Miro Rihu

Tietomurtojen juurisyyt ja vaikutusten minimointi

Tietotekniikan kandidaatintutkielma

15. joulukuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Miro Rihu

Yhteystiedot: miro.rihu@outlook.com

Ohjaaja: Timo Tiihonen

Työn nimi: Tietomurtojen juurisyyt ja vaikutusten minimointi

Title in English: Root causes of data breaches and the mitigation of their effects

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 26+0

Tiivistelmä: Tietomurtojen estäminen on monimutkainen ja haastava ongelma. Tietomurtojen juurisyistä tehdään vuosittaista tutkimusta, jonka avulla voidaan mm. pysyä kartalla erilaisten kyberhyökkäysten trendeistä. Viime vuosina käyttäjätunnukset, ja niihin liittyvien haasteiden merkitys on ollut suuri aihepiirin sisällä. Kuitenkin monia muita juurisyitä on olemassa ja pienetkin virheet esimerkiksi pilvipalveluiden asetuksissa voi johtaa hyväksikäytettävien haavoittuvuuksien luontiin. Paljon on kuitenkin tehtävissä mahdollisuuksien ja vaikutusten pienentämiseen, esimerkiksi ns. Zero Trust arkkitehtuurin käyttöönotolla ja tunkeilijoiden havaitsemisjärjestelmien avulla.

Avainsanat: Tietomurto, Tietovuoto, Hyökkäysvektori, Juurisyy, Käyttäjätunnukset, Tietomurtojen vaikutukset, Tietomurtojen vaikutusten minimointi

Abstract: The prevention of data breaches is a complex and difficult problem to solve. The root causes of data breaches are under annual research, which can be used to, i.e., stay informed about the yearly trends of different kinds of cyberattacks. Within the past few years, user credentials, and the challenges associated with them, have played a major role within the scope of the subject. However, multiple other root causes exist and, for example, even the slightest mistakes during the configuration of cloud services, can lead to the creation of an exploitable vulnerability. However, much can be done to lessen the effects and the possibility of data breaches by i.e., conducting penetration testing or incorporating network-based

intrusion detection systems.

Keywords: Data breach, Data leak, Attack vector, Root cause, User credentials, The effects of data breaches, Data breach effect mitigation

Sisällys

1 JOHDANTO 1

2 YLEISTÄ TIETOMURROISTA 2
2.1 Tietovuoto ja tietomurto 2
2.2 Tietomurto 2
2.3 Motivaatiot vuotojen takana 3
2.4 Tietomurtojen vaikutukset 5
2.4.1 Ensisijaiset vaikutukset 5
2.4.2 Toissijaiset vaikutukset 6

3 YLEISET HYÖKKÄYSVEKTORIT 8
3.1 Varastetut ja vaarantuneet käyttäjätiedot 8
3.2 Tietojenkalastelu 10
3.3 Pilvipalveluiden virheelliset asetukset 10
3.4 Kolmannen osapuolen sovellukset 11
3.5 Sisäpiirin uhat 12

4 TIETOMURTOJEN ESTÄMINEN JA VAIKUTUSTEN MINIMOINTI 14
4.1 Valmistautuvat toimenpiteet 14
4.1.1 Zero-Trust 14
4.1.2 Penetraatiotestaus 15
4.1.3 Tunkeilijan havaitsemisjärjestelmät 15
4.2 Tietomurtoon vastaaminen 16
4.3 Murron jälkeiset toimenpiteet 16

5 YHTEENVETO 17

LÄHTEET 18

1 Johdanto

Tietomurrot koskettavat vuosittain jopa miljardeja ihmisiä ja aiheuttavat yhteiskunnalle merkittävää taloudellista haittaa. Pelkästään Yhdysvalloissa raportoitiin vuonna 2021, 1789 eri kohteisiin kohdistuvaa tietomurtoa (ITRC 2022, s. 6—7). Tuoreimman tutkimuksen mukaan, vuoden 2022 aikana yksittäisen tietomurron kustannuksen maailmanlaajuinen keskiarvo on noussut 2,6 prosenttia vuodesta 2021, tuoden maailmanlaajuisen keskimääräisen kustannuksen arvion 4,35 miljoonaan dollariin tietomurtoa kohden (IBM 2022, s. 5).

Tämän kandidaatintutkielman tarkoituksena on tarkemmin tutustua ja kartoittaa tietomurtojen erilaisia mahdollistavia tekijöitä, ja samalla selvittää tapoja estää ja minimoida tietomurtojen vaikutuksia. Tutkielma suoritetaan kirjallisuuskatsauksena. Aihepiirin valtavan laajuuden vuoksi, hyökkäysvektorien ja tietomurtoihin varautumiseen käytettyjen työkalujen ja menetelmien määrää on kuitenkin jouduttu rajaamaan merkittävästi.

Aiheen laadun ja liiketaloudellisen merkityksen vuoksi, kattavaa julkista tieteellistä lähdekirjallisuutta, on vaikea löytää. Valtava osa yksittäisiin organisaatioihin kohdistuneista hyökkäyksistä tulee julki lehtiartikkeleiden kautta, ja tarkat syyt murron taustalla jäävät usein julkisuudelta pimentoon. Kuitenkin anonyymit tilannekatsaukset antavat hyvää kuvaa tämänhetkisestä tilanteesta. Tämän lisäksi alaa johtavat organisaatiot, kuten F-Secure, ovat hyviä lähteitä yleisen käsityksen saamiseksi tietomurtojen takana olevista juurisyistä, kuten tietojenkalastelusta ja siltä suojautumisesta.

