuuseen saamisen todennäköisyys on ainakin toistaiseksi melko pieni, saadaan hyvin kerätyllä tietomurtoon liittyvällä todistusaineistolla lisättyä ainakin kotimaisten tekijöiden saamista vastuuseen teostaan. Tässä yhteydessä on hyvä muistaa, että taulukosta 1 ilmi käyvien tietojen perusteella tietomurtojen toiseksi yleisin tekotapaa sisältää fyysisen pääsyn kohdelaitteelle, joka siis ainakin puhtaasti kotimaisten yritysten kohdalla edellyttää ainakin tekijän käymistä Suomessa.

Edellä mainitussa kansainvälisen kauppakamarin kuuden kohdan ohjeen viimeisessä kohdassa viitataan tietomurtojen selvittämiseen, kun siinä ohjeistetaan valmistautumaan tietomurtojen varalle. Valmistautumiseen sisältyy valmius nopeasti ryhtyä toimiin tietomurron selvittämiseksi. Teon piirteiden, siitä jääneiden jälkien ja tekijän identiteetin selvittämisen lisäksi valmiuteen korostetaan kuuluvaksi myös vahinkojen minimointi, toiminnan

jatkuvuuden varmistaminen sekä oikeanlaisten resurssien ja työkalujen varaaminen tietomurtojen tapahtumisen varalle. [15, s. 11–12]

3.3 IDS-järjestelmät

Tunkeutumisen havaitsemista varten tarvitaan siihen kykenevä järjestelmä eli niin sanottu IDS-järjestelmä (engl. intrusion detection system). IDS-järjestelmät edustavat palomuurien ja muiden ennalta estävien laitteiden jälkeistä puolustuksen seuraavaa kerrosta. Kyseessä on yleensä erillinen laite, tyypillisesti tietokone, joka seuraa verkkoliikennettä ja tapahtumia haitallisen tai epäilyttävän toiminnan havaitsemiseksi. Havaitessaan tällaista toimintaa järjestelmä pyrkii reagoimaan siihen määrätyillä tavoilla, joita voivat olla esimerkiksi tilanteen tarkempi seuraaminen ja tallentaminen, järjestelmän suojauksen tehostaminen ja ylläpitäjälle ilmoittaminen. [24, s. 484–489] Tietomurtojen havaitsemisessa ja niihin liittyvän tiedon keräämisessä IDS-järjestelmät ovat keskeisessä roolissa. Vastaavasti tietomurtojen selvittämisen ja jälkihoidon kannalta on tärkeää kyetä suojaamaan hyökkäyksen kohteena oleva järjestelmä ja tallentamaan hyökkäyksestä tehdyt havainnot. Kun suojaamiseen liittyy esimerkiksi hyökkääjän yhteyden katkaiseminen ja yhteysosoitteen estäminen, puhutaan jo niin sanotuista tunkeutumisen estojärjestelmistä eli IPS-järjestelmistä (engl. intrusion prevention systems) [32, s. 337].

IDS-järjestelmiä on erilaisia, mutta käytännössä ne voidaan jakaa kahteen eri kategoriaan, jotka ovat tunnusmerkkeihin perustuvat ja poikkeavuuksiin perustuvat. Tunnusmerkkeihin perustuvat järjestelmät etsivät tietovirrasta tunnettuja hyökkäyksiä muistuttavia jälkiä ja piirteitä eli tiedossa olevia tunnusmerkkejä. Esimerkkinä voisi olla hyvin lyhyessä ajassa tapahtuva TCP SYN -pakettien lähettäminen eri portteihin, mikä viittaisi todennäköisesti porttiskannauksen suorittamiseen. Tunnusmerkkeihin perustuvissa järjestelmissä heikkoutena on, että ainoastaan sellaiset hyökkäykset, joiden tunnusmerkit ovat tiedossa, kyetään havaitsemaan. Poikkeavuuksiin perustuvat järjestelmät sen sijaan reagoivat poikkeavaan toimintaan. Niissä määritetään aluksi verkon normaalitila, minkä jälkeen järjestelmä antaa ilmoituksia tästä normaalitilasta poikkeavasta käyttäytymisestä. Tällaiset järjestelmät voidaan myös opettaa pitämään tiettyjä toimintoja normaaleina sen mukaan, kun niitä esiintyy. [24, s. 486–487]

IDS-järjestelmät voidaan lisäksi jakaa verkkopohjaisiin ja isäntäpohjaisiin järjestelmiin. Verkkopohjaisissa järjestelmissä IDS on koko verkon tilaa ja liikennettä seuraava itsenäinen laite. Isäntäpohjaisissa järjestelmissä sen sijaan IDS on asennettu yhdelle laitteelle, jossa se keskittyy suojelemaan tätä kyseistä isäntälaitetta. [24, s. 485]

Liikenteen ja tapahtumien seuraamisen lisäksi IDS-järjestelmillä on usein kyky ottaa vastaan useilta laitteilta lähetettyjä lokeja ja tarkastamaan näitä hyökkäyksien varalta. [32, 335] Lokeihin on pyrittävä tallentamaan mahdollisimman kattavasti tiedot hyökkääjän toiminnasta. Käytännössä tämä edellyttää hyökkäystoiminnan mahdollisimman hyvin

huomioon ottavia tallennussääntöjä ja siten toimivaa lokipolitiikkaa. Lokitiedoilla ja niiden tarkastelulla on merkitystä hyökkäyksen laadun ja laajuuden määrittämisessä.

Käytännössä parhaimmat IDS-järjestelmät ovat yhdistelmä kaikkia edellä mainittuja. Optimaalisessa tilanteessa järjestelmän tulisi olla nopea, yksinkertainen ja tarkka, mutta samalla myös mahdollisimman kattava. IDS-järjestelmien suurin heikkous on virheellisten ilmoitusten antaminen. Niitä suunniteltaessa yksi keskeisimmistä asioista on sopivan ilmoituskynnyksen löytäminen. Liian matala kynnys johtaa virheellisiin ilmoituksiin ja liian korkea taas jättää todellisia hyökkäyksiä huomioimatta. [24, s. 488–490]

IDS-järjestelmien luonne tekee niistä myös kohteen hyökkääjille. Tämän vuoksi on tärkeää, että IDS:n toiminta tietoverkossa olisi mahdollisimman näkymätöntä. Käytännössä tämä voidaan toteuttaa siten, että sillä on verkkoon kaksi erillistä liitäntää. Ensimmäinen on puhtaasti verkon seurantaa varten ja toinen hälytysten lähettämiseen ja mahdollisesti muihin järjestelmän hallintaan liittyviin toimintoihin. [24, s. 487]

IDS-järjestelmiksi laskettavia järjestelmiä on nykypäivänä markkinoilla lukuisia erilaisia. On kaupallisia järjestelmiä, jotka voi ostaa käyttöönsä, tai avoimeen lähdekoodiin perustuvia verkosta ladattavia ilmaisjärjestelmiä. Suljetun koodin ilmaisjärjestelmiin osalta on syytä suhtautua varauksella, sillä niiden laadusta ja kaikista toiminnallisuuksista ei ole mitään takuita. Tämän vuoksi ne on jätetty tämän työn puitteissa huomioimatta.

3.4 Kaupalliset tietoturvaratkaisut ja -palvelut

Koska tietoturvallisuuden merkitys on yhteiskunnassa lisääntynyt, samalla myös erilaisten tietoturvatuotteiden tarjonta on kasvanut. Perinteisesti tietoturvatuotteet on ajateltu palomuurina ja viruksentorjuntaohjelmistona. Nykyään kuitenkin eri yritysten tarjoamat tietoturvapaketit tarjoavat myös muuta. Y-malli Oy:lla on käytössä F-Securen SAFE -ohjelmisto, jonka tehtävänä on suojata yrityksen tietokoneita laittomalta pääsyltä ulkoa päin sekä havaita mahdollisia viruksia ja haittaohjelmia. SAFE-ohjelmisto maksaa Y-mallin tapauksessa 99,90 euroa vuodessa, ja sillä saadaan suojattua 7 tietokonetta [7]. Myös teleoperaattoreilta olisi mahdollista hankkia vastaavanlaisia tietoturvaohjelmistoja. Palomuurien ja viruksentorjunnan osalta löytyy toki myös ilmaisohjelmia, joista Windows-käyttöjärjestelmien kohdalla mahdollisuuksina olisivat esimerkiksi Microsoftin oma Security Essentials Windows 7 -käyttöjärjestelmälle ja Windows Defender Windows 10 -käyttöjärjestelmälle.

Edellä mainitut ohjelmistot auttavat suojaamaan yritystä erilaisten haittaohjelmien varalta ja ohjelmistot pitävät pääsääntöisesti kirjaa havainnoistaan. Ohjelmistot eivät kuitenkaan auta juurikaan muiden tietomurtojen tekotapojen havainnoinnissa. Tätä varten tarvitaan erikseen myös IDS-järjestelmiä, joiden avulla saadaan kerättyä tietoa muun muassa tietojärjestelmiin tunkeutumisista, kirjautumisista, niissä olevan tiedon käytöstä ja siirrosta.

Seuraavassa esitellään muutamia satunnaisesti valittuja markkinoilla nykypäivänä olevia IDS-järjestelmiksi laskettavia tuotteita ja niihin liittyvä palveluja.

Tunkeutumisen havainnointi sisältyy usein yhtenä osana yrityksille tarjottavia SIEM-ratkaisuihin eli keskitetyn tietoturvainformaation ja -tapahtumien hallintajärjestelmiä (engl. Security Information and Event Management). Ruotsalainen IT-yritys Pulsen tuo kotisivuillaan esille SIEM-ratkaisujen käyttöönottoon liittyvän valinnan vaikeuden ja vaadittavan investoinnin määrän ja pitkäaikaisuuden. He markkinoivat omaa SIEM-ratkaisuaan nopeaksi ottaa käyttöön ja mainostavat palvelun muokattavuutta asiakasyrityksen tarpeiden mukaan. Tarvittaessa he voisivat hoitaa myös järjestelmän tuottamien hälytyksien seurannan ja raportoinnin. [27]

Suomalainen F-Secure markkinoi asiakkailleen ratkaisuna omaa Rapid Detection Service -palveluaan. Rapid Detection Service on kokonaisvaltainen palvelu, joka sisältää muun muassa tietoturvauhkien havainnoinnin ja niihin reagoinnin. F-Secure lupaa asiakkailleen, että havaitusta hyökkäyksestä ilmoitetaan asiakkaalle alle 30 minuutissa viikonpäivästä ja vuorokauden ajasta riippumatta. Käytännössä järjestelmä on rakennettu siten, että kaikki yrityksen työasemat ja verkon strategisesti keskeiset paikat varustetaan sensoreilla, jotka keräävät tietoja laitteiden ja verkon tilasta analysointia varten. Varsinaisesti hyökkäysten tunnistaminen tapahtuu poikkeamien etsimisellä hyödyntäen F-Securen analyysityökaluja ja koneoppimista. Kaikki tapahtumien tiedot tallennetaan erilliseen suojattuun tietovarastoon, jolla estetään jälkien hävittäminen ja todistusaineiston manipulointi. [8]

Sen lisäksi, että eri tietoturvayrityksillä on omia tuotteita tunkeutumisen havainnointiin, tarjoaa osa yrityksistä, kuten Nixu ja Insta, tunkeutumisen havainnointijärjestelmien asennus- ja ylläpitopalvelua. Esimerkiksi Nixu markkinoi kotisivuillaan käyttävänsä ohjelmistoina muun muassa HP ArcSightia ja Splunkia [22]. Insta sen sijaan markkinoi itseään suoraan tuoteriippumattomana toimittajana ja auttavansa asiakasyritystä löytämään juuri sille sopivimman ratkaisun [14].

