Tampereen yliopisto

Lasse Kajavalta

YRITYKSIIN KOHDISTUVAT TIETOMURROT JA NIIHIN LIITTYVÄ RISKIENHALLINTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Joulukuu 2019

TIIVISTELMÄ

Lasse Kajavalta: Yrityksiin kohdistuvat tietomurrot ja niihin liittyvä riskienhallinta (Enterprise data breaches and risk management)
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikka, TkK
Joulukuu 2019

Yritysten käsittelemää luottamuksellista dataa uhkaavat jatkuvat tietomurtotapaukset, joissa ulkopuoliset pääsevät käsiksi heille tarkoittamattomaan dataan. Tästä muodostuu riski sekä yritykselle itselleen että sen käyttäjille, joiden tietoja vuotaa ulos yrityksestä. Tässä tutkielmassa tarkastellaan, miten tietomurtoja tapahtuu sekä miten niiden mukanansa tuomaa riskiä voidaan hallita yrityksen näkökulmasta. Tutkielma on kirjallisuuskatsaus, joten käsitellyt tiedot perustuvat alan julkaisuihin, eivätkä omaan tutkimustyöhön.

Ensimmäiseksi työssä tarkastellaan tietomurtojen taustaa. Tietomurtoja voi tapahtua verkon välityksellä tai hyökkääjän fyysisten toimenpiteiden seurauksena. Verkon välityksellä tapahtuvien hyökkäysten nähdään olevan huomattavasti yleisempiä. Tietomurtojen takana olevien tekijöiden havaitaan useimmin olevan peräisin yrityksen ulkopuolelta sekä taloudellisesti motivoituneita. Tietomurtojen todetaan kohdistuvan moniin eri tyyppisiin yrityksiin ja organisaatioihin, joista yleisimmiksi osoittautuvat eri tyyppiset pienyritykset.

Toiseksi työssä käsitellään riskienhallintaa ja pyritään antamaan kuva siitä, miten yritys voi arvioida tietomurtojen aiheuttamaa riskiä. Esitellään myös keinoja uhilta suojautumiseen ja tietomurron tapahtumisen jälkeen siitä toipumiseen tarvittavia toimenpiteitä.

Lopuksi työssä käydään läpi esimerkkinä merkittävä tapahtunut tietomurto, tutkitaan sen seurauksia ja keinoja, joilla tietomurto oltaisiin voitu estää.

Avainsanat: Tietomurrot, Riskienhallinta, Tietoturvallisuus

SISÄLLYSLUETTELO

1 JOHDANTO

Teknologian jatkuvan kehittymisen ja digitalisaation myötä myös yritystoiminta on kokenut merkittäviä muutoksia. Yritykset käsittelevät nykypäivänä paljon liiketoimintaansa liittyvää dataa aina asiakkaiden tiedoista tuotekehitykseen. Yrityksen luottamuksellinen data on arvokasta, joten se kiinnostaa myös ulkopuolisia osapuolia. Tietoturvallisuus nousee esille uutisoinnissa jatkuvasti, kun luottamuksellista dataa päätyy tietomurtojen kautta ulkopuolisten käsiin. Tietomurrot muodostavat merkittävän riskin yritykselle ja sen asiakkaille, jonka vuoksi on tärkeää, että niihin varaudutaan mahdollisimman hyvin.

Tässä työssä käsitellään yrityksiin kohdistuvia tietomurtoja riskienhallinnan näkökulmasta. Työssä käydään läpi tietomurtojen määritelmä ja jaotellaan eri tyyppiset tietomurrot niiden taustalla olevien hyökkäysten perusteella. Työssä tutkitaan, kuinka tietomurtoja tapahtuu, mitä osapuolia niiden taustalla on ja mitkä ovat tyypillisimpiä hyökkääjien kohteita. Käsitellään tietomurtoihin liittyvää riskienhallintaa tutkimalla suojeltavaa dataa, tietomurroista aiheutuvia kustannuksia ja uhilta suojautumista. Ohjeistetaan myös tietomurrosta toipumista sellaisen tapahtuessa. Työssä käydään myös esimerkkitapauksena läpi vuonna 2013 tapahtunut Target Corporationiin kohdistunut tietomurto tutkimalla taustalla ollutta hyökkäystä, tietomurrosta aiheutuneita seurauksia, siihen reagointia ja sitä, miten tietomurto oltaisiin voitu välttää. Työn tavoitteena on antaa kuva siitä, miten tietomurtoja tapahtuu, miksi dataa tulee suojella ja kuinka yritykset voivat varautua niihin ennalta.

Työssä asiat käsitellään edellä esitetyssä järjestyksessä. Luvussa 2 keskitytään tietomurtoihin, luvussa 3 riskienhallintaan ja luvussa 4 käsitellään esimerkkitapaus.

Työn lähteinä on käytetty Tampereen yliopiston kirjaston tarjoamien palveluiden kautta löytyviä alan julkaisuja sekä muita verkon välityksellä saatavissa olevia aihepiiriin kuuluvia lähteitä.

2 TIETOMURROT

Yritykset tarjoavat asiakkailleen paljon eri tuotteita ja palveluita. Sekä asiakkaista että yrityksen omasta liiketoiminnasta kerätään paljon erityyppistä dataa, jonka luotetaan pysyvän vain siihen oikeutettujen osapuolien käytössä. Datan turvallisuutta uhkaavat kuitenkin jatkuvasti lisääntyvät tietomurtotapaukset. Tässä luvussa määritellään, mitä tietomurroilla tarkoitetaan, ja tutkitaan, miten niitä tapahtuu.

2.1 Tietomurtojen määrittely ja jaottelu

Tietomurrolla (engl. data breach) voidaan kontekstista riippuen tarkoittaa hieman eri asioita. Yleisesti tietomurrolla tarkoitetaan tietoturvaloukkausta, jossa luvattomat osapuolet pääsevät käsiksi luottamukselliseen tietoon. Tietomurtoihin voi liittyä datan katoamista, muuttumista sekä salassa pidettävän tiedon vuotamista ulkopuolisten käsiin. [1]

Termiä tietomurto käytetään yleensä vain siinä tapauksessa, kun ulkopuolinen osapuoli tunkeutuu järjestelmään. Tilanteesta, jossa tiedot pääsevät ulkopuolisten käsiin järjestelmän oikeutetun käyttäjän toiminnan seurauksena, käytetään yleensä termiä tietovuoto. Tietovuoto-termillä viitataan kuitenkin usein myös tietomurtoihin ja niiden vaikutuksiin erityisesti uutisoinnissa. Rikoslaissa tietomurto määritellään tarkoittamaan rangaistavaa tekoa, jossa henkilö oikeudettomasti tunkeutuu tietojärjestelmään tai ottaa selon tietojärjestelmässä käsiteltävästä datasta [2].

Tietomurtoja tapahtuu monilla eri tavoilla. Murtojen taustalla olevat tekijät, käytetyt menetelmät sekä tietomurtojen kohteet vaihtelevat paljon. On myös yleistä, että tietomurron tapahtumiseen liittyy useiden eri menetelmien yhdistäminen. Yksi tapa jaotella eri tietomurtotyyppejä on jakaa ne verkon välityksellä tapahtuviin sekä fyysisesti tapahtuviin hyökkäyksiin [3]. Verkon välityksellä tapahtuvat tietomurrot ovat huomattavasti yleisempiä. Yhdysvaltalaisen tietoliikenneyritys Verizonin julkaiseman raportin perusteella vain 4 % vuoden 2018 aikana tapahtuneista tietomurroista sisälsi hyökkääjän tekemiä fyysisiä toimenpiteitä [4].

2.2 Tietomurtojen taustalla olevat hyökkäykset

Verkon välityksellä tapahtuvissa tietomurroissa tekijä kohdistaa kyberhyökkäyksen yrityksen olemassa olevaa verkkoinfrastruktuuria kohtaan tavoitteenaan tietojen varasta-

minen kohdeyritykseltä [3]. Tämän tyyppisiä tietomurtotekniikoita on suuri määrä, ja uusia haavoittuvuuksia löydetään eri järjestelmistä koko ajan. Tässä luvussa esitellään joitakin yleisimpiä esimerkkejä näistä.