Tutkielmassa käydään ensin läpi yleisiä asioita tietomurroista, kuten tietomurtojen määritelmiä, motiiveja ja liiketoiminnallisia vaikutuksia. Tämän jälkeen tarkastellaan hyökkäysvektoreita yleisellä tasolla ja katsotaan vektorien aiheuttamien kustannuksien ohella niiden viimeaikaisia kehityksellisiä trendejä. Lopuksi katsotaan tietomurtojen estämisen ja vaikutusten minimoinnin keinoja, kuten miten varautua tietomurtoihin, mitä tehdä tietomurron sattuessa ja miten toimia tietomurron jälkeen.

2 Yleistä tietomurroista

Tietomurtojen ja tietovuotojen käsitteisiin löytyy monia erilaisia määritelmiä, ja käsitteitä käytetään usein synonyymeinä keskenään. Tässä luvussa käydään läpi molempien käsitteiden määritelmät.

2.1 Tietovuoto ja tietomurto

Sanalla tietovuoto (engl. *data leak*) tarkoitetaan tahallista tai tahatonta arkaluontoisen tiedon vuotoa kolmannelle osapuolelle (Raman, Kayacık ja Somayaji 2011, s. 1). Sanaa tietovuoto käytetään yleisesti synonyyminä tietomurrolle, mutta termeillä on kuitenkin eroa (F-Secure 2022b).

Tietomurto yleensä johtaa tietovuotoon, mutta tietovuoto voi myös tapahtua tahattomasti erinäisten syiden takia, jolloin lakia ei rikota (F-Secure 2022b; Kost 2022; Ledesma 2022). Esimerkiksi väärin konfiguroitu tietokanta voi mahdollisesti näyttää suojeltua dataa julkisesti. Tämä on yksi esimerkki tahattomasta tietovuodosta (Ledesma 2022). Tietomurto yleensä edellyttää jonkinlaisen kyberhyökkäyksen käyttöä tiedon saamista varten, jolloin tietovuodossa saatu informaatio on otettu voimakeinoin (F-Secure 2022b; Kost 2022). Tietovuodon informaatio on täten saatu tietomurrolla.

Tässä tutkielmassa keskitytään enemmänkin rangaistavaan tietomurtoon, mahdollisesti tahattoman tietovuodon sijaan. Molemmissa tapauksissa lopputulos on vuotaneen tiedon näkökulmasta sama, mutta tietomurron takana on aktiivinen ja motivoitunut tekijä. Tämä kasvattaa väärinkäytön riskiä oleellisesti ja täten on perusteltua keskittyä erityisesti tahalliseen tekoon.

2.2 Tietomurto

Sanalle tietomurto (engl. *data breach*) löytyy monta eri määritelmää. Tässä tutkielmassa keskitytään enemmän itse käsitteeseen toisin kuin varsinaiseen tekoon. Määritelmiä on seuraavanlaisia:

Suomen voimassa olevan rikoslain mukaan tietomurtoon syyllistyy hän, "joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan"(Rikoslaki 1889/39, Luku 38 § 8).

Yhdysvaltojen terveys- ja sosiaalipalveluministeriö määrittelee tietomurron olevan "tietoturvaloukkaus, jossa arkaluontoista, suojattua tai luottamuksellista dataa kopioidaan, siirretään, katsotaan, varastetaan tai käytetään valtuuttamattoman henkilön toimesta. Lisäksi kaikenlainen luvaton asiakkaiden datan levittäminen tietojärjestelmään sisäänpääsyyn valtuutetun henkilökuntaan kuuluvan toimesta voidaan myös luokitella tietomurroksi."(USHHS 2015, s. 2 suomennos minun)

Lyhykäisyydessään tietomurrolla tarkoitetaan tekoa, jossa valtuuttamaton henkilö pääsee kyberhyökkäyksellä käsiksi tietoihin tai dataan, johon hänellä ei ole oikeuksia (Rikoslaki 1889/39; F-Secure 2022b), tai tekoa, jossa valtuutettu henkilö tahallisesti levittää ulkopuolisille kuulumatonta dataa (USHHS 2015, s. 2). Koska tietomurron suorittamiseen vaaditaan tahallinen teko, on se rangaistavaa suomen rikoslain mukaan. Tekijä voidaankin tuomita joko sakkorangaistukseen tai enintään 2 vuoden vankeustuomioon (Rikoslaki 1889/39, Luku 38 § 8).

2.3 Motivaatiot vuotojen takana

Tässä osiossa käsitellään yleisimpiä motivaatioita kyberhyökkäyksien takana. Tietomurrot ovat yleensä kyberhyökkäysten avulla tuotettuja tietovuotoja (F-Secure 2022b), jonka takia niiden takana olevat motiivit kuuluvat yleisesti kyberhyökkäysten motiivien joukkoon.