Toisaalta yrityksellä on mahdollisuutena ostaa SIEM-tuote ilman erillistä palvelua, jolloin tuotteen käyttöönotto ja käyttäminen vaativat yritykseltä itseltään osaamista ja aikaa. Tämän työn puitteissa ei suoritettu erikseen maksullisten tuotteiden käytettävyyden ja asentamisen helppouden testaamista, mutta oletettavasti kaupallisten tuotteiden käyttöönotto ei olisi seuraavassa luvussa esitettäviä ilmaisratkaisuja vaativampaa etenkään, kun ongelmatilanteissa olisi mahdollista turvautua tuotteen myyjän asiakastukeen. Käytettävyyden ja ominaisuuksien osalta tuotteissa on varmasti eroja, mutta niiden tarkempi analysointi vaatisi tuotteiden samanaikaista käyttämistä ja testaamista kohdeympäristössä.

Yhtenä erillisenä esimerkkinä on valmiina ostettava ainakin osittaisia SIEM-toimintoja tekevä laite. Tällaisesta esimerkki on BitDefender Box, joka on valmiina ostettava reitittimen yhteyteen liitettävä laite verkon turvallisuuden lisäämiseen ja valvontaan. Laite

pyrkii jatkuvasti seuraamaan verkon ja siinä olevien laitteiden tilaa ja ilmoittamaan mahdollisista tietoturvapuutteista. Tuote-esittelystä ei kuitenkaan käy ilmi, kuinka hyvin laite kykenee havaitsemaan erilaisia tietomurtoja, eikä lokien keräämisestä tai hallinnasta ole mainintaa. Laitetta ei ole toistaiseksi tilattavissa Yhdysvaltojen ulkopuolelle, joten sen toimivuudesta ja käyttökelpoisuudesta pienyrityskäyttöön ei ole mahdollista tämän työn puitteissa tehdä arviota. Kun kuitenkin huomioidaan laitteen hinta, 199 dollaria, muodostaisi sellainen toimiessaan hintansa puolesta varteenotettavan mahdollisuuden pienyritykselle. [2]

Tietomurtojen selvittämiseen ja niistä toipumiseen on yrityksillä nykypäivänä mahdollista hankkia myös niin kutsuttu tietoturvavakuutus. Esimerkiksi vakuutusyhtiö If tarjoaa asiakkailleen muutaman sadan euron vuosimaksun arvoista tietoturvavakuutusta, joka kattaa hakkeroinnin, viruksen, haitallisen koodin tai palvelunestohyökkäyksen aiheuttamia kuluja ja vahinkoja. If tarjoaa vakuutuksen kautta myös asiantuntija-apua tietomurron tutkimiseen ja siitä toipumiseen. [13] Vakuutuksen ottaminen on varmasti hyvä ja kannattava ratkaisu tietomurrosta toipumiseksi erityisesti yrityksille, joilla ei ole omasta takaa vahvaa tietoteknistä osaamista järjestelmien palauttamiseen.

Kaiken kaikkiaan ostettavia ratkaisuja on markkinoilla nykypäivänä useita. Tuoteinformaation mukaan niissä luvataan ainakin suurin piirtein samoja asioita, joihin sisältyvät verkkoliikenteen valvonta, seuranta ja raportointi sekä lokitietojen kerääminen ja analysointi. Osa tietoturvayrityksistä tarjoaa palvelunsa kanssa omia teknisiä ratkaisujaan, kun taas osa hyödyntää muiden tekemiä ohjelmistoja. Hyötynä pienen yrityksen kannalta ostettavissa palvelun sisältävissä ratkaisuissa on niiden helppous. Kun tuotteen ohella ostetaan myös palvelu, on vastuu toteuttamisesta tietoturvayrityksellä, jolloin asiakasyritys voi rauhassa keskittyä omaan ydinliiketoimintaansa. Heikkoutena näissä ratkaisussa on niiden hankinta- ja ylläpitokustannukset, jotka muodostavat jatkuvan kuluerän yritykselle. Jos kuitenkaan hinta ei ole ongelma, on luotettavalta tietoturvayritykseltä ostettu tuote tai palvelu todennäköisesti yksinkertaisin, varmin, kattavin ja luotettavin ratkaisu pienyritystenkin käyttöön.

3.5 Avoimen lähdekoodin ratkaisut ja Security Onion

Erilaisia avoimen lähdekoodin IDS-ratkaisuja on nykypäivänä tarjolla useita. Esimerkeinä tunnetuimmista ovat Snort ja Suricata. Näiden lisäksi on tarjolla myös yksittäisiä ohjelmistoja laajempia ratkaisuja, joista yhtenä esimerkkinä on Linux-käyttöjärjestelmään pohjautuva Security Onion -käyttöjärjestelmä. Security Onion kokoaa yhteen useita yksittäisiä ohjelmistoja mukaan lukien edellä mainitut Snort ja Suricata kokonaisvaltaisemman IDS-järjestelmän toteuttamiseksi. Security Onionin avulla saadaan yhdellä kertaa toteutettua verkkoliikenteen pakettien kaappaus, IDS-järjestelmä ja kerättyjen tietojen analysointi [30].

Yrityksillä on toteutettavia ratkaisuja pohtiessaan mahdollista valita erikseen yksittäisiä ohjelmia ja asentaa ne käyttöönsä. Asennustoimet, seuranta ja ohjelmien väliset yhteensopivuudet tulee kuitenkin jokaisen ohjelman kohdalla toteuttaa erikseen. Security Onion sen sijaan tarjoaa yhdessä paketissa useampia tietomurtojen havaitsemiseen käytettäviä ohjelmia samassa paketissa. Kokonaisvaltaisuutensa johdosta tässä työssä on valittu tarkastelun kohteeksi nimenomaan Security Onion -järjestelmä, jota pienyritysten kannalta voidaan asentamisen ja käyttöönoton yksikertaisuuden sekä ominaisuuksien monipuolisuuden perusteella pitää yksittäisiä ohjelmia tarkoituksenmukaisempana ratkaisuna.

3.5.1 Security Onionin asennus

Ennen järjestelmän asentamista pitää sitä varten olla hankittuna sen käyttöön soveltuva laitteisto. Security Onion suositellaan asennettavaksi erilliselle fyysiselle laitteelle, jolle asetetut vaatimukset riippuvat seurattavan verkon koosta ja liikennemääristä. Vähimmäisvaatimuksina ovat 3 GB RAM-muistia, kaksi erillistä verkkoliitäntää sekä prosessoriytimiä ja kovalevytilaa liikennemäärien mukaan. Security Onion on asennettavissa joko yksittäisenä laitteena, palvelin-sensori-kokoonpanona tai näiden yhdistelmänä. Yksittäisen laitteen mallissa yksi fyysinen laite sisältää sekä palvelin- että sensoritoiminnot. Palvelin-sensori-mallissa palvelin on oma laitteensa, jolle sensorit sitten välittävät tiedot tekemistään havainnoista. Valittu asennustapa heijastaa minkälaisia vaatimuksia käytettävillä laitteilla tulee olemaan. [30]

Security Onion tulee asentaa verkkoon siten, että se kykenee seuraamaan kaikkea seurattavaksi ajateltua liikennettä. Tähän vaihtoehtoina ovat esimerkiksi halutun liikenteen ohjaaminen kulkemaan Security Onionin läpi tai halutun liikenteen reitittäminen tarkoitetun määränpään lisäksi myös Security Onion laitteelle. Näistä jälkimmäinen vaihtoehto edellyttää, että verkkolaitteiden avulla liikenteen niin sanottu peilaaminen voidaan tehdä. Käytännössä tämä voi tarkoittaa sitä, että yritys joutuu uudistamaan oman reitittimensä.

Y-malli Oy:n kaltaisen yrityksen tapauksessa kaikki sisäverkon liikenne kulkee verkon reitittimen kautta, joten ratkaisuksi voidaan valita kaiken sisäverkon liikenteen peilaaminen kulkemaan varsinaisen määränpään lisäksi reitittimeen yhdistetylle Security Onion laitteelle. Tällöin kuitenkin tulee eteen mahdollisesti reitittimen uudistaminen, mikäli nykyisessä reitittimessä tätä ominaisuutta ei ole. Lokien seurannan osalta verkon eri laitteet tulee lisäksi asentaa välittämään tarvittavat lokitiedot esimerkiksi laitteille kirjautumisista Security Onionille.

Kun Security Onionia varten on olemassa sitä varten varattu laite ja verkon rakenne ja laitteet mahdollistavat liikenteen ja lokitietojen seurannan, voidaan aloittaa varsinaisen järjestelmän asentaminen. Security Onion asennetaan sitä varten varatulle tietokoneelle muiden käyttöjärjestelmien tavoin lataamalla ensin ISO-tiedosto ja ajamalla sen asennusohjelma. [30]

Käyttöjärjestelmän asennuksen jälkeen saadaan varsinaiset IDS-ohjelmat asennettua työpöydällä olevan asennusohjelman pikakuvakkeen kautta. Asennusohjelma auttaa käyttäjää asettamaan ohjatusti yrityksen verkkoa vastaavat verkkoasetukset. Niiden jälkeen käyttäjältä muun muassa kysytään, asennetaanko Security Onion yksittäisenä laitteena vai palvelin-sensori-laitteena, käytetäänkö IDS-järjestelmänä Snortia vai Suricataa ja käytetäänkö asennuksessa oletusasetuksia vai haluaako käyttäjä muokata näitä itse. Lopuksi käyttäjä ohjataan luomaan käyttäjätunnukset Squil, ELSA ja Squert analyysiohjelmistoja varten. Tarkemmat ohjeet asennuksen suorittamiseksi löytyvät Security Onionin omasta Wikistä. [30]

3.5.2 Security Onionin käyttö

Asentamisen ja käyttöönoton jälkeen seuraa itse järjestelmän käyttö. Käyttövaiheessa eri havaitsemisohjelmien tarkoituksena on hälyttää aina havaitessaan tietoturvan kannalta uhkaavia tapahtumia. Hälytysperusteiden ja kerättävän tiedon laadun säätäminen kohdalleen on yksi käyttöön liittyvistä merkittävistä toimista, joka ottaa oman aikansa. Käytännössä sopivien hälytysasetusten löytäminen saattaa kestää viikkoja. Tavoitetilana on, että järjestelmä antaisi mahdollisimman vähän erilaisia vääriä hälytyksiä.

Security Onionin eri ohjelmat keräävät ja osiltaan muokkaavat tietoa käyttäjän käsittelyä varten. Kerätyn tiedon analysointia varten Security Onion tarjoaa muun muassa selaimen kautta käytettävän portaalin, jonka avulla käyttäjän on mahdollista hakea ja käsitellä eri ohjelmien keräämiä tietoja ja antamia hälytyksiä. Hälytyksistä on lisäksi mahdollista saada tieto määrättyyn sähköpostiin, jolloin niihin reagoiminen todennäköisesti nopeutuu.