Yksinkertaisimmissa verkon kautta tapahtuvissa hyökkäyksissä tekijä pyrkii hyväksikäyttämään tietojärjestelmän julkista puolta päästäkseen käsiksi salaiseksi tarkoitettuun dataan. Tyypillinen esimerkki tällaisesta hyökkäyksestä on SQL-injektio (engl. SQL injection). [3] SQL-injektiossa hyökkääjä pääsee antamaan tietokantapohjaiseen sovellukseen omia syötteitä, joita ohjelman tekijä ei ole tarkoittanut mahdolliseksi. Hyökkääjä hyödyntää tietokannan kyselykielen ominaisuuksia ja muokkaa käyttämäänsä sovellukseen annettua syntaksia antaakseen sovelluksen taustalla toimivalle tietokannalle omia komentoja. SQL-injektiossa hyökkääjä voi päästä lukemaan, muokkaamaan ja poistamaan dataa, johon hänen ei kuuluisi päästä käsiksi. [5]

Tietojenkalastelu (engl. phishing) on eräs yleisimmistä tietomurtoihin liittyvistä hyökkäystyypeistä. Maailmanlaajuisesti tietomurroista peräti 32 %:iin sisältyy tietojenkalastelua [4]. Tietojenkalastelua tapahtuu eri tavoin, mutta yleisesti ottaen hyökkääjä ottaa yhteyttä kohteeseen tekeytyen joksikin luotetuksi palveluksi tai henkilöksi ja tällä tavoin pyrkii pääsemään käsiksi salattuihin tietoihin. Tietojenkalasteluhyökkäyksessä hyökkääjä voi esimerkiksi ottaa sähköpostitse yhteyttä kohdeyrityksen henkilökuntaan tekeytyen joksikin käytössä olevaksi verkkopalveluksi ja ohjata heidät itse tekemälleen alustalle, johon työntekijä syöttää tietoja tietämättänsä tulevan huijatuksi. [3] Näin toimii esimerkiksi Suomessa yleinen yrityksiin kohdistuva Office 365 -huijaus. Onnistuneessa tietojenkalasteluyrityksessä rikollinen saa käsiinsä yrityksen henkilökuntaan kuuluvan osapuolen sähköpostitunnukset ja pääsee seuraamaan yrityksen sisäistä toimintaa pilvipalvelun kautta sekä esimerkiksi asettamaan sääntöjä sähköpostin uudelleenohjaukseen. Viestintävirasto on joutunut julkaisemaan varoituksia kyseisestä huijauksesta ja kuvaillut sitä vuoden 2018 merkittävimmäksi tietoturvauhaksi yrityksiä kohtaan. [6]

Eri tyyppiset haittaohjelmat ovat osallisena suuressa osassa tietomurtoja. Tapahtuneita tietomurtoja tutkittaessa on havaittu, että 28 % niistä sisälsi hyökkääjien asentamia haittaohjelmia. Tietomurtoihin johtaneiden haittaohjelmien tiedossa olevista tartuntatavoista yleisimmät liittyvät sähköpostin ja internetsivujen käyttöön. Haittaohjelmien tartuttamiseen käytetyistä tiedostotyypeistä yleisimmät ovat Office-dokumentit ja Windows-ohjelmat. [4] Yhden haittaohjelman tartutettua tietokoneen on myös mahdollista, että hyökkääjä saa asennettua kohdetietokoneelle sen avulla uusia eri tyyppisiä haittaohjelmia. Haittaohjelmatyypeistä tietomurtoihin osallisina ovat olleet erityisesti Command and Control -hyökkäykset, kiristyshaittaohjelmat sekä vakoiluohjelmat [4].

Command and Control -hyökkäyksessä hyökkääjä tartuttaa haittaohjelman kohdeyrityksen tietokoneeseen jollakin tavalla, esimerkiksi sähköpostin välityksellä, minkä jälkeen tartutettu laite ottaa yhteyttä hyökkääjän palvelimeen. Hyökkääjä saa palvelimen kautta ohjattua tartutetun tietokoneen toimintaa ja muun muassa asennettua lisää haittaohjelmia. Tämän tyyppisessä hyökkäyksessä on myös tyypillistä, että hyökkääjä pyrkii yhteyden saatuaan levittämään haittaohjelmaa kohdetietokoneen verkon muihin laitteisiin. [7]

Kiristyshaittaohjelmilla (engl. ransomware) tarkoitetaan haittaohjelmatyyppejä, joiden tarkoituksena on nimensä mukaisesti kiristää uhreja maksamaan lunnaita tartutetun järjestelmän sisältämästä datasta. Kiristyshaittaohjelmat saattavat muokata järjestelmän sisältämää dataa käyttökelvottomaksi tai lukita siihen käsiksi pääsemistä. On myös mahdollista, että hyökkääjä lukitsee koko tartutetun laitteen, kunnes lunnaat on maksettu. Kiristyshaittaohjelmiin perustuvat hyökkäykset ovat yleistyneet, sillä yksikin onnistunut hyökkäys voi taata suuret tuotot hyökkääjälle. Lunnaat maksetaan tyypillisesti kryptovaluuttana, joka mahdollistaa hyökkääjän yksityisyyden. Kryptovaluuttojen yleistyminen on ollut osallisena kiristyshaittaohjelmien yleistymiseen. [8] Lunnaiden maksamisesta huolimatta on olemassa riski, että hyökkääjä on kopioinut tiedot itselleen ja julkaisee tai muuten väärinkäyttää varastamaansa dataa.

Vakoiluohjelmat (engl. spyware) ovat haittaohjelmia, jotka keräävät tietoa käyttäjän toiminnasta ja lähettävät nämä takaisin hyökkääjälle. Vakoiluohjelmista erityisesti käyttäjän antamia syötteitä seuraavat näppäilytallentimet (engl. keylogger) ovat riski tietomurtojen kannalta. Näppäilytallentimet voivat sisältyä johonkin tiettyyn sovellukseen, kuten käytössä olevaan selaimeen, tai ne voivat seurata koko käyttöjärjestelmää ja kaikille sovelluksille annettuja syötteitä. Näppäilytallentimien avulla hyökkääjä voi saada haltuunsa paljon luottamuksellista tietoa, kun pääsee käsiksi siihen oikeutetun henkilön syöttämiin kirjautumistietoihin. Nykyaikaiset näppäilytallentimet voivat kerätä muutakin tietoa kuin pelkästään näppäimistön syötteitä. Ne voivat kerätä esimerkiksi tietoa hiiren liikkeistä, sovellusten ja internetin käytöstä sekä tallentaa kuvankaappauksia, mikrofoniin tulevaa ääntä ja web-kameran kuvaa. [9]

Fyysisissä hyökkäyksissä tekijät pyrkivät pääsemään käsiksi luottamuksellisten tietojen käsittelyyn käytettävään laitteistoon ja tätä kautta itse dataan. Tyypillisin tällainen hyökkäys on yritykselle kuuluvan laitteen varastaminen. Laitteista erityisesti kannettavat tietokoneet ja muut yrityksen tilojen ulkopuolella käytetyt mobiililaitteet ovat riskialttiita, mutta hyökkäys voi kohdistua myös yrityksen tiloissa sijaitsevia fyysisesti heikosti suojattuja laitteita kohtaan. [3]

Fyysinen hyökkäys voi tarkoittaa myös pelkän datan varastamista, kun hyökkääjä pääsee käsiksi kohdeyrityksen laitteeseen, josta saa kopioitua itselleen luottamuksellista dataa. Fyysiseksi hyökkäykseksi voidaan laskea myös se, kun ulkopuolinen osapuoli pääsee käsiksi luottamukselliseen dataan yrityksen hävittämien laitteiden tai tiedontallennusvälineiden kautta. [3]

2.3 Tietomurtojen syyt ja aiheuttajat

Tietomurtojen takana voi olla useita eri osapuolia, joiden motivaatiot hyökkäykseen vaihtelevat huomattavasti. Yleisimmin tietomurron takana on yrityksen ulkopuolinen osapuoli, mutta uhkia tietomurtoon esiintyy myös yrityksen sisäpuolelta. Tietomurtoon voi olla syyllisenä myös useampia osapuolia sekä yrityksen sisä- että ulkopuolella.