Rahallisen hyödyn tavoitteleminen on ylivoimaisesti suurin syy kyberhyökkäysten takana. Yli 50 prosentissa vuonna 2020 tapahtuneista tietomurroista oli taustalla rahallisen hyödyn tavoitteleminen (IBM 2020). Esimerkiksi teollisuusvakoilu on yksi tapa hyötyä hyökkäyksestä rahallisesti. Hyökkääjä yrittää saada käsiinsä jonkin organisaation aineetonta omaisuutta ja myydä sitä organisaation kilpailijoille (Gupta ja Mata-Toledo 2016, s. 5). Reaalimaailman esimerkki rahallisen hyödyn tavoittelevasta tietomurrosta on vuonna 2013 tapahtunut

Myspace-verkkosivuston tietomurto, jossa hyökkääjä ilmoitti myyvänsä tietomurrosta saatua dataa kuudella bitcoinilla kenelle tahansa (VICE 2016).

Valtiolliset motivaatiot ovat myös yksi syy kyberhyökkäyksille. Yksi viime vuosikymmenen kohutuimmista alan uutisista oli, kun Edward Snowden paljasti Yhdysvaltain kansallisen turvallisuusviranomaisen, NSA:n, keräävän salaa tietoa kansalaisistaan teleoperaattoreiden (Guardian 2013) ja verkkopalveluntarjoajien kautta. Lisäksi kävi ilmi, että NSA itse suorittaa kyberhyökkäyksiä maailmanlaajuisesti (BBC 2014). Tietomurtojen kohdalla valtiolliset tekijät kattoivat 13 prosenttia vuonna 2020 (IBM 2020, s. 38).

Muitakin kuin pelkästään rahallisia ja valtiollisia motivaatioita on kuitenkin olemassa. Esimerkiksi vuonna 2011 tapahtuneen Sony Entertainmentin tietomurron takana olevan LulzSec hakkerijärjestön motivaatiot hyökkäykseen eivät vaikuttaneet olevat rahallisesti motivoituneita, eivätkä he myöskään olleet valtiollisia tekijöitä (Brito 2011). Heidän motivaatioitansa on kuvailtu pikemminkin anarkistisina tai nihilistisinä (Bonner 2012, s. 9). Toisen hyvin tunnetun hakkerijärjestön Anonymousin motivaatiot ovat taas olleet poliittisia. He ovat esimerkiksi hyökänneet mm. PayPalin, Master Cardin ja Visan kimppuun, osoittaakseen tukensa WikiLeaks-nettisivuston kehittäjälle, Julian Assagnelle. Poliittisesti motivoituneita hyökkäyksiä kutsutaan haktivismiksi (BBC 2012; TIME 2010). Vuonna 2020 haktivismin osuus tietomurroissa oli 13 prosentin luokkaa (IBM 2020, s. 38).

Kuitenkaan kaikki kyberhyökkäykset eivät ole motiiveiltaan haitallisia. Hakkerit voidaankin jakaa kolmeen ryhmään motiivien perusteella. Mustahattuisiin, jotka harrastavat rikollista toimintaa ja valkohattuisiin, jotka käyttävät kyberhyökkäyksiä esimerkiksi tietojärjestelmien haavoittuvuuksien löytämiseen ja paikkaamiseen. Valkohattuiset hakkerit ovat yleensä ulkoisia tietoturvaeksperttejä, jotka pyrkivät ilmoittamaan asiakkailleen järjestelmien haavoittuvuuksista ja riskeistä esimerkiksi penetraatiotestauksen avulla. Tärkeä seikka valkohattuisten hakkereiden kohdalla on, että kohdeorganisaatio on antanut heille luvan hyökätä heidän järjestelmäänsä, kuitenkin sopimuksen puitteissa (Weidman 2014, s. 2—3; Harper ym. 2022, s. 3—6). Musta- ja valkohattuisten hakkereiden välimaastossa operoivat harmaahattuiset hakkerit, jotka hakkeroivat eettisin keinoin tahallista haittaa aiheuttamatta. Harmaahattuiset hakkerit eivät välttämättä ole kenenkään palkkaamia, vaan murtautuvat järjestelmiin esimerkiksi yleisen turvallisuuden edistämiseksi (Harper ym. 2022, s. 3—6). Kuitenkin tämä luvaton tun-

keutuminen luokitellaan lain mukaan tietomurroksi, ja on täten laitonta (Rikoslaki 1889/39, Luku 38 § 8).

2.4 Tietomurtojen vaikutukset

Tietomurrot aiheuttavat erilaisia haittavaikutuksia, ja samalla valtavia kustannuksia yrityksille ja organisaatioille. Vaikutukset voidaankin jakaa ensisijaisiin ja toissijaisiin vaikutuksiin. Ensisijaisiin vaikutuksiin kuuluu mm. suorat kustannukset, jotka aiheutuvat tietomurtoihin varautumisesta ja niihin vastaamisesta. Toissijaisiin vaikutuksiin taas kuuluu esimerkiksi mahdolliset sanktiot ja identiteettivarkaudet, jotka tulevat mahdollisiksi vuodetun datan avulla. Seuraavaksi tarkastellaan näitä ensi- ja toissijaisia vaikutuksia syvällisemmin.

2.4.1 Ensisijaiset vaikutukset

Tietomurrosta aiheutuvat ensisijaiset kustannukset voidaan jakaa neljään osaa. Kustannuksia syntyy, menetetystä liiketoiminta, murtojen havaitsemisesta ja toimenpiteiden aloittamisesta, murron ilmoittamisesta, sekä murron jälkeisistä toimenpiteistä. (IBM 2022, s. 12).