Järjestelmän toimintaa tulee myös testata hyökkäyksien varalta toteuttamalla näitä itse sisäverkossa ja varmistaa, että ne tulevat havaituksi. Testattavat hyökkäyksien tulisi olla mahdollisimman todenmukaisia ja mallintaa niitä uhkia, jotka todennäköisimmin yritykseen kohdistuvat. Testausta varten on olemassa myös testausautomaatteja, kuten testmyids.com, johon yhdistämällä on mahdollista todeta ainakin Security Onionin oletusasetusten toimivuus [30].

Lokien hallintaa varten Security Onion tarjoaa OSSEC-ohjelmiston, joka mahdollistaa lokien keräämisen ja siirron verkon eri laitteilta palvelimelle analysointia varten. OSSEC varmistaa lokien hallintaan liittyen myös tiedostojen eheyden valvonnan seuraamalla säännöllisesti tiedostoista laskettuja MD5/SHA1-tarkistussummia. Niiden perusteella OSSEC kykenee antamaan hälytyksen aina odottamattomista muutoksissa tiedostoissa. Tiedostoissa tapahtuneiden muutosten lisäksi OSSEC saadaan antamaan ilmoituksia tiettyjen kiellettyjen sovellusten käytöstä ja piilohallintaohjelmistojen (engl. rootkit) käytöstä [3, s. 150–170]. Näin toteutettu eheyden varmistaminen on erittäin keskeistä tietomurtojen selvittämiseen tarvittavan todistusaineiston eheyden ja luotettavuuden kannalta.

Lokienhallinnan lisäksi OSSEC-ohjelmiston avulla on mahdollista toteuttaa myös automatisoituja aktiivisia vastatoimia tietomurtojen rajaamiseksi, vahinkojen minimoimiseksi ja selvittämisen helpottamiseksi. OSSEC mahdollistaa määrättyjen sääntöjen perusteella muun muassa käyttäjätilien sulkemisen, IP-osoitteiden kieltämisen, palomuurin sulkemisen ja sähköposti-ilmoituksen lähettämisen. [3, s. 176–184]

Kaiken kaikkiaan Security Onionin käyttöönotto on varsin suoraviivainen prosessi ja hyvin mahdollista myös pienyritysten käyttöön. Haasteena kuitenkin tulee olemaan kaikkien sen sisältämien ohjelmien ja toiminnallisuuksien muokkaaminen yrityksen käyttöön optimaaliseksi, mikä saattaa vaatia merkittävästi aikaa etenkin, jos asiaan liittyen ei ole aiempaa asiantuntemusta. Joka tapauksissa Security Onionin kaltainen järjestelmä antaa varteenotettavan vaihtoehdon tietomurtojen havaitsemiseen yrityksille, joilla ei ole halua tai mahdollisuutta sijoittaa kaupalliseen ratkaisuun mutta joilla on mahdollista sijoittaa jonkin verran aikaa ratkaisun toteuttamiseen.

3.6 Lainsäädännön vaikutukset

Tietomurtojen havaitsemiseen keskittyvissä ratkaisuissa edellytetään käytännössä aina ainakin jonkinasteista verkon ja laitteiden valvontaa, jolloin yksi keskeisimmistä huomioitavista laeista on vuoden 2015 alussa voimaan tullut tietoyhteiskuntakaari. Tietoyhteiskuntakaaren 17 luvussa [33] säädetään sähköisten viestien ja välitystietojen käsittelystä ja 18 luvussa annetaan yhteisötilaajaa koskevia erityissäännöksiä.

Se, miltä osin tietoyhteiskuntakaaren säädöksiä sovelletaan, riippuu hyvin pitkälti siitä, miten yrityksen viestintäverkko on toteutettu ja miten tietoa siellä siirretään. Tietosuojakaarta koskevan hallituksen esityksen HE 221/2013 [11, s. 95] mukaan yritys katsotaan yhteisötilaajaksi, kun se on tilannut viestintäpalvelun tai lisäarvopalvelun työntekijöidensä käyttöön.

Viestintäpalvelulla tarkoitetaan tässä yhteydessä muun muassa sähköpostipalvelua ja internetyhteyspalvelua. Internetyhteyspalvelulla tarkoitetaan taas palvelua, jonka avulla on mahdollisuus muodostaa yhteys internetiin ja käyttää siellä olevia palveluja, eli esimerkiksi yrityksen työntekijöilleen tarjoamaa internet-yhteyttä. Se on kuitenkin rajattu koskemaan ainoastaan sitä osaa yhteydestä, jota teleyritys kykenee hallinnoimaan. [11, s. 85–95] Täten yrityksen oma sisäverkko ei kuuluisi internetyhteyspalvelun piiriin.

Tietoyhteiskuntakaaren 17 luvussa [33] säädetään useita rajoituksia liittyen sähköisten viestien kuten sähköpostien käsittelyyn. Näistä huolimatta lain 272 § antaa yhteisötilaajalle eli siten myös yritykselle oikeuden ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi. Näihin toimiin lasketaan muun muassa viestin sisällön automaattisen selvittäminen, välittämisen ja vastaanottamisen automaattinen estäminen tai rajoittaminen sekä tietoturvaa vaarantavien haitallisten ohjelmien automaattinen poistaminen viestistä. Ky-

seinen pykälä mahdollistaa siten yrityksen verkkoon saapuvan sähköpostiliikenteen tarkastamisen automaattisesti haittaohjelmien torjumiseksi ja niiden poistamiseksi. Huomioitavaa on automatiikan merkitys käsittelyssä, sillä mikäli viestiä joudutaan käsittelemään manuaalisesti, tulee tästä ilmoittaa viestin lähettäjälle ja vastaanottajalle.

Tietoyhteiskuntakaaren 18 luvussa [33] säädetään yhteisötilaajia koskevista oikeuksista ja velvollisuuksista. Lain 146 § antaa yritykselle oikeuden käsitellä viestien välitystietoja eli viestin välittämiseksi tarvittavaa ja johonkin tiettyyn oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, kuten lähde- tai kohdekoneen yksilöiviä osoitetietoja. Lain seuraavassa eli 147 §:ssä säädetään, että ennen välitystietojen käsittelyn aloittamista tulee yrityksen suojata oma verkkonsa ulkopuolisilta. Tähän sisältyvät muun muassa palomuurien asettaminen ja niiden asetusten muokkaaminen sekä langattomien verkkojen suojaus. Tämän lisäksi yrityksen sisäverkon luvattoman käytön torjumiseksi yrityksen tulee määritellä, mitä viestejä verkossa saa välittää, hakea ja mihin niitä saa lähettää sekä miten verkkoa muutoin saa käyttää. Vastaavasti yrityssalaisuuksien torjumiseksi yrityksen tulee määritellä, mitä yrityssalaisuuksiksi laskettavia tietoja verkossa saa siirtää, luovuttaa tai käsitellä sekä mihin kohdeosoitteisiin tietoja ei saa siirtää.

Edellisten lisäksi ennen verkon valvonnan aloittamista yrityksen tulee huomioida myös tietoyhteiskuntakaaren 148 §, jonka mukaan yrityksen on määriteltävät ne henkilöt, jotka saavat käsitellä valvonnassa seurattavia ja kerättäviä tietoja, sekä 154 §, jossa säädetään ennakkoilmoituksen tekemisestä tietosuojavaltuutetulle ennen välitystietojen käsittelyn aloittamista. Näiden lisäksi yrityksen tulee määritellä valvonnassa käytettävien menettelyjen perusteet ja käytännöt. [33] Koska tässä työssä keskitytään ainoastaan pieniin korkeintaan noin 10 hengen yrityksiin, riittää tiedottaminen henkilöstölle valvonnan tarkoituksesta, käyttöönotosta, menetelmistä sekä tietoverkon ja sähköpostin käytöstä sekä heidän kuulemisensa näistä asioista. Suuremmissa yrityksissä asia pitää käsitellä yhteistoimintamenettelyssä. [20]

Kun laissa mainitut ennakkovaatimukset on täytetty, tulee huomioitavaksi itse toteutukseen liittyvät säädökset. Viestintään liittyvien välitystietojen käsittelyssä yrityksellä on oikeus hyödyntää automaattista hakutoimintoa, joka voi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin. Kun automaattinen hakutoiminto havaitsee viestinnässä poikkeaman tai verkossa sinne kuulumattoman laitteen taikka yksittäistapauksessa muusta näihin rinnastettavasta seikasta voidaan päätellä verkkoa käytettävän luvattomasti, voidaan välitystietoja käsitellä manuaalisesti, jos on lisäksi perusteltu syy epäillä verkon luvatonta käyttöä. Vastaava mahdollisuus manuaaliseen käsittelyyn on, jos yrityssalaisuus julkaistaan, sitä käytetään hyväksi tai yrityssalaisuus on luvattomasti annettu ulkopuoliselle ja jos on perusteltu syy epäillä, että viestintäverkkoa on luvattomasti käytetty yrityssalaisuuden luovuttamiseen ulkopuoliselle. Manuaalisesta käsittelystä on laadittava tietoyhteiskuntakaaren 152 §:n mukainen

kirjallinen selvitys. Manuaalisista käsittelyistä on lisäksi vuosittain selvitys työntekijöiden edustajalle tai pienten yritysten tapauksessa usein koko henkilöstölle sekä tietosuojavaltuutetulle. [33]

Mikäli verkon valvonnassa havaitaan esimerkiksi tietomurto ja tapauksesta ilmoitetaan poliisille, antaa tietoyhteiskuntakaaren 157 § yritykselle oikeuden luovuttaa tekoon liittyvät sähköisiä viestejä koskevat välitystiedot poliisille esitutkintaa varten. Muilta osin kerättyjen tietojen osalta tulee huomioida säilyttämistä koskevat määräykset. Tietoyhteiskuntakaaren 145 §:n mukaisesti välitystietojen käsittelyyn liittyvät tapahtumatiedot on säilytettävä tietojärjestelmässä kaksi vuotta niiden tallentamisesta. [33]

Kun pohditaan erilaisia tietomurtojen havaitsemiseen keskittyviä järjestelmiä, tulisi välitystietojen ja verkkoliikenteen tarkkailun lisäksi kyseeseen muun muassa lokitietojen kerääminen eri laitteiden ja tietojärjestelmien käytöstä. Koska tällöin tietoihin tallentuisi tietoja muun muassa käyttäjätunnuksista ja IP-osoitteista, muodostuu tiedoista laissa määritetty henkilörekisteri, jolloin sovellettavaksi tulevat henkilötietolain säädökset. Lisäksi jatkossa tulevat huomioitavaksi myös EU:n uuden tietosuoja-asetuksen säädökset.