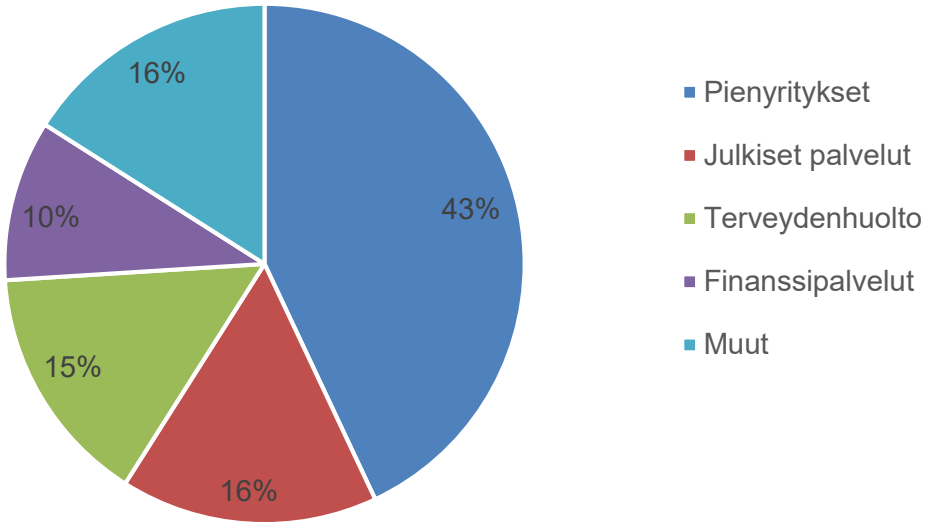
Ulkopuoliset tekijät voivat olla yksityisiä hakkereita, hakkeriryhmiä tai esimerkiksi kilpailevia yrityksiä, jotka suorittavat yritysvakoilua. Merkittävä määrä tietomurtoja tapahtuu myös eri valtioiden toimesta [4]. Yrityksen sisäpuolelta luottamuksellista dataa uhkaavat tekijät voivat olla esimerkiksi tyytymättömiä tai entisiä työntekijöitä sekä pahaa tahtovia vierailijoita.

Tietomurtojen taustan tutkimus on haasteellista, sillä eri yritykset reagoivat tietomurtoihin ja tiedottavat niistä eri tavoin tai eivät lainkaan. Tietomurtoja tapahtuu myös valtava määrä ja niistä tehdyt tutkimukset käyttävät eri lähteitä. Verizonin tuottaman raportin mukaan 69 % luottamuksellisen datan menetykseen johtaneista tapauksista sisälsi ulkopuolisia tekijöitä [4]. Yhdysvaltalaisen tietoturvayritys McAfeen tekemän tutkimuksen mukaan vastaava lukema on 57 % [10]. Tutkimusten prosenttilukemat sisältävät varsinaisten tietomurtojen lisäksi myös yrityksen sisäisten tekijöiden tahattomasti aiheuttamia tietovuotoja, mutta lukemat viittaavat kuitenkin siihen, että suurempi uhka dataa kohtaan kohdistuu yrityksen ulkopuolelta.

Tietomurtojen tekijöiden motivaatiot vaihtelevat, mutta yleisimmin hyökkääjät ovat taloudellisesti motivoituneita [4]. Hyökkääjät voivat esimerkiksi pyrkiä kiristämään kohdeyritykseltä rahaa tietojen avulla, myymään varastettua dataa eteenpäin tai käyttämään dataa itse hyötyäkseen siitä taloudellisesti. Tietomurron kohteen mukaan hyökkääjä voi päästä käsiksi esimerkiksi yrityksen liikesalaisuuksiin, käyttäjien tunnuksiin tai asiakkaiden luottokorttitietoihin. On myös mahdollista, että hyökkääjän tarkoituksena on vain pyrkiä vahingoittamaan kohdeyrityksen mainetta ja tuotemerkin arvoa.

2.4 Tietomurtojen kohteet

Kaikilla yrityksillä nykypäivänä on dataa, jonka menettämisestä tulee olla huolissaan. Tietomurron kohteen valintaan voivat vaikuttaa esimerkiksi varastettavan datan lopullinen käyttötarkoitus sekä kohdejärjestelmän turvallisuus. Kohteet vaihtelevat huomattavasti, ja tietomurtojen riski onkin läsnä kaiken tyyppisissä yrityksissä ja organisaatioissa. Yrityksen koko ei suoraan vaikuta riskin suuruuteen. Pienillä yrityksillä suojeltavan datan määrä on todennäköisesti pienempi, mutta sen suhteellinen arvo yritykselle voi olla huomattavasti suurempi.



Kuva 1. *Tietomurtojen kohteet* ***[4]****.*

Yksittäisistä eri tyyppisistä palveluista tutkitusti eniten luottamuksellista dataa päätyy ulkopuolisten käsiin julkisista, terveydenhuollon sekä finanssialan palveluista. Nämä palvelut muodostavat yhdessä 41 % tapauksista, joissa ulkopuoliset osapuolet ovat päässeet dataan käsiksi. Yhdessä eri tyyppiset pienyritykset muodostavat kuitenkin vielä suuremman 43 %:n osuuden tietomurroista. [4] Tietomurtojen yleisempiä kohteita on havainnollistettu myös kuvassa 1.

3 RISKIENHALLINTA

Tietomurtojen riski koskettaa nykypäivänä lähestulkoon kaikkia yrityksiä. Valtaosa yrityksistä nykypäivänä käyttää tietotekniikkaa ja internetiä toiminnassaan monin tavoin riippumatta siitä, millaisia tuotteita tai palveluja tuotetaan. Yrityksen toiminnasta ja sen asiakkaista kerätään paljon luottamuksellista dataa ja sen suojauksesta tulee olla huolissaan. Tässä luvussa tarkastellaan, miten tietomurtoihin voidaan varautua riskienhallinnan näkökulmasta.

3.1 Suojeltava data ja sen ominaisuudet

Yritykset käsittelevät nykypäivänä paljon eri tyyppistä dataa liiketoiminnassaan. Yrityksen toimintaan liittyvä data kiinnostaa monia ulkopuolisia tahoja, ja siksi on oleellista, että sitä suojellaan, ja vain oikeutetut osapuolet pääsevät siihen käsiksi. Datan suojelulla pyritään takaamaan sen luottamuksellisuus, eheys ja saatavuus. Mikäli datan turvallisuudesta ei pidetä huolta, seuraukset itse yritykselle sekä sen asiakkaille voivat olla merkittäviä. Ensimmäisenä askeleena riskienhallinnan näkökulmasta on oleellista, että yrityksellä itsellään on tieto siitä, mitä suojeltavaa dataa sillä on käsiteltävänä.

Eri tyyppistä yritystoimintaan liittyvää suojeltavaa dataa on merkittävästi. Yritykset, jotka pitävät kirjaa asiakkaistaan saattavat kerätä esimerkiksi asiakkaiden nimiä, osoitteita, luottokorttitietoja, pankkitunnuksia, henkilötunnuksia, potilasasiakirjoja, luottotietoja ja tilaustietoja [11]. Kaikki nämä ovat sellaista dataa, joka voi aiheuttaa asiakkaille merkittävää vahinkoa joutuessaan ulkopuolisten käsiin. Asiakkaiden tietojen lisäksi yrityksillä on dataa omasta toiminnastaan. Yrityksen omaa suojeltavaa dataa ovat muun muassa yrityksen talouteen liittyvät asiakirjat, liiketoimintasuunnitelmat, tuotesuunnitteludata, asiakaslistat, hinnoittelutiedot, henkilöstödata, yritysyhteistyöhön ja toimittajiin liittyvät tiedot sekä aineeton omaisuus, kuten lähdekoodi ja patentit [11]. Kun tiedetään, mitä suojeltavaa dataa yrityksellä on, voidaan lähteä suunnittelemaan siihen liittyviä suojaustoimenpiteitä ja riskienhallintaa.

Sen lisäksi että tiedetään, mitä suojeltavaa dataa yrityksellä on, yrityksen on tärkeää pystyä jäljittämään tietoa itse datasta. On tärkeää tietää esimerkiksi datan merkitys nyt ja tulevaisuudessa, mikä on datan alkuperä sekä mihin käyttötarkoitukseen data on tarkoitettu. Näin voidaan minimoida turhan datan määrä. Yritykselle on tärkeää olla tietoinen, kuinka paljon suojeltavaa dataa oikeasti on ja miten se on suojattu.