Suurin kustannus syntyy tietomurron ennaltaehkäisevistä, havaitsemisen mahdollistavista ja murron jälkeisistä korjaavista toimenpiteistä, kuten murron tutkinnasta, järjestelmien auditoinnista ja kriisinhallinnan tiimin johtamisesta. Nämä kustannukset kattavat nykyisin yli 33 prosenttia kokonaiskustannuksista (IBM 2022, s. 12).

Toiseksi suurin kustannus syntyy menetetystä liiketoiminnasta, joka johtuu esimerkiksi järjestelmän alhaalla olosta, asiakkuuksien menetyksestä ja uusien asiakkuuksien hankinnasta. Menetetyn liiketoiminnan kustannukset ovat olleet tyypillisesti suurimmat tietomurroista aiheutuvat kustannukset, mutta vuonna 2022 murtojen havaitsemisen ja toimenpiteiden aloittamisen kustannukset nousivat edellä mainittuja kustannuksia korkeammiksi. Kuitenkin menetetyn liiketoiminnan osio kustannuksista liikkuu 32-33 prosentin välillä (IBM 2022, s. 12; 2019, s. 12).

Kolmanneksi suurin kustannus syntyy murron jälkeisistä toimenpiteistä, jotka ovat suurimmaksi osaksi toissijaisia kustannuksia. Murron jälkeisten toimenpiteiden kustannukset vievät

27 prosenttia kokonaiskustannuksista. Pienin tietomurroista syntyvä kustannus syntyy murron ilmoittamisesta, joka sisältää kaiken viestinnän eri sidosryhmien välillä. Ilmoittamisen kustannukset kattaa noin 7 prosenttia kokonaiskustannuksista (IBM 2022, s. 12).

Vuonna 2022 yhden tietomurron globaali keskimääräinen kustannus oli 4,35 miljoonaa dollaria, ja Yhdysvalloissa keskiarvo on 9,44 miljoonaa dollaria, joka oli 9,04 miljoonaa vuonna 2021 (IBM 2022, s. 9—10). Vuonna 2021 tapahtui 1789 yksittäiseen yritykseen kohdistuvaa tietomurtoa Yhdysvalloissa (ITRC 2022, s. 7). Vuotuinen kustannus pelkästään Yhdysvalloissa siis liikkuu kymmenissä miljardeissa.

2.4.2 Toissijaiset vaikutukset

Vuodessa sadat miljoonat joutuvat tietomurtojen sivullisiksi uhreiksi, jolloin heidän henkilötietonsa vuotavat julkiseksi (ITRC 2022, s. 6). Lähes kaikissa vuoden 2021 Yhdysvalloissa tapahtuneissa tietomurroissa vuoti henkilöiden nimet, yli 60 prosentissa täydet henkilötunnukset ja yli kolmasosassa vuoti syntymäpäivät. Harvinaisempia, mutta kuitenkin suhteellisen yleisiä vuodettuja henkilötietoja olivat kotiosoitteet, terveystiedot, ajokortit, pankkitiedot, puhelinnumerot ja täydet pankkikorttitiedot (ITRC 2022, s. 13).

Näiden vuodettujen henkilötietojen avulla rikolliset voivat tehdä identiteettivarkauksia, jossa rikollinen kerää mahdollisimman paljon dataa henkilöstä, ja käyttää tätä dataa omaan hyötyyn (ITRC 2022, s. 3). Kuitenkin identiteettivarkaus on suomen rikoslain alla pelkästään sakolla rangaistava teko (Rikoslaki 1889/39, Luku 38 § 9a).

Tietomurtojen kohteille aiheutuvat kustannukset ovat merkittäviä, ja tämä näkyy osittain myös asiakkaille. IBM Securityn tutkimuksen mukaan 60 prosenttia vastanneista organisaatioista kertoi joutuneensa nostamaan tuotteiden- ja palveluidensa hintoja tietomurron jälkeen (IBM 2022, s. 13).

Tietomurroista voi aiheutua myös oikeudellisia seuraamuksia uhrille. Mikäli käy ilmi, että jotain tietynlaista luottamuksellista dataa on käsitelty väärällä tavalla, voi dataa käsittelevä organisaatio syyllistyä esimerkiksi henkilötietojen kohdalla tietosuojarikoksiin (Raman, Kayacık ja Somayaji 2011, s. 1). Tämä johtaa suomen nykyisen lainsäädännön mukaan joko sakkorangaistukseen, tai enintään vuoden vankeustuomioon (Rikoslaki 1889/39, Luku 38 §

9). Organisaatioita voidaan myös pitää vastuussa esimerkiksi tietomurrossa levinneistä korttitiedoista. Lisäksi liikesalaisuuksien leviäminen voi johtaa liiketoiminnan menetykseen ja ajaa pahimmillaan koko yrityksen konkurssiin (Raman, Kayacık ja Somayaji 2011, s. 1).

3 Yleiset hyökkäysvektorit

Tietomurtojen takana on yleensä jokin kyberhyökkäys. Vuonna 2021 Yhdysvalloissa tapahtuneista 1789 tietomurrosta, yli 90 prosenttia tapahtui jonkin kyberhyökkäyksen avulla, oli se sitten esimerkiksi tietojenkalastelun (engl. *Phishing*), tai haittaohjelman ansiota (ITRC 2022, s. 6—7).