Henkilötietolain 8 §:ssä säädetään henkilötietojen käsittelyn perusteista ja pykälässä annetaan muun muassa työnantajalle oikeus käsitellä työntekijöidensä henkilötietoja. Työnantajan on laadittava rekisteristä henkilötietolain 10 §:n mukainen rekisteriseloste, joka pitää olla jokaisen saatavilla. Käytännössä siis lokien keräämisestä pitää laatia ilmoitus, joka on jollain tavalla kaikkien työntekijöiden saatavilla. Lokien säilyttämisen ja tallentamisen osalta tulee vielä huomioitavaksi lain 22 §, jonka mukaan tietojen siirtäminen EU:n tai ETA:n ulkopuolelle on sallittua ainoastaan, jos kyseisessä maassa voidaan taata riittävä tietoturvan taso. Tämä tulee erityisesti huomioitavaksi, mikäli pohditaan lokitietojen tallentamista jonkin ulkopuolisen yrityksen tarjoamaan pilvipalveluun. Tähän on kuitenkin säädetty joitakin poikkeuksia, joista rekisteröidyn yksiselitteinen suostumus on yksi. Täten jos esimerkiksi kaikki yrityksen työntekijät suostuvat lokitietojen varmuuskopiointiin pilvipalveluun, voidaan tietoja suostumusperusteisesti sinne siirtää. [12]

4. TARKOITUKSENMUKAISET TIETOTURVA-RATKAISUT PIENYRITYKSILLE

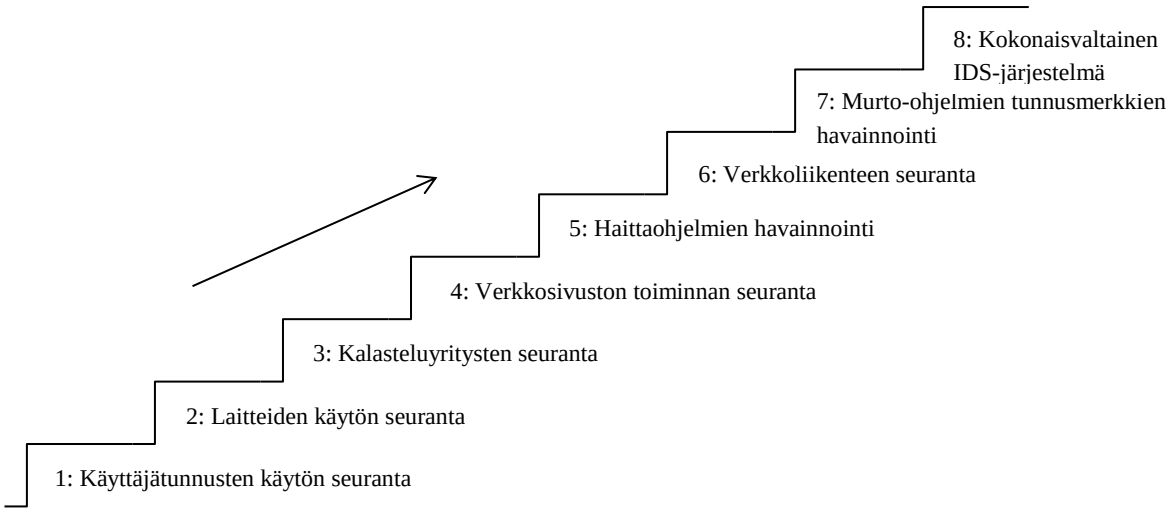
Pienillä yrityksillä on usein hyvin rajalliset resurssit sekä taloudellisesti että ajallisesti tietoturvaratkaisujen toteuttamisen, mikäli nämä eivät suoraan ole yrityksen ydinliiketoimintaa. Tämän johdosta näille yrityksille on olennaista, että resurssien käytössä keskitytään tärkeimpiin ja olennaisimpiin seikkoihin eli toteutetaan mahdollisimman tarkoituksenmukaisia ratkaisuja.

Tähän mennessä on luvussa kaksi tuotu esille erilaisia tapoja, joilla tietomurtoja tehdään, sekä esitelty eri tekotapojen yleisyyttä. Luvussa 3 sen sijaan on käsitelty tietomurtojen havaitsemista ja siihen käytettävissä olevia ratkaisuja pienten yritysten näkökulmasta. Seuraavaksi tarkoituksena on pohtia näiden tähän mennessä kerättyjen ja esitettyjen tietojen perusteella, mitkä erilaisista ratkaisuista olisivat tarkoituksenmukaisimpia pienten yritysten kannalta, kun otetaan huomioon erilaisten tekotapojen yleisyys.

4.1 Tietomurtojen havaitseminen

Puhuttaessa kyvystä havaita ja selvittää tietomurtoja on keskeistä, että havaituksi tulisivat ainakin yleisimmät ja siten siis todennäköisimmät tietomurtojen tekotavat. Se, kuinka monimutkaisten ja harvinaisten tekotapojen havaitsemiseen pyritään, tulee hyvin pitkälti riippumaan käytettävissä olevista resursseista. Toki tähän voivat vaikuttavat myös muun muassa asenteet ja riskianalyysin tulokset, mutta kuten alaluvussa 3.2 tuotiin esille, on nykypäivänä olemassa jo säädöksiä, jotka sanktioiden uhalla edellyttävät tiettyjä muun muassa tietomurtojen havaitsemiseen liittyviä toimintoja.

Luvussa kaksi esiteltiin tietomurtojen yleisimpiä tekotapoja. Pohdittaessa niiden havaitsemiseen keskittyviä ratkaisuja voidaan tekotavat muodostaa seuraavalla sivulla olevan kuvan 5 mukaisesti tietomurron tekotapojen portaikoksi. Tietomurtojen havaitsemisratkaisut on jaettu kahdeksaan portaaseen siten, että alimmilla portailla toteutettavilla ratkaisuilla pyritään havaitsemaan taulukossa 1 esitetyt yleisimmät tekotavat ja ylimmillä portailla harvinaisemmat tekotavat. Huomionarvoista tässä kohtaa on, että ratkaisujen toteuttamisjärjestys on valittu puhtaasti tekotapojen yleisyyden mukaan eikä esimerkiksi ratkaisujen toteuttamisen helppouden tai yksikertaisuuden perusteella, mikä usein on lähtökohtana. Ratkaisujen toteuttamisessa saatetaan helposti sortua siihen, että tehdään sitä, mikä on helppoa, sujuvaa tai hienoa, eikä keskitytä siihen, mitä todellisuudessa tarvitaan. Jos esimerkiksi yritys keskittyisi kuvan 5 portaikon portaiden 4-8 ratkaisuihin ja unohtaisi portaat 1-3, jäävät selkeästi yleisimmät tekotavat kokonaan huomioimatta ja siten toteutuessaan myös todennäköisesti havaitsematta.



Kuva 5. *Tietomurtojen yleisimpien tekotapojen havaitsemisratkaisut suositellussa toteuttamisjärjestyksessä*

Portaikon ajatuksena siis on, että ensin olisi pyrittävä havaitsemaan ensimmäisen portaan eli kaikista yleisimmät tekotavat ja sen jälkeen pyrkiä ottamaan huomioon myös muut tekotavat käytettävissä olevien resurssien ja ajan mukaisesti. Yritys voisi täten jo alussa tehdä päätöksen, mille portaalle toteutettavilla ratkaisuilla pyritään nousemaan, tai aloittaa ensimmäisestä portaasta ja sen saavuttamisesta, minkä jälkeen yritys voisi nousta ajan kanssa portaikkoa askel kerrallaan. Kummassakin tapauksessa on tärkeää, että portaikossa kiipeäminen olisi jatkuva prosessi ja että tavoitteena olisi päästä portaikossa mahdollisimman ylös. Toisin sanoen kun tietty porras on saavutettu, tulisi saman tien alkaa suunnitella, miten seuraava porras voitaisiin saavuttaa. Toki portaikossa on mahdollista myös pudota alaspäin, jos toteutettujen ratkaisujen annetaan vanheta eikä esimerkiksi tietomurtojen tekotavoissa tapahtuvaa kehitystä seurata eikä niissä tapahtuviin muutoksiin reagoida. Portaikon ylimmällä portaalla oleva kokonaisvaltainen IDS-järjestelmä yhdistää kaikki alempien portaiden kokonaisuudet ja sen toteuttamisessa kiinnitetään erityisesti huomioita alempien portaiden ratkaisujen saumattomaan yhteistoimintaan.

Lisäksi on erittäin tärkeää ymmärtää, ettei portaikon järjestyksen noudattamisesta saisi myöskään tulla itse tarkoitus. Esimerkiksi jos yrityksen resurssit eivät tähän hätään riittäisi portaan 2 ratkaisujen toteuttamiseen, mutta riittäisivät portaiden 4-6 toteuttamiseen, ei portaikon järjestykseen vetoaminen ja portaiden 4-6 toteuttamatta jättäminen olisi tarkoituksenmukaista. Yritykselle on luonnollisesti järkevää toteuttaa ratkaisut 4-6, mutta niiden toteuttaminen ei saisi aiheuttaa toteuttamatta olevien portaiden 2 ja 3 unohtamista, vaan niiden toteuttamista varten olisi syytä alkaa suunnitella, kerätä ja varata resursseja.

Tässä työssä keskitytään tietomurtojen havaitsemiseen liittyviin ratkaisuihin. On kuitenkin syytä huomata, että vastaavaa portaikkoajattelua voitaisiin hyödyntää yhtä lailla myös

tietojärjestelmän suojauksia suunniteltaessa ja toteutettaessa. Tällöin lähtökohtana toteuttavissa ratkaisuissa olisi yleisimpien tekotapojen torjuminen ja myöhemmin sitten harvinaisemmilta tekotavoilta suojautuminen. Todellisuudessa näitä molempia on hyvä toteuttaa yhdessä, sillä esimerkiksi tilanteissa, joissa tietyn tekotavan havaitsemiseen keskittyvän ratkaisun toteuttaminen osoittautuu haastavaksi tai vaikeaksi, voidaan tietomurron riskiä kyetä poistamaan ja havaitsemista helpottamaan parantamalla kyseisen tekotavan torjumiseen keskittyviä mekanismeja.

Varsinaisten havaitsemisratkaisujen pohdinnassa joudutaan luonnollisesti ottamaan huomioon käytettävissä olevat resurssit sekä lakien, asetusten ja muiden säädösten aiheuttamat edellytykset ja rajoitukset. Käytännössä tietoturvatoimenpiteitä saa suorittaa yrityksen omissa tietojärjestelmissä melko vapaasti, kunhan ei käsitellä henkilötietoja, tunnistamistietoja, paikkatietoja tai muita vastaavia tietoja, joista yksittäinen henkilö olisi tunnistettavissa ja yksilöitävissä [19, s. 185]. Jos tällaisia tietoja käsitellään, pitää huomioida niiden käsittelyä säätelevä lainsäädäntö, jota käytiin läpi alaluvussa 3.6.

Se, minkälaisia ratkaisuja kunkin portaan saavuttamiseksi konkreettisesti toteutetaan, riippuu pitkälti yrityksestä ja sen rakenteesta. Seuraavassa on pohdittu ratkaisuvaihtoehtoja esimerkkiyritys Y-malli Oy:n näkökulmasta sekä annettu esimerkkeinä mahdollisia ratkaisuja kunkin tekotavan havainnointiin.

4.1.1 Käyttäjätunnusten käytön seuranta

Käyttäjätunnusten käytön osalta on hyvä muistaa, että suurin osa tietomurroista on tehty voimassa olevilla käyttäjätunnuksilla, jotka on pääsääntöisesti saatu haltuun muutoin kuin teknisin keinoin. Tämä tarkoittaa sitä, että epäonnistuneiden kirjausten seuraaminen antaa tähän kategoriaan melko vähän. Tässä yhteydessä käyttäjätunnusten käyttö liittyy niillä kirjautumiseen tiettyyn tietojärjestelmään. Tietomurron havaitseminen edellyttää täten tietojärjestelmässä siihen tehtyjen kirjautumisten seuraamista. Tätä varten tulisi kaikissa tietojärjestelmissä olla kirjautumisloki, jota sitten pyritään analysoimaan väärinkäytösten varalta.