Esimerkiksi yhdysvaltalaiseen internetpalveluita tarjoavaan yhtiöön Yahoo! Inc. vuonna 2013 kohdistuneessa tietomurrossa menetettiin valtava määrä käyttäjien tietoja, ja osa näistä tiedoista oli joko salaamatonta tai heikosti salattua riippuen siitä, kuinka vanhaa data oli. [12] Kyseisessä tietomurrossa Yahoo ei ollut päivittänyt vanhempaa käyttäjädataa noudattamaan samaa salaustasoa, kun uudet datansuojauskäytännöt otettiin käyttöön.

Tietomurtoihin liittyvän riskin kannalta yritykselle on kannattavaa pyrkiä hävittämään turha data, jolle ei ole enää käyttöä. Vanhentuneet tiedot voivat olla merkityksettömiä yritykselle, mutta mahdollinen hyökkääjä voi saada niistä jotain hyötyä päästessään niihin käsiksi.

Suunnitellessa datan säilytykseen liittyviä suojaustoimenpiteitä sekä sen käsittelyyn liittyvää pääsynhallintaa on tärkeää pyrkiä luokittelemaan data sen mukaan, kuka on oikeutettu pääsemään siihen käsiksi. Yksi tapa luokitella yrityksen käsittelemää on jakaa se eri tasoille, esimerkiksi julkiseen, sisäiseen, luottamukselliseen sekä salaiseen tietoturvaluokitukseen. Eri luokittelutasoille luodaan omat säännöt sen käsittelyyn liittyen millä laitteilla, missä ja kuka sitä voi käsitellä. Esimerkiksi julkista dataa voidaan jakaa vapaasti sosiaalisessa mediassa, kun taas salaiseksi luokiteltua dataa voidaan käsitellä vain tietyillä yrityksen tiloissa olevilla verkkoon kytkemättömillä laitteilla.

3.2 Tietomurtojen aiheuttamat kustannukset

Tietomurtoihin liittyvän riskienhallinnan kannalta on oleellista tunnistaa datan arvo yritykselle sen mukaan, kuinka suuret vahingot koituvat, mikäli tiedot vuotavat ulkopuolisille. Tietomurtojen yritykseen kohdistuvaa taloudellista riskiä voidaan lähteä arvioimaan kaavan $riski = kustannukset * tapahtuman\ todennäköisyys$ mukaisesti. Yritykseen kohdistuvan tietomurron todennäköisyyttä on kuitenkin hyvin vaikeaa lähteä määrittämään, mutta niistä aiheutuvia kustannuksia on kuitenkin mahdollista arvioida. Tietomurrosta aiheutuvat kokonaiskustannukset yritykselle saadaan laskettua kaavalla $kustannukset = suorat\ kustannukset + epäsuorat\ kustannukset$. [13]

Tietomurroista aiheutuvien kustannuksien laskennassa tulee ottaa huomioon niistä aiheutuvat suorat sekä epäsuorat kustannukset yritykselle. Suoriin kustannuksiin kuuluvat esimerkiksi seuraavat asiat:

1. tietomurron mahdollistaneen käytännön, sovelluksen, järjestelmän tai muun verkon haavoittuvuuden tutkiminen
2. henkilöstökustannukset uusien tietoturvakäytäntöjen ja -strategioiden suunnittelusta, käyttöönotosta ja ylläpidosta

3. tietomurrosta aiheutuneet datan saatavuuteen liittyvät kustannukset
4. kadonneen tai käyttökelvottoman datan palauttaminen
5. asiakkaisiin kohdistuvasta tiedotus- ja suhdetoiminnasta aiheutuvat kulut
6. mahdolliset oikeudenkäyntikulut
7. asiakkaille maksetut korvaukset
8. kilpailijoiden saama etu luottamuksellisesta datasta
9. luottoluokituksen lasku
10. vakuutusmaksujen kasvu. [13]

Vastaavasti epäsuorat kustannukset voivat koostua muun muassa seuraavista asioista:

1. yrityksen maineen kokemat tappiot: nykyisten ja potentiaalisten asiakkaiden menettäminen, tuotemerkin arvon vähentyminen
2. henkilöstön kokema lisääntynyt stressi
3. henkilöstön vaihtuvuudesta koituvat kustannukset
4. kohonnut riski tietomurron toistumiseen
5. varastettujen henkilötietojen käyttö identiteettivarkauksissa
6. tietosuojalakien ja -asetusten rikkomisesta aiheutuvat syytteet. [13]

Arvioimalla käsiteltävää dataa ja siihen kohdistuvan mahdollisen tietomurron aiheuttamia kustannuksia yritys voi arvioida, kuinka suuria investointeja luottamuksellisen datan turvaamiseen on järkevää käyttää. Lopullisten kustannuksien määrä riippuu paljolti siitä, millaista dataa yritys käsittelee ja kuinka paljon sitä on. Yrityksen koko vaikuttaa siis merkittävästi lopullisten kokonaiskustannusten määrään, mutta on kuitenkin otettava huomioon aiheutuvien kustannusten vaikutus yrityksen normaaliin toimintaan. Pienet yritykset voivat kärsiä tietomurron aiheuttamista kustannuksista huomattavasti enemmän, vaikka ne olisivatkin rahamäärällisesti pienemmät.

3.3 Riskien tunnistaminen ja uhkatekijät

Tietomurtoihin liittyvien riskien ymmärtämiseksi yrityksen tulee olla tietoinen siitä, mistä suunnasta riski luottamuksellista dataa kohtaan syntyy. Tietomurtoihin liittyviä osapuolia ja motivaatioita käsiteltiin jo aiemmin luvussa 2. Tarkastellaan nyt tarkemmin, millaisia uhkatekijöitä tietomurtoihin liittyy ja miten niitä voidaan pyrkiä hallitsemaan.

Yrityksen käsittelemää dataa kohtaan liittyvät tietomurtoihin johtavat uhkatekijät voidaan jaotella sisäisiin ja ulkoisiin uhkatekijöihin. Datan luottamuksellisuutta uhkaavat sisäiset uhkatekijät koostuvat yrityksen luottamien osapuolien toiminnasta. Näitä luotettuja osapuolia voivat olla yrityksen omien työntekijöiden lisäksi esimerkiksi alihankkijat, yhteistyökumppanit ja vierailijat. Kaikkia yrityksen verkossa toimivia ja sen dataa käsitteleviä osapuolia voidaan pitää sisäisinä uhkatekijöinä.

Sisäisten uhkatekijöiden luomat riskit tietomurtoihin koostuvat enimmäkseen tahattomasti aiheutetuista tilanteista, kuten työntekijöiden tekemistä virheistä, mutta luotetut osapuolet voivat vuotaa tietoja ulkopuolisten käsiin myös tarkoituksella. Tietomurtojen sisäisten uhkatekijöiden taustalla voivat olla esimerkiksi yrityksen huonot tietoturvakäytännöt tai datan käsittelijöiden huolimattomuus. Pahaa tahtovat työntekijät voivat aiheuttaa paljon vahinkoa yritykselle, sillä työntekijöillä on pääsy suuren määrään dataa, he tietävät mitä dataa on saatavilla, tunnistavat sen arvon ja heidän toimintansa ei yleensä ole tarkkailun alaisena. [11]

Tietomurtoihin liittyvät ulkoiset uhkatekijät koostuvat eri tyyppisistä hyökkäyksistä, joita käsiteltiin jo luvussa 2. Ulkoisten uhkatekijöiden aiheuttamia tietomurtoriskejä voidaan pyrkiä tunnistamaan tarkemmin, kun tiedetään tarkasti, mitä kautta mahdollinen tietomurto voisi tapahtua. Yksittäisten ulkoisten hyökkääjien ennalta tunnistaminen on käytännössä mahdotonta, mutta eri tyyppisiä hyökkäyksiä voidaan tutkia ja selvittää, kuinka todennäköisesti ne voisivat kohdistua omaan yritykseen. Yrityksen tarjoamien palveluiden mahdolliset haavoittuvuudet tulee kartoittaa, ja pyrkiä tunnistamaan, millaiset hyökkäykset niihin voisivat vaikuttaa. Tärkeää on myös tunnistaa, millaista dataa eri palveluissa käsitellään. Lisäksi tulee olla tietoinen siitä, mitä ulkoisia palveluita yritys käyttää liiketoiminnassaan ja kuinka riskialttiiksi ne tekevät käsiteltävät tiedot.