Vuoden 2021—2022 kaikista hyökkäyksistä 75 prosenttia voidaan jakaa viiteen hyökkäysvektoriin Ne ovat järjestyksessä yleisimmästä harvinaisimpaan, varastetut ja vaarantuneet käyttäjätiedot, tietojenkalastelu, pilvipalveluiden virheelliset asetukset, kolmannen osapuolen sovellusten haavoittuvuudet ja organisaation sisäiset uhat. (IBM 2022, s. 17) Tässä tutkielmassa tarkastellaan kyseisten hyökkäysvektorien määritelmien lisäksi niiden historiallista asemaa viimeaikaisissa kehitystrendeissä.

3.1 Varastetut ja vaarantuneet käyttäjätiedot

Viimeisen kolmen vuoden aikana vaarantuneiden käyttäjätietojen osuus hyökkäysvektoreista on liikkunut 19—20 prosentin välillä, ja tietojenkalastelu sisällytettynä, kirjautumistietojen osuus hyökkäysvektoreista kattaa yli kolmasosan kaikista hyökkäyksistä.

Käyttäjätietojen vaarantumiseen ja varastamiseen on monia eri syitä ja tapoja, kuten erilaiset haittaohjelmat, käyttäjätietokantojen tietovuodot ja tietojenkalastelu (Thomas ym. 2017, s. 2).

Yksinkertaisuutensa ansiosta salasanat ovat vieläkin yksi suosituimmista käytössä olevista tunnistautumismenetelmistä, monista vioistaan huolimatta (Bošnjak, Sreš ja Brumen 2018). Kuitenkin nykyään laajasti käytössä olevat kaksivaiheiset todennuspalvelut, kuten Googlen Authenticator-sovellus, pyrkivät parempaan tietoturvallisuuteen vaatimalla käyttäjältä toissijaisen tunnisteen antamista (Dmitrienko ym. 2014, s. 1).

Käyttäjätietokantojen vuodot johtaa pahimmillaan satojen miljoonien käyttäjätunnusten vaarantumiseen, kun käyttäjänimi ja salasana parit löytyvät vuodoista. Esimerkiksi Myspacen kuuluisa tietomurto, joka johti yli 360 miljoonan käyttäjän tunnusten vaarantumiseen, kun

tiedot vuodettiin ilman salausta (Thomas ym. 2017, s. 2—4; VICE 2016). Vuodossa vaarantuvat salasanat voivat olla joko salattuja yhdellä tai useammalla salausalgoritmilla, tai salaamattomia salasanoja selväkielisessä muodossa, riippuen vuodon kohteen toimintatavoista. (Thomas ym. 2017, s. 2)

Nämä vuodetut salasanat voidaan murtaa salasananmurtotyökaluja käyttämällä esimerkiksi väkisin jokaista kombinaatiota kokeillen, tai sanalistoja hyödyntävillä, sanakirja hyökkäyksillä (Bošnjak, Sreš ja Brumen 2018, s. 2—3). Internetissä on avoimesti löydettävissä useita salasananmurtotyökaluja, kuten Hashcat, John the Ripper ja Brutus. Selväkielisessä muodossa olevia vuodettuja salasanoja ei luonnollisesti salauksen puutteen takia tarvitse murtaa.

Käyttäjätunnusten uudelleenkäyttö on suuri ongelma. Se on ongelmallista, sillä yhteen tietojärjestelmään kohdistuva tietovuoto vaarantaa käyttäjätunnukset useammassa paikassa. Kuitenkin käyttäjien kasvavan käyttäjätunnusten määrän takia, iso osa käyttäjistä turvautuu käyttäjätunnusten uudelleenkäyttämiseen (Das ym. 2014, s. 1).

Dasin tutkimuksessa käy ilmi, että 43 prosenttia tutkimuksessa olevista käyttäjätunnuksien salasanoista oli toistensa kanssa identtisiä, ja 19 prosenttia oli helposti alkuperäiseksi muokattavissa eri palveluiden välillä. Lisäksi 77 prosenttia kyselyyn vastanneista tutkimukseen osallistuneista uudelleenkäyttäisi, tai hiukan muokkaisi samaa salasanaa uuden käyttäjän luonnissa. (Das ym. 2014, s. 4—6)

Muulla, kuin tietojenkalastelulla varastettujen käyttäjätietojen aiheuttamien tietomurtojen kustannukset ovat pienentyneet viime vuosien aikana, ja ovat nykyään tietojenkalastelun kustannuksia keskimääräisesti alhaisemmat. Vuonna 2022 tällä tavalla saatujen käyttäjätietojen aiheuttamien tietomurtojen kustannukset olivat keskimäärin 4,5 miljoonaa dollaria verrattuna tietojenkalastelun 4,91 miljoonaan dollariin. Vaarantuneiden tai varastettujen käyttäjätietojen huomaamiseen ja uhkaan vastaamiseen menee kuitenkin kaikista hyökkäysvektoreista eniten aikaa. Keskimääräinen aika tapahtumasta hallintaan on noin 327 päivää (IBM 2022, s. 17; 2021, s. 20; 2020, s. 36).