Väärinkäytösten havaitsemiseksi järjestelmään olisi syytä toteuttaa lokiratkaisu, jossa kerätään tiedot ainakin kirjautumiseen käytetyistä käyttäjätileistä, kirjautumisajankohdista ja kestoista. Poikkeavan käyttäytymisen havaitsemiseksi tulisi lokitietoja kerätä myös käyttäjän toimenpiteistä järjestelmästä ja etsiä niistä poikkeavia toimia. Lokiratkaisussa on tärkeää huomata, että kerätään riittävästi tietoa, muttei sellaista määrää, että seuranta ja analysointi tulevat mahdottomaksi. Kerääntyvän tiedon määrän rajoittamiseksi ja havaitsemisen helpottamiseksi voidaan hyödyntää erilaisia tietojärjestelmän tietoturvaa parantavia ratkaisuja. Jos esimerkiksi saadaan lailliset kirjautumiset rajattua ainoastaan tiettyihin laitteisiin ja IP-osoitteisiin, on helpompi todeta muilta laitteilta tai osoitteista tehdyt kirjaukset laittomiksi.

Y-malli Oy:n tapauksessa todettiin, että lokitietojen kerääminen ja seuranta ei ole toteutettavuutensa ja toimivuutensa puolesta tarkoituksenmukainen ratkaisu. Sen sijaan yrityksessä tehtiin päätös ottaa käyttöön kahden tekijän varmennus työasemille kirjautumiseen. Täten onnistunut kirjautuminen edellyttää voimassaolevien käyttäjätunnusten lisäksi erillisen fyysisen autentikointiavaimen käyttöä. Kahden tekijän varmennuksen johdosta lokiratkaisulle todettiin riittäväksi, että seurataan ainoastaan epäonnistuneita kirjautumisia. Autentikointiavaimen käytön osalta ohjeistettiin sen säilyttäminen koko ajan mukana tai muuten turvallisessa paikassa sekä ilmoittamaan ensi tilassa sen mahdollisesta katoamisesta. Voimassaolevia tunnuksia käyttäen tehty havaitsematta jäävä väärinkäyttö edellyttää siten sen, että hyökkääjä saa tietoonsa käyttäjätunnuksen ja siihen liittyvän salasanan sekä fyysisen autentikointiavaimen, minkä riski arviointiin sen verran alhaiseksi, että se voitiin hyväksyä.

Muiden laitteiden kuin työasemien osalta toteutettiin niille lokiratkaisu, jossa kerätään tietoja muun muassa epäonnistuneista kirjautumisista. Tämän lisäksi asetettiin, että niihin sallitaan yhteydet ainoastaan määrätyistä työasemista. Muilta laitteilta yritettävät epäonnistuneet yhteydenotot tallennetaan lokitietoihin.

4.1.2 Laitteiden käytön seuranta

Laitteiden käytön seuranta liittyy läheisesti käyttäjätunnusten käytön seurantaan, minkä johdosta näihin liittyvät ratkaisut ovat osiltaan samoja. Seurannan mahdollistamiseksi pitää ensinnäkin suojata käytettävät laitteet ulkopuolisten pääsyä vastaan. Tämän jälkeen laitteille tulisi luoda ratkaisu, jolla kyetään seuraamaan yrityksiä suojausten kiertämiseksi tai murtamiseksi. Ongelmaksi tällöin muodostuu edelleen laillisten käyttäjätunnusten väärinkäyttö, mitä käsiteltiin edellisissä kappaleissa. Näiden havaitsemiseksi yksinkertaisimpia ratkaisuja olisi ohjeistaa ja velvoittaa käyttäjä seuraamaan omia kirjautumisiaan väärinkäytösten havaitsemiseksi. Monimutkaisempiin ratkaisuihin sen sijaan kuuluu poikkeavuuksien hakeminen käyttäjien käyttäytymisessä, mikä mahdollisesti viittaisi siihen, että käyttäjätunnuksia käyttää joku muu. Esimerkki tällaisesta poikkeavuudesta voisi olla käyttäjätunnusten käyttö työajan ulkopuolella.

Laitteiden käytön seurantaan liittyvät myös kaikkien yrityksen tiloihin sekä tietoverkkoon liittyvien sisään- ja ulostulokohtien kartoittaminen ja tarkastaminen. Kaikki yrityksen laitteisto on hyvä käydä säännöllisesti läpi mahdollisesti asennettujen luvattomien lisälaitteiden varalta. [1, s. 257] Tähän samaan yhteyteen sisältyy lisäksi tietoturvallisten toimintatapojen noudattaminen erilaisten siirrettävien tallennusmedioiden kohdalla. On esimerkiksi tärkeää, ettei tuntemattomista lähteistä olevia tallennusmedioita liitetä noin vain yrityksen järjestelmiin ja ettei omia tallennusmedioita käsitellä huolimattomasti tai varomattomasti.

Käytännössä käyttäjätunnusten ja laitteiden väärinkäytön tunnistamiseen voidaan hyödyntää useampia eri tekijöitä. Yksi on tilastovertailu muun muassa sovellusten käyttömääristä, käytettyjen resurssien laadussa, käytössä olevista prosesseista ja niiden käyttäjistä. Toisena on käyttäjien käyttäytymisen seuranta, mihin sisältyvät esimerkiksi sisään- ja uloskirjautumistiedot, käyttöoikeuksien muutokset, epäonnistuneet yritykset salattujen tiedostojen näkemiseksi tai suojattuihin verkon osiin siirtymiseksi sekä resurssien käyttö. Käyttäjätunnusten väärinkäyttö saattaa ilmetä toistuvina epäonnistuneina kirjautumisina, kirjautumisina epätavallisista paikoista tai laitteista, epätavallisten prosessien tai tiedostojen käyttönä tai epätavallisena pituisina kirjautumisaikoina. [1, s. 247–248] Kolmas vaihtoehto on tiedostojen käytön ja eheyden seuranta, jonka avulla pyritään havaitsemaan erilaisia odottamattomia muutoksia, luonteja ja poistoja tiedostoissa sekä niiden asetuksissa ja käyttöoikeuksissa. Erityisesti erilaisten asetus-, salasana-, suodatus- ja suojaustiedostojen muutokset on tärkeää huomioida. [1, s. 251–254]

Yksi laitteiden käyttöön liittyvä nykypäivänä yleistynyt ilmiö on omien laitteiden tuominen työpaikalle ja niiden käyttäminen tiedon käsittelyyn, tallentamiseen ja siirtämiseen. Nämä laitteet aiheuttavat myös omanlaisensa haasteen kaikenlaisten tietoon kohdistuvien hyökkäysten havainnoinnille. Koska tällaisten laitteiden käytön seuranta osoittautuu helposti kovin haastavaksi, ongelman ehkäisemiseksi olisikin yrityksessä tärkeää sopia pelisäännöistä omien ja ulkopuolelta tuotujen laitteiden käytön ja tiedon käsittelyn osalta. [23, s. 106–107] Luvattomien laitteiden havaitsemiseksi tulee kaikki verkon osat käydä läpi aktiivisesti etsimällä. Etsinnässä tulisi päivittäin tarkastaa verkkoon liittyneet MAC- ja IP-osoitteet sekä uudet ja odottamattomat verkkoportit kytkimissä. Myös mahdollisesti puuttuvat laitteet on syytä huomioida. [1, s. 256]

Tietomurtojen yritysten ehkäisemisen ja havaitsemisen yksinkertaistamisen kannalta olisi yrityksen tietoverkon ja -järjestelmien käyttö syytä rajata mahdolliseksi vain tietyiltä ennalta määrätyiltä yrityksen omilta laitteilta. Tunkeutumisyritysten havaitsemisen kannalta olisi sitten hyvä toteuttaa ratkaisu, jolla havaitaan verkkoon liittymistä ja tietojärjestelmään kirjautumista yrittävä sallitun listan ulkopuolella oleva laite.

Y-malli Oy:n tapauksessa edellisessä alaluvussa mainittu kahden tekijän varmennus ja työasemissa ja muissa laitteissa käyttöönotettu lokiratkaisu huolehtii myös osiltaan luvattoman fyysisen pääsyn havaitsemisesta. Tämän lisäksi kulunvalvontaan ja fyysisten laitteiden tarkastamiseksi luotiin tarkastuslista ja sovittiin säännöllinen aikaväli sen läpikäymiseksi ja menetelmä mahdollisten havaittujen poikkeamien raportoimiseksi.

4.1.3 Kalasteluyritysten seuranta

Kalasteluyrityksiin voidaan olettaa sisältyvän jonkinlainen viestintä hyökkääjän ja uhrin välillä. Valtaosa kalasteluyrityksistä tapahtuu sähköpostin välityksellä, mikä tarkoittaa sitä, että havaitsemisen tulisi perustua saapuvien sähköpostien analysointiin [25]. Koska täydellisen ja varmuudella kaikki kalasteluyritykset tunnistavaa analysointiohjelmaa on

käytännössä mahdotonta toteuttaa, on yrityksen henkilöstölle syytä kouluttaa ja ohjeistaa kalasteluyritysten havaitsemista ja tunnistamista sekä erityisesti korostaa niistä ilmoittamista. Myös hyvin määritetyt tietoturvapolitiikat auttavat tässä kohtaa.

Esimerkkinä jälleen Y-malli Oy:n henkilöstön kanssa sovittiin menettelytavoista kalasteluyritysten havaitsemiseksi. Lisäksi tarkennettiin niin sanotut pelisäännöt sähköpostien lukemiseen ja niiden käsittelyyn. Lisäksi annettiin yrityksen myyntipäällikölle tehtäväksi säännöllisesti seurata muun muassa viestintäviraston tiedotteita uusien havaittujen kalasteluhyökkäysten tietoon saamiseksi.

4.1.4 Verkkosivuston toiminnan seuranta

Verkkosivustoa voidaan hyvin pitkälle kohdella kuten mitä tahansa muutakin tietojärjestelmää, joten edellä mainitut työasemia ja muita laitteita koskevat ratkaisut tulevat käytettäviksi myös WWW-palvelimelle. Verkkosivuston toiminnan seuraamiseksi ensinnäkin pitää kerätä lokitietoja verkkosivuston sisällön hallintaan ja ylläpitoon liittyvästä käytöstä.

Käyttäjätietojen lisäksi myös verkkosivuston toimintaa tulisi pyrkiä seuraamaan haittaohjelmien ja muun mahdollisen verkkosivustolle kuulumattoman toiminnan havaitsemiseksi. WWW-palvelimella olisi siten hyvä olla ajan tasalla oleva palomuuri ja virus-/haittaohjelmatorjunta. Erityisesti ohjelmiston ajantasaisuus on keskeisessä roolissa tietomurtojen ennaltaehkäisyssä ja siten havaitsemisjärjestelmien toimivuuden tehostamisessa, sillä merkittävä osa verkkosivustoille tunkeutumisista onnistuu verkkosivustoilla olevien päivittämättömissä ohjelmistoissa olevien haavoittuvuuksien kautta [25].

Y-malli Oy:n tapauksessa verkkosivuston ylläpito on ulkoistettu WWW-palvelimen tarjoavalle yritykselle. Täten myös väärinkäytösten havaitsemisen vastuu on sopimusperusteisesti siirtynyt heille. Y-malli Oy:n myyntipäällikön vastuulla on lisäksi sivuston sisällön päivittäinen seuraaminen sen oikeellisuuden osalta. Tällainen malli on monessakin mielessä pienelle yritykselle käyttökelpoinen ratkaisu, sillä ylläpidon ulkoistamisesta aiheutuvat kustannukset ovat nykypäivänä pienet ja sen mukanaan tuomat helpotukset ovat huomattavat. Palveluntuottajaa valittaessa on kuitenkin syytä kiinnittää huomiota palvelun luotettavuuteen ja turvallisuuteen.