3.4 Uhilta suojautuminen

Minimoidakseen tietomurtojen mukanaan tuoman riskin yrityksen tulee suunnitella datan käsittelyyn turvatoimet niin, että tietomurtoihin liittyvien uhkien tapahtumatodennäköisyys on mahdollisimman pieni. Yrityksen datan hallintaan liittyvät tietoturvaratkaisut voidaan jakaa niiden toteutuksen vaikeuden, toteuttajan ja kustannusten perusteella kolmelle eri tasolle: perustason, keskitason ja edistyneen tason suojaustoimiin [14]. Eri tasoja sekä niihin liittyviä tietoturvaratkaisuja on havainnollistettu kuvassa 2.

Kuva 2. *Tietomurtojen suojaustoimet* ***[14]****.*

Perustason suojaustoimet koostuvat nimensä mukaisesti yleisimmistä, toteutukseltaan yksinkertaisimmista ja edullisimmista tietoturvaratkaisuista. Perustason suojaustoimiin kuuluvat kaikki yksinkertaisimmat hyökkääjien torjumiseen suunnitellut järjestelmät sekä yrityksen sisäiset datan käsittelyyn liittyvät tietoturvakäytännöt.

Huolehtimalla hyvien tietoturvakäytäntöjen laatimisesta ja niiden noudattamisesta vähennetään riskiä sekä sisäisten että ulkoisten uhkatekijöiden kannalta. Käytännöt voivat liittyä esimerkiksi pääsynhallintaan tai itse datan käsittelyyn. Pitämällä huolta pääsynhallinnasta luottamuksellisiin tietoihin vähennetään sekä tahallisesti että tahattomasti aiheutettujen tietovuotojen riskiä yrityksen sisällä. Yrityksen tulee olla tietoinen, kuka pääsee käsiksi luottamukselliseen dataan, ja rajoittaa pääsy vain sitä tarvitseville osapuolille. On myös oleellista, että datan käsittelystä tiedetään, miten ja missä se tapahtuu. Yrityksen tulee luoda selkeät ohjeet luottamuksellisen datan käsittelyyn sen työntekijöille, muuten uhkana voi olla esimerkiksi datan käsittelyyn käytettyjen laitteiden hukkaaminen tai varastaminen. Tämä on nykyään entistä tärkeämpää, kun työtä tehdään yhä enemmän etänä ja eri tyyppisillä mobiililaitteilla.

Perustasolla hyökkääjien torjuntaan kuuluvat virustorjuntaohjelmat, palomuurit, tunkeilijoiden havaitsemisjärjestelmät (engl. intrusion detection system) sekä suojeltavan datan salaus [14]. Virustorjuntaohjelmat tarkkailevat järjestelmää ja huolehtivat haittaohjelmien havaitsemisesta sekä niiden poistamisesta. Palomuurin tehtävänä on suojella yrityksen sisäistä verkkoa ulkopuolisilta hyökkääjiltä tarkkailemalla ulkoa päin tulevia yhteyksiä ja

sallimalla läpi vain luotetut osapuolet samalla estäen epäilyttävät yhteydet. Tunkeilijoiden havaitsemisjärjestelmät tarkkailevat kaikkea liikennettä yrityksen sisäverkon ja ulkoverkon (internet) välillä, pitävät kirjaa verkkoliikenteestä sekä varoittavat epäilyttävistä tapahtumista [14].

Edellä mainitut järjestelmät pyrkivät estämään tietomurron tapahtumisen. Datan salauksella pyritään hallitsemaan tietomurroista aiheutuvaa riskiä salaamalla luottamukselliset tiedot niin, että onnistuneenkaan hyökkäyksen tapauksessa ei ole todennäköistä, että hyökkääjä kykenee käyttämään varastamiaan tietoja. Datan salaukseen on olemassa eri tyyppisiä salausalgoritmeja. Yrityksen tulee olla tietoinen siitä, miten vahva käytössä oleva salaus on, sillä salausalgoritmit kehittyvät jatkuvasti, kun vanhoja algoritmeja murretaan ja korvataan uusilla.

Perustasolla tarvittavat järjestelmät voivat olla ilmaisohjelmia, laitehankintojen mukana tulleita ohjelmia tai erikseen ostettuja tietoturvatuotteita. Yleisesti ottaen perustason suojaustoimien käyttöönotosta ja ylläpidosta huolehtii yritys itse, ja säännöllisten päivitysten kautta ne muodostavat riittävän suojan ulkopuolisia hyökkääjiä kohtaan [14].

Keskitason suojaustoimet ovat perustasoa monimutkaisempia ja niiden tarpeellisuus korostuu erityisesti yrityksissä, joissa datan käsittelyyn liittyvät tottumukset ovat huolenaihe. Keskitason suojaustoimet ovat erityisesti suunnattuja suuremmille yrityksille, ja ne pitävät huolen siitä, että edes jonkin asteinen suojaus toteutuu koko yrityksessä. Keskitason järjestelmiin kuuluvat esimerkiksi tietovuotojen havaitsemiseen ja estämiseen suunnitellut DLP-ohjelmistot (engl. data loss prevention) sekä kevyet asiakaspäätteet (engl. thin client). [14]

Kuva 3. *DLP-ohjelmisto valvoo kaikkea datan käsittelyä yrityksessä: siirtoa, käyttöä ja varastointia* ***[15]****.*

DLP-ohjelmistot ovat suurempia tietoturvaohjelmistoja, joiden tehtävä on tarkkailla ja ohjata kaikkea yrityksessä tapahtuvaa datan käsittelyä. Ohjelmisto kykenee analysoimaan datan siirtoa, käyttöä sekä varastointia. DLP-ratkaisut kykenevät tarkkailemaan kaikkien verkossa toimivien käyttäjien toimintaa sekä estämään luottamuksellisen datan kopioinnin ja jakamisen. [15] Siinä missä palomuurin tehtävänä on suojata dataa sisäverkon ulkopuolisilta toimijoilta, DLP-ohjelmisto suojaa dataa myös yrityksen verkossa toimivien luotettujen osapuolien toiminnalta. DLP-ratkaisuiden toiminnot vaihtelevat, mutta ohjelmisto pystyy esimerkiksi tunnistamaan suojausta vaativat tiedostot, seuraamaan datan kopiointia ulkoisille tiedontallennusvälineille sekä analysoimaan eri tiedonsiirtomenetelmien ja -protokollien käyttöä. [14] DLP-ohjelmiston toimintaa esitetty myös kuvassa 3.

Kevyet asiakaspäätteet ovat pienen laskentatehon tietokoneita tai ohjelmistoja, jotka tarjoavat käyttäjälle suuren laskentatehon ja pääsyn suureen määrään dataa ja toimintoja yhdistämällä erilliseen palvelimeen. Kevyiden asiakaspäätteiden avulla luottamuksellista dataa voidaan käsitellä missä tahansa ilman, että sitä joudutaan siirtämään pois hyvin

suojatusta ympäristöstä. [14] Kevyiden asiakaspäätteiden käytöllä kadonneet ja varastetut laitteet eivät aiheuta tietomurtoriskiä, sillä data ei sijaitse laitteella ja yhdistäminen palvelimeen vaatii vahvan tunnistautumisen.

Keskitason suojaustoimenpiteiden toteuttajana toimii yleensä alaan erikoistunut palveluntarjoaja [14]. Asiakasyritykset maksavat käyttämistään palveluista ja eivät joudu huolehtimaan monimutkaisten tietoturvaratkaisujen ylläpidosta.