3.2 Tietojenkalastelu

Tietojenkalastelu (engl. *Phishing*) on tapa, jonka avulla varastetaan käyttäjätietojen lisäksi muita henkilötietoja, kuten nimiä, puhelinnumeroita ja pankkitunnuksia (F-Secure 2022a). Tietojenkalastelu rajoittuu pääsääntöisesti huijaussähköposteihin ja valheellisiin verkkosivuihin, mutta hyökkäyksistä on myös olemassa eri variaatioita, kuten tekstiviesteillä tapahtuvat "Smishing", puhelimitse tapahtuvat "Vishing"ja kohdennetut "Spear Phishing"hyökkäykset (F-Secure 2022a).

Tietojenkalasteluun on olemassa valmiita paketteja, joihin on integroitu automaattisia toiminnallisuuksia varastettujen tietojen raportointiin ja validointiin. Näitä kutsutaan "Phishing Kiteiksi". Ne mahdollistavat nopean hyökkäyksen luonnin, ja jotkin niistä sisältävät yksityiskohtaiset käyttöohjeet. (Cova, Kruegel ja Vigna 2008, s. 1—2; Thomas ym. 2017, s. 7) Kitit voivat kerätä kirjautumistietojen lisäksi myös muita tunnistautumis- ja henkilötietoja, kuten laite ja sijaintitietoja, joka voi mahdollistaa lisäturvajärjestelyjen päihittämisen (Thomas ym. 2017, s. 7). Verrattuna satunnaisiin käyttäjiin, tietojenkalastelun uhrit ovat yli 400 kertaa suuremmassa riskissä joutua käyttäjäntietojen varastamisen ja väärinkäytön uhriksi (Thomas ym. 2017, s. 9—10). Kuitenkin hyökkäyksen onnistuminen vaati käyttäjän tekevän mitä hyökkääjät haluavat, ja antavan kirjautumistiedot hyökkääjille (F-Secure 2022a).

Vuonna 2022 keskimääräinen maailmanlaajuinen kustannus tietojenkalastelun aiheuttamalle tietomurrolle oli 4,91 miljoonaa dollaria tietomurtoa kohden, ja tietojenkalastelu on toiseksi suurin hyökkäysvektori varastettujen ja vaarantuneiden käyttäjätietojen jälkeen. Tietojenkalastelun onnistumisen huomaaminen ja siihen vastaaminen kestää keskimäärin noin 300 päivää, ja tietojenkalastelu hyökkäysten määrä ja niiden aiheuttamat kustannukset ovat olleet viime vuodet nousussa. Vuonna 2022 hyökkäysten määrä kuitenkin laski prosentilla verrattuna aikaisempaan vuoteen. Vuonna 2021 tietojenkalastelu nousi toiseksi suurimmaksi hyökkäysvektoriksi (IBM 2022, s. 17—18; 2021, s. 20; 2020, s. 36—37).

3.3 Pilvipalveluiden virheelliset asetukset

Kolmanneksi suurin hyökkäysvektori tietomurtojen yhteydessä, on pilvipalveluiden virheellinen konfiguraatio, joka kattaa noin 15 prosenttia kaikista hyökkäyksistä (IBM 2022, s. 17).

Jokaisen heterogeenisen verkon tärkein prosessi on verkon konfigurointi (Wood ja Pereira 2011, s. 3). Järjestelmän konfiguroinnilla tarkoitetaan järjestelmän asetusten säätöä (Suomisanakirja 2022). Virheellinen konfiguraatio voi johtua monesta eri syistä, joista yksi yleisimmistä on vääränlaiset lähestymistavat konfigurointiin. Yleisesti käytetyt työkalut eivät välttämättä toimi tehokkaasti laajoihin ja monimutkaisiin skaalautuviin järjestelmiin. Vaikka järjestelmä voisikin toimia normaalisti, sen tehokkuus kärsii, tai se avaa mahdollisuuden kyberhyökkäyksille. Syistä riippumatta virheelliset asetukset kasvattavat riskiä järjestelmän käyttökatkoille ja kyberhyökkäyksille (Wood ja Pereira 2011, s. 3—5). Tehokkaan muutoksenhallinnan (engl. *change control*) puute on myös yksi syy, joka voi johtaa virheelliseen konfiguraatioon (Roza ym. 2019, s. 10).

Yleisiä hyökkäyksen kohteita ovat suojaamattomat dataa säilyttävät elementit tai kokoelmat, liialliset oikeudet, oletuskäyttäjätunnukset ja konfiguroimattomat pilvipalvelut, ja pilvipalvelut, joissa yleiset turvavalvontatoimenpiteet (engl. *security controls*) on jätetty pois päältä (Roza ym. 2019, s. 10).

Keskimääräinen maailmanlaajuinen kustannus pilvipalveluun kohdistuneen hyökkäyksen aiheuttamalle tietomurrolle oli 4,14 miljoonaa dollaria tietomurtoa kohden vuonna 2022, ja hinta on hyökkäysten frekvenssin kanssa laskenut viime vuosina. Vielä vuonna 2020, kyseiset hyökkäykset olivat yhtä yleisiä käyttäjätietojen kanssa. Onnistumisen huomaaminen ja siihen vastaaminen kestää keskimäärin 244 päivää, ja ovat keskimäärin toiseksi nopeimmat vektorit vastata (IBM 2022, s. 17—18; 2021, s. 20; 2020, s. 36—37).

3.4 Kolmannen osapuolen sovellukset

Neljänneksi yleisimmän hyökkäysvektorin paikan 13 prosentin osuudella ottaa haavoittuvuudet kolmannen osapuolen sovelluksissa (IBM 2022, s. 17).