4.1.5 Haittaohjelmien havainnointi

Haittaohjelmien havainnointia varten on olemassa sekä ilmaisia että maksullisia valmisohjelmia. Näiden ohjelmien osalta haittaohjelmien havaitsemiskyvyn tehokkuuden osalta on tärkeää, että ne pidetään koko ajan päivitettyinä viimeisimpiin versioihinsa. Mahdolliset havainnot haittaohjelmista tulee kerätä talteen tapauksen selvittämistä varten. Löydetyn haittaohjelman osalta olisi tärkeää kyetä selvittämään, miten se on päässyt järjestelmään vastaavien tapauksien ehkäisemiseksi tulevaisuudessa.

Y-malli Oy:ssä oli jo ennen tämän työn aloittamista asennettu kaikille tietokoneille asennettu F-Securen SAFE virus- ja haittatorjuntaohjelmisto. Kyseinen ohjelmisto seuraa reaaliajassa järjestelmien tilaa ja ilmoittaa käyttäjälle saman tien mahdollisista haittaohjelma havainnoista ja aloittaa alustavat toimet sen toiminnan rajoittamiseksi.

Yleisestikin haittaohjelmien torjuntaan soveltuvien ohjelmistojen edullisuus, tehokkuus ja helppokäyttöisyys tekevät niistä hyvin tarkoituksenmukaisen ratkaisun haittaohjelmien havainnointiin. Haittaohjelmia on mahdollista havaita verkkoliikennettä seuraamalla, mutta tämän toiminnallisuuden toteuttaminen tuo samalla käytännössä mukanaan myös seuraavan portaan eli verkkoliikenteen seurannan toteuttamisen. Tällä portaalle tarkoituksenmukaiseksi ratkaisuksi on siten katsottu laitekohtaisesti asennettavien haittaohjelmien torjuntaan keskittyvien ohjelmistojen käyttäminen.

4.1.6 Verkkoliikenne, murto-ohjelmat ja IDS-järjestelmä

Portaikon kolme ylintä porrasta verkkoliikenteen seuranta, murto-ohjelmien tunnusmerkkien havainnointi ja kokonaisvaltainen IDS-järjestelmä liittyvät jonkinasteisen edellä esitettyjen lokiratkaisujen lisäksi verkon liikennettä seuraavan IDS-ratkaisun toteuttamiseen. Tällöin tavoitteena olisi kerätä tietoa muun muassa seuraavista asioista:

- erilaisten ohjelmistojen tai ihmisten antamista hälytyksistä
- verkon toimintaan liittyvistä virheraporteista
- itse verkkoliikenteestä
- järjestelmätoiminnoista
- tiedostojen ja hakemistojen odottamattomista muutoksista
- verkkoon liitetyistä laitteista
- fyysisten resurssien luvattomasta käytöstä. [1, s. 237–268]

Verkkoliikenteen osalta olisi hyvä seurata liikennekuormien määriä sisään ja ulos, liikenteeseen liittyviä virhelukumääriä ja liikenteeseen liittyvien tapahtumien laatua. Näitä on lisäksi hyvä verrata aikaisempaan ja kartoittaa mahdollisia muutoksia. Verkkoliikenteen laadun tarkkailussa pyritään havaitsemaan muun muassa hyökkäystä edeltävää verkon skannausta, yhteyksiä epätavallisista kohteista, protokollamääritysten loukkauksia, omaan verkkoon kuulumattomia paketteja, väärennettyjä osoitekenttiä sisältäviä paketteja, epätavallisia porttiyhdistelmiä, -numeroita ja protokollia sekä epätavallista ARP- ja DHCP/BOOTP-liikennettä. Lisäksi poikkeuksellisina aikoina muodostettuja yhteyksiä ja epätavallisten sovellusten käyttöä olisi hyvä seurata. [1, s. 237–243]

Murto-ohjelmien havaitsemisen mahdollisuudet riippuvat pitkälti ohjelman toimintatavasta. Mikäli murto-ohjelma toimii verkossa aktiivisesti, on se todennäköisesti helpompaa havaita. Jotkut ohjelmat saattavat kuitenkin tyytyä passiiviseen toimintaan, jolloin niiden havaitsemiseksi tarvitaan itse suoritettuja aktiivisia toimia verkon kartoittamiseksi

ja skannaamiseksi, mikä mahdollistaisi tällaisten ohjelmien toiminnan havaitsemisen [1, s. 250].

Käytännössä murto-ohjelmien toiminnan havaitseminen tapahtuu pääsääntöisesti osana verkkoliikenteen seurantaa tai lokitietojen käsittelyä. Kyseisiin tarkoituksiin käytettävät ohjelmat on kuitenkin määritettävä ja säädettävä kykeneviksi havaitsemaan eri murto-ohjelmien käytöstä aiheutuvia merkkejä ja seurauksia. Periaatteessa jokaista toiminnallisuutta varten on mahdollista hankkia erillinen ohjelmistonsa, mutta yksinkertaisinta olisi kuitenkin pyrkiä hankkimaan yksi kaikki nämä yhdistävä ratkaisu, joista esimerkkeinä ovat alaluvussa 3.5 esitelty Security Onion ja alaluvussa 3.4 esitellyt kaupalliset ratkaisut.

Y-malli Oy:n tapauksessa päädyttiin toteuttamaan IDS-järjestelmä Security Onionin avulla. Ratkaisu katsottiin edulliseksi toteuttaa, vaikka sitä varten jouduttiinkin tekemään muutamia laitehankintoja. Koska järjestelmä toteutettiin tämän diplomityön osana, ei sen toteuttamiseen tarvittu juurikaan yrityksen oman henkilöstön työaikaa, mikä myös vaikutti kyseiseen ratkaisuun päätymiseen.

4.2 Tietomurtojen tutkinta ja muu jälkiselvittely

Tietomurron tapahduttua ja sen tultua havaituksi riippuu tutkinnan ja muiden jälkiselvittelyjen toteuttaminen ensinnäkin siihen osallistuvista tahoista. Mikäli yrityksellä on käytössään jokin kaupallinen tietomurron havaitsemiseen kykenevä järjestelmä, tulee järjestelmän toimittaja mahdollisesti suoraan mukaan selvittämisprosessiin. Jos näin ei ole, on asianomistajayrityksellä mahdollisuus valita, minkä tahon puoleen kääntyä. Jos yrityksellä on tietoturvavakuutus, on vakuutusyhtiö todennäköisesti ensimmäisiä ilmoituksen saajia, jolloin vakuutuksen sisältö saattaa määrittää mahdollisia toimintatapoja. Muina mahdollisuuksina on ulkopuolisen tietoturvayrityksen puoleen kääntyminen ja jonkinasteisen tietomurron selvittämiseen keskittyvän palvelun tilaaminen tai yhteyden ottaminen viranomaisiin, kuten poliisin tai viestintävirastoon. Luonnollisesti yrityksellä on myös mahdollisuutena olla ottamatta yhteyttä yhteenkään ulkopuoliseen tahoon ja pyrkiä tutkimaan asia omin päin.

Asianomistajan intressit tapahtuman selvittämisessä vaikuttavat merkittävästi siihen, mihin tahoon mahdollisesti tapahtuman johdosta ollaan yhteydessä. Erilaisia selvittämiseen liittyviä intressejä ovat muun muassa:

- vahinkojen minimointi ja rajaaminen
- vahinkojen ja järjestelmän korjaaminen
- toiminnan palauttaminen
- tekijän vastuuseen saaminen
- korvausten saaminen.

Näiden osalta on hyvä huomata, että ne saattavat olla osittain jopa ristiriidassa keskenään. Esimerkiksi tekijän vastuuseen saaminen edellyttää asian ilmoittamista poliisille, todistusaineiston suojaamista ja rikosprosessin läpikäymistä, mikä voi olla ristiriidassa toiminnan nopean palauttamisen kanssa. Tämän johdosta yrityksen tulisikin omalla kohdallaan pohtia, mitkä ovat sen itsensä kohdalla ne tärkeimmät intressit tietomurron tapahtuessa.

Käytännössä yrityksen vaihtoehdot tietomurron selvittämisessä voidaan jakaa kolmeen eri kategoriaan. Ensinnäkin yritys voi tehdä kaiken selvitys- ja korjaustyön itse, jolloin vaaditaan riittävää osaamista omasta henkilöstöstä. Lisäksi resursseja joudutaan irrottamaan muusta toiminnassa selvitys- ja korjaustoimia varten. Intresseistä tekijöiden vastuuseen saaminen ja korvauksen saaminen eivät tule mitä ilmeisimmin tällöin toteutumaan. Merkittävänä riskinä on myös tutkinnan ja muiden jälkitoimien jääminen puutteelliseksi.

Toisena vaihtoehtona on tietoturvayrityksen hyödyntäminen. Tähän kohtaan sisältyvät vaihtoehdot ovat tutkintapalvelun ostaminen, vakuutusyhtiön tietoturvavakuutuksen kautta tarjoaman yrityksen tutkintapalvelu sekä jo valmiina asiakasyrityksen kanssa yhteistyötä tekevän yrityksen suorittama tapauksen selvittäminen. Tässä kohtaa etuna on, että tapaus tulee todennäköisemmin suhteellisen nopeasti korjattua ja selvitettyä sekä yritys voinee luottaa siihen, ettei korjaustoimien jälkeen ongelma pääse ainakaan ihan heti toistumaan. Haittapuolena tässä kohtaa ovat selvittämisen kustannukset, jotka saattavat pienelle yritykselle olla merkittäviä. Tietoturvavakuutus tuo luonnollisesti tähän helpotusta. Intressien osalta tässäkin vaihtoehdossa jäävät kuitenkin tekijän vastuuseen saaminen ja korvausten saaminen toteutumatta. Toki asiasta on mahdollista ilmoittaa poliisille myöhemmässäkin vaiheessa, mutta on tärkeää tiedostaa, että kaikenlainen toiminta mukaan lukien tietoturvayrityksen toimet laskevat todennäköisesti saatavissa olevan todistusaineiston todistusarvoa.

Kolmantena vaihtoehtona on ottaa yhteyttä viranomaisiin. Poliisille voi tietomurrosta ilmoittaa käytännössä joko soittamalla asiasta hätäkeskukseen tai paikallisen poliisilaitoksen poliisipäivystykseen, tekemällä rikosilmoituksen poliisilaitoksella tai poliisin internet-sivuilla tai ilmoittamalla tapahtumasta keskusrikospoliisin Nettivinkki-palvelun kautta. Tietomurtotapauksissa tarkoituksenmukaisin tapa ilmoittaa asiasta poliisille on todennäköisesti joko soittamalla palvelupäivystykseen tai menemällä itse paikan päälle tekemään tapahtuneesta rikosilmoitus poliisilaitokselle. Hätäkeskukseen soittaminen ei siinä mielessä ole tarkoituksenmukaista, että heillä ei ole suoraa yhteyttä poliisin tietoteknisen tutkinnan hälyttämiseksi. Internetin kautta tehtävissä ilmoituksissa on heikkoutena ilmoituksen vastaanottamiseen liittyvä viive. Käytännössä internetin kautta tehty rikosilmoitus saattaa johtaa tutkinnan aloittamiseen vasta muutaman päivän päästä ilmoituksen tekohetkestä, mikä tietomurtojen tapauksessa on viiveenä liian suuri. Soittaminen suoraan poliisille tai meneminen poliisilaitokselle tekemään ilmoitusta antaa poliisille mahdollisuuden saman tien tehdä arvio tutkinnan tarpeesta ja tarkoituksenmukaisista toimista.