Edistyneiksi datan suojaustoimenpiteiksi voidaan luokitella normaaleista tietoturvaratkaisuista poikkeavat toimenpiteet, joihin investoimalla yritykset pyrkivät vielä paremmin turvaamaan palveluidensa tietoturvallisuuden. Tällaisiin toimenpiteisiin kuuluvat esimerkiksi aktivismi ja penetraatiotestaus. [14]

Aktivismilla ja penetraatiotestauksella tarkoitetaan yksityisten hyvää tahtovien hakkereiden suorittamia eettisiä tietomurtoja. Hakkerit löytävät haavoittuvuuksia järjestelmästä, jotka he ilmoittavat järjestelmän ylläpitäjälle. Ilmoituksen saatuaan ylläpitäjä suorittaa tarvittavat korjaustoimenpiteet palvelun tietoturvan parantamiseksi. Hakkerit voivat suorittaa eettisiä tietomurtoja omillaan tai yritykset voivat kannustaa tähän esimerkiksi palkkiota vastaan.

Tässä luvussa esitettyjen tietoturvaratkaisuihin painottuvien suojaustoimenpiteiden lisäksi yritys voi pyrkiä vähentämään tietomurroista koituvaa riskiä myös muilla keinoin. Riskiä voidaan hallita esimerkiksi vakuuttamalla data ulkopuolisilta hyökkääjiltä tai huolehtimalla työympäristöstä sekä työntekijöiden tyytyväisyydestä. Luotettuja osapuolia voivat motivoida tietomurtoihin esimerkiksi tyytymättömyys palkkatasoon ja työilmapiiriin, jotka voivat johtaa tietojen vuotamiseen, myymiseen eteenpäin tai viemiseen uuteen työpaikkaan [11].

3.5 Tietomurrosta toipuminen

Tietomurron kohdistuessa omaan yritykseen on oltava valmis sen mukana tuleviin haasteisiin. Tietomurtoon voidaan varautua ennalta luomalla selkeä suunnitelma tapahtuman vaatimista toimenpiteistä. Tietomurtoon reagointi ja siitä toipuminen koostuvat monista eri askeleista, joihin kuuluvat vähintäänkin tietomurron pysäyttäminen, menetetyn datan tutkiminen, tappioiden arviointi, asiakkaiden huomauttaminen, sekä uusien tietomurtojen estäminen.

Ensimmäisenä askeleena on tutkittava, pääsevätkö tietomurron aiheuttaneet hyökkääjät tai muut ulkopuoliset tahot edelleen käsiksi luottamukselliseen dataan. Riippuen tietomurron tyypistä vahingoittuvuudet voivat olla edelleen olemassa ja hyökkäys jatkua vielä sen jälkeenkin, kun se on ensimmäisen kerran huomattu. Hyökkäys on syytä pysäyttää

heti, kun se huomataan. Tarvittaessa hyökkäyksen kohdistamat palvelut voidaan sulkea, kunnes hyökkäyksen mahdollistaneet haavoittuvuudet on korjattu.

Tietomurron pysäyttämisen jälkeen seuraavina askeleina tutkitaan, mitä dataa menetettiin ja aletaan arvioida tappioita. Menetettyä dataa tulee tutkia ja selvittää tarkasti, millaista tietoa päätyi ulkopuolisten käsiin. Asiakkaita koskevien tietojen tapauksessa selvitetään, kuinka suuresta asiakasmäärästä on kysymys. Tutkitaan myös, mikä oli tietomurron tapahtumaketju, jotta voidaan lähteä arvioimaan murron mahdollistaneita järjestelmiä ja käytäntöjä. Tappioiden arvioinnissa tulee ottaa huomioon suuri määrä eri kustannuksia, joita käsiteltiin jo aiemmin luvussa 3.2.

Asiakkaiden huomauttaminen on tärkeä osa tietomurtoon reagointia. Eri puolilla maailmaa on määritelty erilaisia luottamuksellisen datan käsittelyyn ja tietomurtoihin liittyviä sääntöjä. Euroopan unionissa sijaitseva tai siellä toimintaansa harjoittava yritys on voimassa olevan yleisen tietosuoja-asetuksen mukaan velvoitettu ilmoittamaan kaikkia tietomurron koskettamia asiakkaita henkilökohtaisen datansa vuotamisesta ulkopuolisten käsiin. Tietosuoja-asetuksen laajan henkilökohtaisen datan määritelmän sekä verkkopalvelujen kansainvälisyyden takia tämä koskettaa lähestulkoon kaikkia verkossa toimintaansa harjoittavia yrityksiä. Tiivistettynä voidaan sanoa, että asetus määrittelee henkilökohtaiseksi dataksi kaiken datan, joka voidaan millään tavalla yhdistää olemassa olevaan henkilöön. [1]

Viimeisenä tärkeänä askeleena tulee arvioida yleisesti tietomurron aiheuttaneita taustatekijöitä ja pyrkiä parantamaan nykyistä järjestelmää niin, että tulevaisuudessa ollaan paremmin varauduttu tietomurtoja kohtaan. Tähän voi kuulua esimerkiksi uusien järjestelmien käyttöönotto, tietoturvaan erikoistuneen henkilöstön palkkaaminen, yrityksen yleisten tietoturvakäytäntöjen parantaminen tai henkilöstön kouluttaminen tietoturva-asioissa. Kun tietomurrosta on kunnolla selvitty, voidaan tehdä vielä selvä arvio siitä aiheutuneista kustannuksista ja siihen reagoinnista, jotta ollaan varmasti varauduttu uusien tietomurtojen varalta.

4 TARGET CORPORATION -TIETOMURTO

Eräs merkittävimmistä ja maailmanlaajuisesti uutisoiduimmista tietomurroista on vuoden 2013 lopulla tapahtunut murto, jonka kohteena oli yhdysvaltalainen vähittäiskauppaketju Target Corporation. Tietomurrossa hyökkääjät saivat haltuunsa merkittävät määrät asiakastietoja sekä maksukorttidataa. Tietomurron takana ollut hyökkäys koostui monesta eri vaiheesta, ja siihen reagointiin liittyi monia virheitä kohdeyrityksen puolelta, joiden takia sen seuraukset olivat huomattavasti suuremmat kuin ne olisivat olleet seuraamalla hyviä tietoturvakäytäntöjä. Tässä luvussa käydään läpi tietomurron yksityiskohtia liittyen tapahtuneeseen hyökkäykseen, sen seurauksiin sekä tietomurtoon reagointiin.

4.1 Hyökkäys

Target Corporation ei ole vahvistanut tarkkoja tietoja hyökkäyksen etenemisestä, mutta yleisesti hyväksytyn teorian mukaan tietomurto alkoi hyökkäyksellä Targetin käyttämää ilmastointitekniikkaan erikoistunutta urakoitsijaa Fazio Mechanical Servicesiä kohtaan. Hyökkääjät kohdistivat sähköpostin välityksellä tapahtuvan tietojenkalasteluhyökkäyksen Faziota kohtaan, minkä seurauksena hyökkääjät pääsivät asentamaan haittaohjelmia urakoitsijan käyttämiin järjestelmiin. [16]

Osana yritysten yhteistyötä heidän käytössään oli Targetin käyttämä hankintajärjestelmä, joka oli yksi osa suurempaa Targetin liiketoimintaa mahdollistavien järjestelmien kokonaisuutta. Hyökkääjien saastutettua Fazion järjestelmät he saivat annettua niille komentoja ja pääsivät käsiksi kaikkiin heille tarkoitettuihin Targetin palveluihin. Targetin käyttämän heikon verkon segmentoinnin takia ulkoisten urakoitsijoiden käyttöön tarkoitettujen palveluiden kautta hyökkääjät pääsivät käsiksi myös kaikkiin verkkoon yhdistettyihin järjestelmiin. [16]

Hyökkääjät tunnistivat verkossa toimivat haittaohjelmille alttiit luottamuksellista dataa käsittelevät järjestelmät, joihin kuuluivat muun muassa yksittäisten myyntipisteiden maksukortinlukijat. Seuraavana osana hyökkäystä yksittäisille maksukortinlukijoille asennettiin haittaohjelma, joka pystyi lukemaan laitteen keskusmuistia. Normaalisti asiakkaan maksaessa kortilla lukija ottaa yhteyden ulkopuoliseen palveluun, joka käsittelee maksuvahvistuksen. Maksuvahvistuksien käsittelyyn liittyvään dataan kuuluvat muun muassa kortin numero, kortinhaltijan nimi sekä voimassaoloaika. Kaikki tämä data käsitellään nor-

maalisti salattuna, mutta laitteen sisäisessä keskusmuistissa se sijaitsee ilman minkäänlaista suojausta. [17] Kortinlukijaan asennettu haittaohjelma tarkkaili keskusmuistia ja tallensi sitä käyttäneiden asiakkaiden maksukorttitiedot.