Sovelluksissa on luonnostaan haavoittuvuuksia (Shahzad, Shafiq ja Liu 2012, s. 1). Haavoittuvuudet mahdollistavat erilaisten kyberhyökkäysten suorittamisen, jotka johtavat mm. tietovuotoihin (Zeng ym. 2020, s. 1). Kansainvälinen, yhteisöön perustuva, *Common Vulnerabilities and Exporures*, eli CVE hanke, on tietokanta johon kirjataan ylös yleisiä sovellushaavoittuvuuksia. Tällä hetkellä (10.11.2022) tietokannasta löytyy 188300 vapaasti haettavaa

CVE dokumenttia. (CVE 2022a)

Yksi kolmannen osapuolen sovelluksen haavoittuvuuden esimerkki löytyy suositusta Mojangin kehittämästä tietokonepelistä, Minecraftista. Minecraftin Java versiossa löydettiin haavoittuvuus, joka mahdollisti hyökkääjän ajaa mitä tahansa koodia muiden pelaajien tietokoneilla (PCMagazine 2022). Haavoittuvuus oli peräisin Java ohjelmointikielelle tehdystä Apachen log4j kirjastosta, jota käytetään lokitiedostojen kirjoittamiseen. Katsottaessa CVE tietokantaa, voidaan löytää dokumentteja, jotka varoittavat kyseisen kirjaston eri versioiden mahdollisuudesta ajaa haitallista koodia (CVE 2022b). Myös Apache (2022) varoittaa tästä mahdollisuudesta log4j kirjaston sivuilla. Tämä johti siihen, että Mojangin (2022) oli vastattava tietoturvariskiin antamalla pelaajille ohjeet, miten toimia tietokoneensa turvaamiseksi. Kuitenkin, koska log4j on Java pohjainen kirjasto, sen vaikutukset eivät rajaudu pelkästään Minecraftiin, vaan kaikkiin kyseistä kirjastoa käyttäviin sovelluksiin.

Vuonna 2022 keskiarvoinen kustannus kolmannen osapuolen haavoittuvuuksien aiheuttamalle tietomurrolle oli 4,55 miljoonaa dollaria. Vuosittainen määrä on ollut tasaisessa laskussa viimeisen kolmen vuoden aikana, mutta kustannukset vaihtelevat vuosittain 4,3—4,7 miljoonan dollarin välillä. Onnistuneeseen hyökkäykseen vastaaminen kestää keskimäärin 284 päivää haavoittuvuuksien osalta (IBM 2022, s. 17—18; 2021, s. 20; 2020, s. 36—37).

3.5 Sisäpiirin uhat

Viidenneksi suurin, ja tässä tutkielmassa viimeinen tarkastelun kohde on organisaation sisäiset uhat. Sisäisten uhkien osuus hyökkäysvektoreissa on noin 11—12 prosentin luokkaa (IBM 2022, s. 17). Sisäpiirin uhat voivat johtaa aineettoman omaisuuden menetykseen, ja järjestelmien käyttökatkokset aiheuttavat yrityksille kustannuksia (Roza ym. 2019, s. 22).

Sisäpiirin uhkalla tarkoitetaan "nykyistä tai entistä työntekijää, urakoitsijaa, tai toista liikekumppania, jolla on tai oli valtuutettu sisäänpääsy organisaation verkkoon, järjestelmiin tai dataan, ja ketä tahallisesti ylitti tai väärinkäytti valtuuksia tavalla, joka vaikutti haitallisesti organisaation tietojen, datan tai tietojärjestelmien luottamuksellisuuteen, eheyteen, tai saatavuuteen. Lisäksi sisäpiirin uhka voi myös olla tahaton."(CERT 2017, s. 6, suomennos minun).

Suurin osa sisäpiirissä tapahtuneista rikoksista jakautuu neljään kategoriaan. IT sabotaasiin, aineettoman omaisuuden varastamiseen, petokseen ja vakoiluun. Vuonna 2011 tehdyssä tutkimuksessa tarkastelluista IT sabotaasitapauksista, joista tiedettiin ajat ja paikat, yli puolet ajoittuvat yleisen työajan ulkopuolelle, ja tapahtuvat etäyhteyden välityksellä. Vain 34 prosenttia rikoksista tapahtui työpaikalla, ja 42 prosenttia tapahtui työaikana (CERT 2011, s.4—6).

Kuitenkin vuonna 2018 tapahtuneista sisäpiirin hyökkäyksistä, 64 prosenttia johtui työntekijän tai urakoitsijan vahingosta. kaikista hyökkäyksistä 36 prosenttia johtui oikeasti rikoksesta, ja näistä 23 prosenttia johtui haitallisesta sisäpiiriläisestä. hyökkäyksistä 13 prosenttia johtui käyttäjätietojen varastamisesta (Ponemon-Institute 2018, s. 7).