Virka-aikana poliisilla on mahdollisuus lähettää tietotekniseen tutkintaan erikoistunut partio paikan päälle suorittamaan tarvittavia tutkimuksia. Virka-ajan ulkopuolella viive on pidempi, mutta viimeistään seuraavana päivänä mahdollisuus partion saamiseen paikalle on olemassa. Poliisille ilmoittamisessa on etuna mahdollisuus tekijän saamiseksi vastuuseen ja siten korvausten hakeminen. On myös hyvä huomata, että tietomurtojen tekijät syyllistyvät mahdollisesti myös muihin tietomurtoihin, minkä vuoksi tekijän vastuuseen saamisella on mahdollista estää muita tulevaisuudessa tapahtuvia tietomurtoja. Ilman rikosten ilmoittamista poliisille tekijöillä on mahdollisuus jatkaa omaa toimintaansa vapaasti. Poliisin tutkinnan kautta on myös mahdollista saada tieto tietomurron tekotavasta ja sen mahdollistaneista tekijöistä. Haittapuolena on, että poliisilta ei ole mahdollista saada vahinkojen korjauspalvelua.

Aiemmin poliisille ilmoittamista on voitu pitää haitallisena yrityksen maineen kannalta eikä sen hyötyä ole välttämättä nähty tai osattu arvostaa. Kuten kuitenkin alaluvussa 3.2 tuotiin ilmi, jatkossa yrityksellä on velvollisuus ilmoittaa tietomurrosta niille henkilöille, joiden tietoja murto koskee. Kun kerran asia on joka tapauksessa tuotava ilmi, ei poliisille ilmoittamisesta todennäköisesti ole maineen menettämisen kannalta enää lisähaittaa.

Tässä työssä esitetyn Y-malli Oy:n kannalta tarkoituksenmukaisin tapa olisi yhdistää edellä mainittuja vaihtoehtoja. Ensinnäkin tapauksesta tulisi ilmoittaa saman tien poliisille puhelimitse tai poliisilaitoksella. Tätä varten havainnon tekemisen jälkeen tulisi tietokone pyrkiä eristämään verkosta irrottamalla fyysinen verkkokaapeli tietomurron kohteena olevasta järjestelmästä tai laitteesta, vaikka mahdollisesti tälläkin menetetään joitain jälkiä, mutta murron ja sen aiheuttamien vahinkojen rajaaminen on tehokkaampaa. Varsinainen tietojärjestelmä ja laite pyritään pitämään koskemattomana ja samassa tilassa, kun tietomurron havaitsemishetkellä. Poliisin tietoteknisen tutkinnan suorittamisen tai siihen liittyvien ohjeiden jälkeen seuraa vahinkojen ja järjestelmän korjaaminen. Tätä varten Y-malli Oy:lle olisi hyvä ottaa tietoturvavakuutus korjaamisesta aiheutuvien kulujen kattamiseksi.

Tietomurtojen selvittämiseen liittyen tulisi yrityksellä olla ennalta sovittu toimintamalli tietomurtojen varalta. Toimintamallin tulee olla koko henkilöstön tiedossa ja sen tulee olla riittävän selkeä, että sitä on mahdollista noudattaa kaikissa tilanteissa. Edellä mainittujen toimenpiteiden ohella selvittämiseen liittyvät olennaisesti kaiken saatavilla olevan tiedon kerääminen, suojaaminen ja tallentaminen, murrettujen järjestelmien varmuuskopiointi ja eristäminen, murtautumisen laajuuden määrittäminen, lokien tutkiminen sekä hyökkääjän tunkeutumistavan ja tekojen selvittäminen. [1, 270–278] Hyvin olennaista on myös kaikkien tehtyjen toimien dokumentointi: kuka teki, mitä teki ja milloin teki sekä missä tietoa on käsitelty. Dokumentoinnilla on erittäin tärkeä merkitys kerätyn aineiston todistusarvoa arvioitaessa, minkä vuoksi se ei juurikaan voi olla liian pikkutarkkaa. Käytännössä tavoitteena on kyetä jälkeenpäin ilmoittamaan tarkalleen, missä todistusaineisto on minäkin ajanhetkenä sijainnut ja miten sitä on paikasta toiseen siirretty. [1, s. 283–284]

Selvittämiseen liittyen yrityksen on hyvä pohtia myös lokien ja muun mahdollisesti kertyvän todistusaineiston tallentamista ja säilyttämistä. Kuten on tuotu esille, on keskeistä aineiston säilyminen eheänä. Jälkeenpäin on kyettävä todentamaan, etteivät tiedot ole muuttuneet. Tähän liittyen muun muassa OSSEC-ohjelmassakin olevan kaltainen tarkistussummien käyttö on käytännöllinen ja tarkoituksenmukainen tapa eheyden tarkistukseen.

Eheyden huomioimisen lisäksi olisi lokitiedot hyvä säilyttää siten, ettei niiden tuhoaminen ole helppoa. Käytännössä tämä edellyttää toimivaa ja tehokasta varmuuskopiointia. Varmuuskopiot olisi syytä säilyttää täysin erillisellä sitä varten varatulla laitteella. Yhtenä varteenotettavana vaihtoehtona on myös varmuuskopioiden tallentaminen yrityksen oman rakennuksen ulkopuolelle niin sanottuun pilvipalveluun tai yrityksen omalle muualla sijaitsevalle laitteelle. Kummassakin tapauksessa tulee hyvin tarkasti huolehtia, että kyseinen palvelu tai säilytyspaikka täyttää tietoturvalle asetetut vaatimukset. Pilvipalvelujen käytössä on lisäksi huomioitava sen käyttämien palvelinten fyysinen sijainti ja siihen liittyen tietojen siirtoon liittyvä alaluvussa 3.6 esitetyt lainsäädännölliset tekijät. Kaiken tiedon säilyttäminen omissa tiloissa aiheuttaa tiedon tuhoutumiselle hieman korkeamman riskin kuin pilvipalvelujen hyödyntäminen, joka taas saattaa ainakin tuntua turvattomammalta vaihtoehdolta. Molemmat vaihtoehdot kuitenkin voidaan perustella tarkoituksenmukaisiksi pienyritykselle heidän omasta tilanteestaan riippuen.

Varsinaista selvittämistä seuraa järjestelmän korjaaminen ja palauttaminen. Selvitystyön tuloksena olisi olennaista kyetä hahmottamaan, miten hyökkääjä on päässyt tunkeutumaan järjestelmään, jotta vastaavanlainen toiminta kyetään jatkossa estämään. Järjestelmä tulisikin paikata tietomurron jälkeen sitten, että kaikki hyökkääjän käyttämät murtautumisreitit tulevat tukituksi. Käytännössä järjestelmän korjaaminen saattaa sisältää salasanojen vaihtoa, järjestelmien uudelleen asentamista, asetusten tarkastamista, tietoturva-aukkojen paikkaamista sekä turva- ja havaitsemismekanismien parantamista. [1, s. 289–293]

5. YHTEENVETO

Työssä lähdettiin liikkeelle kahdesta tutkimuskysymyksestä, joiden kautta oli tarkoituksena ensinnäkin selvittää, minkälaisilla ratkaisuilla pienten yritysten on ylipäänsä mahdollista pyrkiä havaitsemaan tietomurtoja ja edesauttamaan niiden selvittämistä. Toiseksi tarkoituksena oli selvittää, missä määrin nämä ratkaisut olisivat pienen yrityksen kannalta toteutettavissa.

Erilaisia ratkaisuvaihtoja tietomurtojen havaitsemiseen esiteltiin luvussa 3. Käytännössä pienellä yrityksellä on vaihtoehtona olla toteuttamatta mitään ratkaisuja, ostaa eri tietoturvayrityksien tarjoamia kaupallisia ratkaisuja tai toteuttaa ratkaisut itse esimerkiksi tarjolla olevien ilmaisten avoimeen lähdekoodiin perustuvien ohjelmistojen pohjalta. Yhdeksi merkittävimmiksi haasteiksi tietoturvaratkaisujen toteuttamisessa muodostuu helposti niihin vaadittavat resurssit. Kattavien kaupallisten ratkaisujen rahalliset kustannukset saattavat nousta merkittäviksi, kun taas itse toteutettavissa avoimen lähdekoodin ohjelmistoja hyödyntävissä ratkaisuissa tarvitaan aika ja henkilöstöä. Toki näiden ratkaisujen osittainen yhdisteleminen on myös mahdollista.

Ratkaisuvaihtojen pohdinnassa vaikuttavat merkittävästi yrityksen käytössä olevat resurssit. Mikäli yrityksellä on rahaa sijoittaa tietoturvan parantamiseen, antavat kaupalliset ratkaisut todennäköisimmin helpomman tavan tietoturvallisuuden parantamiseen. Mikäli rahaa ei kuitenkaan kaupallisia ratkaisuja varten ole käytettävissä, tulee pohdittavaksi työtuntien käyttäminen tietoturvaratkaisujen toteuttamiseen itse. Tarjolla olevat avoimen lähdekoodin ratkaisut, kuten esille tuotu Security Onion, tarjoaa melko vaivattoman tavan ottaa käyttöön tietomurtojen havaitsemiseen kykenevä järjestelmä. Tällöin kuitenkin edellytyksinä ovat järjestelmän vaatiman laitteiston olemassaolo tai hankinta ja riittävä tietotekninen osaaminen, jotta järjestelmän asetukset saadaan säädettyä sopivaksi. Haasteellisin tilanne tulisi olemaan yrityksillä, joilla ei ole taloudellisen tilanteensa vuoksi oikein irrottaa rahaa tietoturvaratkaisujen toteuttamiseen eikä osaamista tai aikaa niiden toteuttamiseen itse. Tällöin kuitenkin tärkeää olisi pyrkiä keskittämään voimavaroja edes jossain määrin tietoturvan parantamiseen pieni askel kerrallaan.

Työssä selvitettiin, mitkä ovat tietomurtojen tekotavoista yleisimpiä ja siten todennäköisimpiä uhkia juuri Suomen oloissa. Tietoja haettiin sekä julkisista lähteistä että Suomen poliisin rikosilmoitustiedoista. Tutkimusten tuloksena todettiin, että tietomurtojen yleisimpiä tekotapoja vuosina 2014–2016 olivat käyttäjätunnusten luvaton hyödyntäminen, fyysinen pääsy kohdelaitteelle ja kalastelu. Näitä seurasivat sitten verkkosivustoille tunkeutuminen ja haittaohjelmien hyödyntäminen. Käytännössä yleisimpien tekotapojen perusteella kävi ilmi, että ihminen vaikuttaisi edelleen olevan tietoturvan heikoin lenkki. Kirjatuista rikosilmoituksista yli 70 % olisi nimittäin saatu ehkäistyä huolellisilla ja tietoturvallisilla toimintatavoilla.