Hyökkääjät salasivat haittaohjelman keräämät maksukorttitiedot ja siirsivät ne muille Targetin verkossa sijaitseville saastuttamilleen laitteille. Tietomurron aikana hyökkääjät saivat luotua käyttäjätunnukset Targetin sisäisessä verkossa toimiville palvelimille. Päivän aikana maksupäätteen haittaohjelma lähetti kerätyt maksukorttitiedot lähimmälle hyökkääjän hallinnassa olevalle palvelimelle, joka välitti niitä muille saastutetuille laitteille ja lähetti ne lopulta myös ulos Targetin verkosta palvelimille eri puolilla maailmaa. Lopulta varastetut tiedot päätyivät Venäjällä sijaitsevalle palvelimelle, johon hyökkääjät saivat kerättyä 11 gigatavua maksukorttidataa marraskuun ja joulukuun 2013 aikana. [16] Hyökkäyksen eteneminen on vielä esitetty kuvassa 4.

Kuva 4. *Target Corporation -tietomurron vaiheet* ***[16]****.*

Tietomurron takana olevia osapuolia ei ole tunnistettu, mutta tietojen lopullisen sijainnin perusteella hyökkääjien on ajateltu olevan peräisin Itä-Euroopasta tai Venäjältä. Tietomurrolla kerättyä dataa on yritetty myydä eteenpäin nimimerkillä Rescator, mutta ei ole varmaa tietoa, miten myyjä on yhteydessä tietomurtoon [16]. Tietomurtoon käytetyn haittaohjelman kehitykseen käytetyn testausohjelmiston kehittänyt henkilö tuomittiin 14 vuoden vankeuteen vuonna 2018. Target on vaatinut korvauksia testausohjelmiston kehittäjältä tietomurtoon liittyen. [18]

4.2 Seuraukset

Target Corporationiin kohdistuneessa tietomurrossa miljoonien asiakkaiden tiedot päätyivät ulkopuolisten käsiin. Hyökkääjät saivat käsiinsä jopa 40 miljoonan henkilön maksukorttitiedot maksupäätteille asennettujen haittaohjelmien avulla. Näiden lisäksi jopa 70 miljoonan asiakkaan henkilökohtaisia tietoja päätyi ulkopuolisten käsiin. Henkilökohtaisten tietojen joukossa oli nimiä, osoitteita, puhelinnumeroita sekä sähköpostiosoitteita. [19]

Vuoden 2014 alussa Target arvioi tietomurron aiheuttaneiksi kustannuksiksi 61 miljoonaa dollaria. Ulkopuolisten lähteiden tekemät arviot liittyen pelkästään maksukorttidatan menetyksestä johtuviin luvattomiin maksutapahtumiin vaihtelivat 240 miljoonan dollarin ja 2,2 miljardin dollarin välillä. [19] Tietomurron seurauksena Targetin toimitusjohtaja Gregg Steinhafel joutui eroamaan tehtävistään ja Target lupasi parantaa tietoturvallisuuttaan 100 miljoonan dollarin investoinneilla [16]. Target on ollut myös jatkuvien oikeudenkäyntien alaisena tietomurrosta asti. Targetille tietomurrosta aiheutuneet kokonaiskustannukset kasvavat edelleen, sillä eri osapuolien nostamat kanteet tuottavat yritykselle jatkuvia oikeudenkäyntikuluja ja korvaustenmaksua. Targetia vastaan kohdistuneissa oikeudenkäynneissä on ollut mukana muun muassa finanssialan palveluja, Yhdysvaltain osavaltiota sekä, erityisesti ryhmäkanteiden muodossa, suuria määriä Targetin asiakkaita. Kahdeksan kuukauden kuluttua tietomurrosta Targetia kohtaan kohdistuneiksi kustannuksiksi ilmoitettiin 236 miljoonaa dollaria, joista yrityksen vakuutukset korvasivat 90 miljoonaa dollaria. Targetin maine, tulos sekä osakekurssi kärsivät myös lyhytaikaisia seurauksia tietomurtoon liittyen. [20]

Asiakkaiden kokemat seuraukset Targetin tietomurtoon liittyvät paljolti maksukorttitietojen menetykseen ja sen tuomiin vaikeuksiin, mutta merkittävä riski piilee myös muiden henkilötietojen menetyksessä. Tietomurron seurauksena miljoonat asiakkaat joutuivat tarkkailemaan maksukorteillaan tehtyjä ostoksia sekä uusimaan olemassa olevia maksukortteja. Lisäksi tietomurron uhrina olleiden asiakkaiden henkilötietoja voidaan vieläkin käyttää identiteettivarkauden merkeissä.

Target ei ole ainut yritys, joka kärsi tapahtuneesta tietomurrosta. Maksukortteihin liittyvät sopimukset sitovat seurauksiin mukaan myös luottoyhtiöt ja pankit. Myös ulkopuolisen urakoitsijan rooli tietomurrossa vaikeuttaa kokonaiskustannusten laskentaa. Kaikki nämä osapuolet ovat tavalla tai toisella kytkettynä asiakkaiden kokemiin seurauksiin ja kokevat

myös itse haittavaikutuksia, kun asiakkaat vaativat korvauksia tietomurtoon liittyen. Tyypillisesti maksukortin myöntäjä joutuu kustantamaan korttien uusimisen sekä korvaamaan korteilla tehdyt luvattomat ostokset. [19]

4.3 Tietomurtoon reagointi ja sen estäminen

Tietomurron onnistumiseen ja lopullisen seurausten suuruuteen vaikuttivat merkittävästi Targetin tekemät virheet tietoturvajärjestelmien suunnittelussa ja niiden käytössä. Tietomurtoon johtaneista virheistä merkittävimmät liittyivät verkon suunnitteluun, välittämättömyyteen tietoturvavaroituksia kohtaan sekä maksupäätelaitteiden turvaamiseen [16].

Targetin tekemät virheet alkoivat verkon suunnittelusta. Targetin verkkoa ei ollut segmentoitu osiin vaan kaikki laitteet sijaitsivat samassa verkossa riippumatta siitä, kuinka riskialttiita laitteet olivat mahdollisille hyökkäyksille. Targetin verkkoarkkitehtuuri oli suunniteltu yleisen mallin mukaan, jossa pyritään rakentamaan mahdollisimman hyvä suojaus pitämään ulkopuoliset osapuolet verkon ulkopuolella. Tällaisessa ratkaisussa verkon sisäisistä tietoturvaratkaisuista voidaan tinkiä, sillä kaikki käyttäjät ovat luotettuja. Yhdessä segmentoinnin puute sekä käytetty suunnittelumalli mahdollistivat sen, että hyökkääjät pääsivät saastuttamaan merkittävän määrän verkossa toimivia laitteita. [16]

Targetin käyttämät strategiat verkon suunnittelussa ovat vieläkin käytössä monissa yrityksissä. Tällaisessa verkossa luotettujen käyttäjien tunnusten väärinkäyttö on jatkuva riski, jonka vuoksi on kehitetty vastakohtainen malli, jossa kaikkia verkossa toimivia osapuolia pidetään epäluotettavina. Zero Trust -mallissa kaikkea verkossa tapahtuvaa liikennettä valvotaan ja näin pystytään suojaamaan verkossa sijaitsevaa dataa tehokkaasti sekä ulkopuolisilta että sisäisiltä uhkatekijöiltä. [16]

Target oli tietoinen ulkopuolisten hyökkääjien tuomista riskeistä ja olikin panostanut merkittävästi tietoturvaratkaisuihin tietomurtojen estämiseksi. Targetin käytössä oli useampia tietoturvaratkaisuja datan turvaamiseksi, kuten useita erillisiä palomuureja, haittaohjelmien havaitsemiseen ja poistamiseen käytettyjä työkaluja sekä tunkeutumisen havainnointiin ja estoon tarkoitettuja ohjelmia [17].