Kuten edellä on tullut esille, on niin sanottu inhimillinen tekijä merkittävimmässä roolissa tietomurtojen mahdollistumisessa. Tämän johdosta ensisijainen ratkaisu yrityksille tietoturvan parantamiseen olisi henkilöstön tietoisuuden ja osaamisen parantaminen. Henkilöstön osaamisen parantamiseksi voidaan esimerkiksi järjestää henkilöstölle tietoiskuja, koulutusta, seminaareja sekä parantaa sisäistä viestintää ja tiedottamista myös tietoturvaan liittyvistä asioista. Erityisesti tietoisuutta tulisi pyrkiä lisäämään erilaisten kalasteluyritysten varalle, omien tunnusten turvallisesta säilyttämisestä ja käsittelystä sekä sähköpostin turvallisesta käytöstä. [23, s. 108–109]

Käytännössä inhimillisen tekijän roolin suuruus tuo esille myös sen, että tietomurtojen torjumis- ja havaitsemiskyvyn parantaminen yleisimpien tekotapojen osalta ei välttämättä vaadi kalliita tai työläitä tunkeutumisenhavaitsemisjärjestelmiä. Pelkästään jo henkilöstön tietoisuuden lisääminen, kouluttaminen ja poikkeavuuksista ilmoittamisen kannustaminen edesauttavat merkittävästi tietomurtojen ehkäisyä ja havaitsemista. Tämän lisäksi tietoteknisiä ratkaisuja on myös toteuttavissa asteittain, jolloin kertaheitolla toteutettu täydellinen IDS-järjestelmä ei ole välttämätön.

Poliisin rikosilmoitustiedoista kerättyjen tietojen pohjalta luotiin 8-portainen portaikko tietomurtojen havaitsemiskyvyn parantamiseen käytettävä. Portaikon ajatuksena on, että portaille on kirjattu tietomurron tekotavat yleisimmästä harvinaisempaan. Yrityksen tarkoituksena on portaikkoa hyödyntäessään aloittaa ratkaisujen toteuttaminen alimmalta portaalta eli yleisimmästä tekotavasta ja toteuttaa sen havaitsemiseen kykenevä ratkaisu. Tämän jälkeen tarkoituksena on siirtyä seuraavalla portaalle ja siitä sitten taas eteenpäin. Näin edeten yritys tulee toteuttaneeksi sellaisia havaitsemisratkaisuja, jotka keskittyvät niihin uhkiin, jotka todennäköisesti heitä kohtaisivat.

EU:n tietosuoja-asetus tuo mukanaan yrityksille säädetyn velvollisuuden ensinnäkin kyetä havaitsemaan ja toiseksi ilmoittaa henkilötietoihin kohdistuneista tietomurroista. Asetuksessa ei ole kuitenkaan sen tarkemmin säädetty sitä, mikä on riittävä havaitsemisen taso. Tässä vaiheessa ei myöskään ole tämän osalta tarkempaa kansallista ohjeistusta tarvittavasta havaitsemiskyvyn tasosta. Asetuksessa mainitaan, että ratkaisujen tulisi olla asianmukaisia ja vastata tietojen turvallisuuteen kohdistuvat riskin tasoa. [28] Se, mitä asianmukaisuudella tarkoitetaan, jää avoimeksi, mutta on vaikeaa kuvitella, että nykytilanteessa tultaisiin pienimmiltä muutaman henkilön yrityksiltä edellyttämään kokonaisvaltaisen IDS-järjestelmän käyttöönottoa. Tällöin pienemmille yrityksille säädetty tavoitetaso portaikossa voitaisiin ajatella olevan jollain alemmalla portaalla.

Tässä työssä ratkaisujen tarkastelun pohjana käytettiin poliisin rikosilmoitustietoja tietomurroista. Kuten yksityisten organisaatioiden raporteissakin, on näin kerätyissä tiedoissa omat puutteensa. Ensinnäkin yrityksiin kohdistuvia tietomurtoja oli kirjattu verrattain vähän. Toiseksi merkittävä osa ilmoituksista ei sisältänyt riittävästi tietoa tekotavasta, jotta sen tiedot olisi ollut mahdollista sisällyttää tähän tutkimukseen, millä oli varmasti ainakin

jonkinasteista vaikutusta eri tekotapojen välisiin suhteisiin. Esimerkiksi on hyvin todennäköistä, että kalastelun avulla tehtyjen tietomurtojen määrä taulukossa 1 on todellista määrää jonkin verran alhaisempi. Tämä oli mahdollista päätellä siitä, että merkittävä määrä kalastelulta vaikuttavia tietomurtoilmoituksia jätettiin tekotapatietojen ulkopuolelle, koska kalastelun osuutta ei ollut riittävällä varmuudella tuotu esille, vaikka viitteitä tästä olikin.

Kaiken kaikkiaan poliisin rikosilmoitustietojen hyödyntäminen toi mukanaan harvinaisemman ja siten uuden näkökulman tietomurtotilastoihin. Positiivista oli huomata, että verrattaessa erilaisiin yksityisiin raportteihin, yhteneväisyyksiä oli merkittävästi. Täten jatkoa ajatellen voidaan ajatella, että erityisesti laajimmat kansainväliset raportit antavat myös viitteitä tietomurtojen tekotapojen suuntauksista ja todennäköisyyksistä myös Suomessa.

LÄHTEET

[1] J. Allen, A.Toivonen (kään.), Verkkotietoturvan hallinta - CERT, Helsinki, Edita Prima Oy, 2002.

[2] BitDefender, BitDefender Box, verkkosivu. Saatavissa: https://www.bitdefender.com/box. Luettu: 3.4.2017.

[3] R. Bray, D. Cid, A. Hay, OSSEC HIDS Host-Based Intrusion Detection Guide, Burlington MA, Syngress Publishing Inc., 2008.

[4] Esitutkintalaki, L 22.7.2011/805, 2011. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2011/20110805

[5] Euroopan unionin verkko- ja tietoturvavirasto, ENISA Threat Landscape 2015, 2016. Saatavissa: https://www.enisa.europa.eu/publications/etl2015. Luettu: 10.2.2017.

[6] D. Frände, J. Matikkala, J. Tapani, M. Tolvanen, P. Viljanen, M. Wahlberg, Keskeiset rikokset, 3. uudistettu ja laajennettu painos, Edita Publishing Oy, Porvoo, 2014, 1066 s.

[7] F-Secure, F-Secure SAFE, verkkosivu. Saatavissa: https://www.f-secure.com/fi_FI/web/home_fi/safe. Luettu: 14.2.2017.

[8] F-Secure, F-Secure Rapid Detection Service -brochure. Saatavissa: https://www.f-secure.com/documents/10192/1617120/2016-05-9-RDS-brochure.pdf. Luettu: 14.2.2017.

[9] Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi, HE 94/1993, 1993, 560 s. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_94+1993.pdf

[10] Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeksi, HE 232/2014, 2014, 63 s. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_232+2014.pdf

[11] Hallituksen esitys eduskunnalle tietoyhteiskunta-kaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta, HE 221/2013, 2013. Saatavissa: http://www.finlex.fi/fi/esitykset/he/2013/20130221

[12] Henkilötietolaki, L 7.8.2015/901, 2015. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

[13] If Vahinkovakuutusyhtiö Oy, Tietoturvavakuutuksen faktaesite. Saatavissa: https://www.if.fi/web/fi/sitecollectiondocuments/commercial/yritysten_vastuu-vakuutukset/66623_tietoturvavakuutus%20esite_11_8_hyv.pdf. Luettu: 20.3.2017.

[14] Insta Oy, Lokienhallinta & SIEM, verkkosivu. Saatavissa: http://security.insta.fi/solutions-tt-fi/product-tt-fi/productid=22791710/solutionid=45957246. Luettu: 19.3.2017.

[15] International Chamber of Commerce, ICC Cyber security guide for business, 2015. Saatavissa: http://kauppakamari.fi/wp-content/uploads/2015/04/icc-cyber-security-guide-for-b-2015.pdf. Luettu: 19.3.2017.

[16] KKO:2003:36, Korkeimman oikeuden ennakkoratkaisu. Saatavissa: http://www.finlex.fi/fi/oikeus/kko/kko/2003/20030036

[17] KKO 2013:20, Korkeimman oikeuden ennakkoratkaisu. Saatavissa: http://www.finlex.fi/fi/oikeus/kko/kko/2013/20130020

[18] KKO 2015:42, Korkeimman oikeuden ennakkoratkaisu. Saatavissa: http://www.finlex.fi/fi/oikeus/kko/kko/2015/20150042

[19] M. Laaksonen, T. Nevasalo, K. Tomula, Yrityksen tietoturvakäsikirja, Helsinki, Edita Publishing Oy, 2006, 324 s.

[20] Laki yksityisyyden suojasta työelämässä, L 30.12.2014/1345, 2014. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

[21] J. Limnell, K. Majewski, M. Salminen, Kyberturvallisuus, Jyväskylä, Docendo Oy, 2014, 246 s.

[22] Nixu Oyj, Tietoturvatiedon ja tapahtumien hallinta (SIEM), verkkosivu. Saatavissa: https://www.nixu.com/fi/palvelualueet/tietoturvatiedon-ja-tapahtumien-hallinta-siem. Luettu: 19.3.2017.

[23] K. Norppa, J. Peltomäki, Rikos meni verkkoon, Helsinki, Talentum Media Oy, 2015, 179 s.

[24] C. Pfleeger, S. Pfleeger, Security in Computing, Fourth edition, Boston, Pearson Education Inc., 2007, 845 p.

[25] Poliisiasiain tietojärjestelmä, PATJA

[26] Poliisin valtakunnallinen tulostietojärjestelmä, PolStat

[27] Pulsen Oy, Lokienhallinta ja SIEM, verkkosivu. Saatavissa: http://www.pulsen.fi/sivut/palvelut/lokienhallinta-ja-siem.html. Luettu: 19.3.2017.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Saatavissa: http://eur-lex.europa.eu/eli/reg/2016/679/oj

[29] Rikoslaki, L 21.12.2016/1287, 2016. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

[30] Security Onion, Security Onion Wiki, verkkosivu. Saatavissa: https://github.com/Security-Onion-Solutions/security-onion/wiki. Luettu: 30.3.2017.

[31] Symantec, 2016 Internet Security Threat Report, 2016. Saatavissa: https://www.symantec.com/security-center/threat-report. Luettu: 10.2.2017.

[32] T. Thomas, J. Holttinen (kään.), Verkkojen tietoturva, Helsinki, Edita Prima Oy, 2005.

[33] Tietoyhteiskuntakaari, L 29.6.2016/558, 2016. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2014/20140917

[34] Valtionvarainministeriö, EU-tietosuojan kokonaisuudistus, VAHTI-raportti 1/2016. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128.

[35] Valtionvarainministeriö, Sisäverkko-ohje, VAHTI-ohje 3/2010. Saatavissa: https://www.vahtiohje.fi/web/guest/3/2010-sisaverkko-ohje

[36] Valtionvarainministeriö, Valtionhallinnon tietoturvasanasto, VAHTI-ohje 8/2008. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

[37] Verizon, 2016 Data Breach Investigations Report, 2016. Saatavissa: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/. Luettu: 10.2.2017.

[38] Viestintävirasto, Tietoturvan vuosi 2016, 2017. Saatavissa: https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2017/tietoturvanvuosi2016.html. Luettu: 12.3.2017.