Merkittävistä investoinneista huolimatta tietomurtoa ei pystytty estämään, sillä Targetin tietoturvajärjestelmien tuottamia varoituksia hyökkääjien toiminnasta ei huomioitu millään tavalla. Haittaohjelmatyökaluille ovat tyypillisiä väärät varoitukset, joiksi Targetin tietoturva-ammattilaiset tulkitsivat myös hyökkääjien toiminnasta aiheutuneet varoitukset. [16] Targetin käytössä olleet työkalut olisivat pystyneet myös poistamaan haittaohjelmat automaattisesti, mutta tämä ominaisuus oli otettu pois käytöstä, koska sen oli todettu hidastavan sähköpostin ja internetin käyttöä [17].

Ensimmäisenä ilmenneet hyökkääjien asentamista haittaohjelmista aiheutuneet varoitukset eivät olleet ainoat varoitukset, jotka jäivät Targetin työntekijöiltä huomioimatta. Tietoturvajärjestelmät tuottivat varoituksia myös hyökkääjien ryhtyessä siirtämään dataa ulos Targetin verkosta. [16] Näistäkään varoituksista ei välitetty. Huomioimalla saadut varoitukset tietomurto olisi mahdollisesti voitu pysäyttää jo aikaisessa vaiheessa, ja siitä aiheutuneet seuraukset oltaisiin voitu minimoida.

Tietomurto oltaisiin voitu mahdollisesti kokonaan estää paremmalla pääsynhallinnalla, joka olisi rajoittanut Fazio Mechanical Servicesin tunnusten oikeuksia Targetin verkossa. Toinen asia, jolla tietomurto olisi voitu estää jo alkuvaiheessa, olisi ollut alkuperäisen tietojenkalasteluhyökkäyksen onnistumisen estäminen. Riittävällä tietoturvakoulutuksella ja työntekijöiden tietoisuudella tietojenkalasteluhyökkäyksistä hyökkääjät eivät olisi saaneet tietomurtoon tarvitsemiansa tunnuksia. Käytössä olisi voinut myös olla jonkin tyyppinen kaksivaiheinen tunnistautuminen, jotta hyökkääjät eivät olisi pystyneet hyödyntämään varastamiaan tunnuksia.

Edellä mainittujen asioiden lisäksi paremmat tietoturvaratkaisut maksupäätelaitteissa olisivat auttaneet tietomurron estämisessä. Maksukorttidataa keräävät haittaohjelmat oltaisiin voitu estää käyttämällä maksupäätteissä listaa sallituista prosesseista, jolloin hyökkääjien käyttämät haittaohjelmat eivät olisivat päässeet toimimaan lainkaan [16].

5 YHTEENVETO

Tietomurtoja tapahtuu jatkuvasti ja niihin liittyvät hyökkäykset, kohteet sekä hyökkääjät ja heidän motivaatiot vaihtelevat paljon. Työssä tutustuttiin yrityksiä uhkaaviin tietomurtoihin ja esitettiin, kuinka niiden tuomaa riskiä voidaan pyrkiä hallitsemaan.

Työssä tietomurtoihin liittyvät hyökkäykset jaoteltiin verkon välityksellä tapahtuviin ja hyökkääjän fyysisten toimenpiteiden avulla tapahtuviin hyökkäyksiin, joista verkon kautta tapahtuvien hyökkäysten todettiin olevan huomattavasti yleisempiä. Verkon välityksellä tapahtuvista hyökkäyksistä käytiin läpi yleisimmät, joiksi osoittautuivat SQL-injektiot, tietojenkalastelu sekä haittaohjelmat. Haittaohjelmista esiteltiin useimmiten esiintyviä, joihin kuuluivat Command and Control -hyökkäykset, kiristyshaittaohjelmat sekä vakoiluohjelmat.

Yritykseen kohdistuvan tietomurtojen uhan todettiin kohdistuvan todennäköisimmin sen ulkopuolelta ja hyökkääjän olevan useimmiten taloudellisesti motivoitunut. Tietomurtojen kohteiden todettiin vaihtelevan, mutta yleisimmin onnistuneen tietomurron kohteena todettiin olevan yksityinen pienyritys.

Tietomurtoihin liittyvien yksityiskohtien jälkeen tutkittiin niihin liittyvää riskienhallintaa. Yritysten tulee tunnistaa, mitä dataa sillä on käsiteltävänä sekä millaisia suojaustoimenpiteitä se vaatii. Yrityksen suojeltava data koostuu sekä asiakkaiden tiedoista että sen omasta liiketoimintaa mahdollistavasta datasta. Tietomurtojen aiheuttamaa taloudellista riskiä voidaan arvioida siitä koituvien kustannuksien avulla. Yrityksen tulee ottaa huomioon niistä aiheutuvat suorat kustannukset, kuten tietoturvan parantaminen ja asiakkaille maksetut korvaukset, sekä epäsuorat kustannukset, kuten yrityksen maineen kokemat vauriot. Tuntemalla, miten tietomurtoja tapahtuu ja tunnistamalla yrityksen sisä- ja ulkopuolelta muodostuvat uhkatekijät, voidaan niiltä pyrkiä suojautumaan. Käsiteltävän datan määrän ja arvon perusteella voidaan arvioida tietoturvaan tarvittavia investointeja ja ottaa käyttöön eri tasoisia suojaustoimia tietomurtoriskin hallintaa varten.

LÄHTEET

[1] European Commission, General Data Protection Regulation, 2016. Saatavissa: https://gdpr-info.eu/ (Viitattu 3.11.2019)

[2] Rikoslaki, Luku 38, 8§ (10.4.2015/368). Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001 (Viitattu 3.11.2019)

[3] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, A. Rashid, Data exfiltration: A review of external attack vectors and countermeasures, Journal of Network and Computer Applications, Vol.101, 2018, pp. 18–54.

[4] Verizon, 2019 Data Breach Investigations Report, 2019. Saatavissa: https://enterprise.verizon.com/resources/reports/dbir/ (Viitattu 9.9.2019)

[5] J. Clarke, SQL Injection Attacks And Defense, Elsevier, 2012.

[6] Viestintävirasto, Tietoturvan Vuosi 2018, 2019. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf (Viitattu 3.11.2019)

[7] Palo Alto Networks Inc., Command-and-Control Explained. Saatavissa: https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained (Viitattu 8.10.2019)

[8] A. Liska, T. Gallo, Ransomware, O'Reilly Media, Inc, 2016.

[9] S. Sagiroglu, G. Canbek, Keyloggers, IEEE Technology and Society Magazine, Vol.28, No.3, 2009, pp. 10–17.

[10] McAfee, Grand Theft Data, 2017. Saatavissa: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf (Viitattu 14.10.2019)

[11] G. Bunker, G. Fraser-King, Data Leaks For Dummies, For Dummies, 2009.

[12] Yahoo! Inc., Yahoo 2013 Account Security Update FAQs. Saatavissa: https://help.yahoo.com/kb/account/SLN28451.html. (Viitattu 29.10.2019).

[13] R. Layton, P. Watters, A methodology for estimating the tangible cost of data breaches, Journal of Information Security and Applications, Vol.19, No.6, 2014, pp. 321–330.

[14] C. Phua, Protecting organisations from personal data breaches, Computer Fraud & Security, Vol.2009, No.1, 2009, pp. 13–18.

[15] S. Alneyadi, E. Sithirasenan, V. Muthukkumarasamy, A survey on data leakage prevention systems, Journal of Network and Computer Applications, Vol.62, 2016, pp. 137–152.

[16] X. Shu, K. Tian, A. Ciambrone, D. Yao, Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, Computer Research Repository, 2017.

[17] N. Manworren, J. Letwat, O. Daily, Why you should care about the Target data breach, Business Horizons, Vol.59, No.3, 2016, pp. 257–266.

[18] R. Weiner, Hacker linked to Target data breach gets 14 years in prison, The Washington Post, 21.9.2018. Saatavissa: https://www.washingtonpost.com/local/public-safety/hacker-linked-to-target-data-breach-gets-14-years-in-prison/2018/09/21/839fd6b0-bd17-11e8-b7d2-0773aa1e33da_story.html (Viitattu 20.10.2019)

[19] M. Hardy, Target Store Data Breaches : Examination and Insight, Nova Science Publishers, Inc., 2014.

[20] B. Ives, Targeting Target with a 100 million dollar data breach, Journal of Information and Technology Teaching Cases, Vol.8, No.1, 2018, pp. 9–23.