Sisäpiirin uhat kustansivat keskimäärin 4,18 miljoonaa dollaria hyökkäystä kohden vuonna 2022. Hyökkäysten osuus hyökkäysvektoreista on ollut tasaisessa nousussa, ja kustannukset vaihtelevat vuosittain 4,0—4,7 miljoonan dollarin välillä. Hyökkäyksen huomaamisen ja siihen vastaamiseen kulunut aika on keskimäärin 284 päivää. (IBM 2022; 2021; 2020, s. 17—18, 20, 36—37)

4 Tietomurtojen estäminen ja vaikutusten minimointi

Tietomurtojen estämisen ja vaikutusten minimoinnin hyvien käytäntöjen päätoimenpiteet on jaettu kolmeen luokkaan: Tietomurtoon valmistautuvat toimenpiteet, tietomurtoon vastaaminen ja tietomurron jälkeiset toimenpiteet (USHHS 2015, s. 2—6).

Laajuutensa ansiosta, tässä tutkielmassa käydään läpi vain murto-osa tietomurtojen estämisen ja vaikutusten minimoinnin aihepiiristä. Jokaisen aihepiirin tärkeimmät toimenpiteet käydään kuitenkin läpi pääpiirteittäin.

4.1 Valmistautuvat toimenpiteet

Yhdysvaltojen terveys- ja sosiaalipalveluministeriön ohjeistuksen mukaan valmistautuva toimenpiteet ovat: Järjestelmän, pätevien lakien, riskien ja uhkien arviointi, organisaatiotason menetelmien, Tietomurron vastaussuunnitelman ja tietosuojaselosteen laadinta, sekä työntekijöiden kouluttaminen ja turvatarkistusten toteutuksen jatkuva valvonta (USHHS 2015, s. 2—4).

Tietomurtoon valmistautuvien toimenpiteiden toteuttamiseen löytyy monia erilaisia työkaluja ja menetelmiä, kuten: Zero-Trust arkkitehtuuri, penetraatiotestaus ja tunkeilijan havaitsemisjärjestelmät. Jokaisella menetelmällä ja työkalulla on oma tehtävänsä turvallisuuden kokonaisuuden rakentamisessa.

4.1.1 Zero-Trust

Zero trust on verkkoturvallisuuden paradigma, jossa jokainen käyttäjä luokitellaan mahdolliseksi hyökkääjäksi, eikä heihin ikinä luoteta implisiittisesti. Lähestymistapa kattaa mm. kyttäjätunnukset, käyttöoikeuksien hallinnan ja isännöinti ympäristöt. Järjestelmä, joka toimii Zero Trust periaatteella, evaluoi käyttäjän yhteyttä jatkuvasti, ja päättää käyttäjän oikeudesta käyttää verkkoa mm. tämän fyysisen sijainnin ja kaksinkertaisen tunnistautumisen avulla (WatchGuard 2021; Rose ym. 2020, s. 4).

Zero trust arkkitehtuurin perusperiaatteiden mukaan kaikki datan lähteet ja laskenta palvelut

ovat resursseja, kaikki kommunikointi on turvattua verkon sijainnista riippumatta ja yksittäisten resurssien käyttöoikeus annetaan sessioperusteisesti. Käyttöoikeus määritellään dynaamisesti käyttäjän tietojen perusteella, eikä yhteenkään resurssiin luoteta, vaan kaikkista tarkistetaan eheys ja turvallisuus resurssipyyntöjen yhteydessä. Samalla varmistetaan käyttäjän oikeus resurssiin dynaamisella ja ankaralla tavalla. Lopuksi resurssien tilasta, verkon infrastruktuurista ja kommunikaatiosta kerätään dataa, jota käytetään turvallisuuden parantamiseen (Rose ym. 2020, s. 6—7).

4.1.2 Penetraatiotestaus

Penetraatiotestaus on tapa etsiä haavoittuvuuksia ja kartoittaa hyökkäysten riskejä. Se jakautuu yhdeksään osaan: Alustavaan vaiheeseen, tiedon keruuseen, uhkien mallintamiseen, haavoittuvuuksien analysointiin, haavoittuvuuksien hyödyntämiseen, hyökkäyksen jälkeisiin toimenpiteisiin, raportointiin, tiivistelmään ja tekniseen raporttiin (Weidman 2014, s. 1—6).

Penetraatiotestauksen tärkein vaihe on alustava vaihe. Alustavassa vaiheessa käydään läpi kaikki tärkeimmät testin seikat asiakkaan kanssa, kuten mm. testauksen suorittamisen ajat, testauksen laajuus ja testauksen lupa-asiat (Weidman 2014, s. 2—4).

Tämän jälkeen aloitetaan testaus, jossa ensin kerätään vapaasti saatavaa tietoa kohteesta, luodaan hyökkäys strategioita, etsitään haavoittuvuuksia ja käytetään löydettyjä haavoittuvuuksia toteuttamaan hyökkäyssuunnitelma. Kun testi on suoritettu, kerrotaan havainnot asiakkaalle ja luodaan tiivistelmä ja tekninen raportti penetraatiotestistä (Weidman 2014, s. 4—6).

4.1.3 Tunkeilijan havaitsemisjärjestelmät

Tunkeilijan havaitsemisjärjestelmät ovat sovelluksia, jotka tarkkailevat verkkoa epäilyttävien tekojen tai käyttäytymismallien varalta. Järjestelmä sijaitsee yleensä verkon laidalla, jossa se suorittaa pakettien syvätutkimusta. Järjestelmä vertaa läpi kulkevaa verkkoliikennettä tuhansiin erilaisiin hyökkäyskuvioita malintaviin sääntöihin, ja ilmoittaa haitallisesta liikenteestä verkon ylläpitäjille (Salah ja Qahtan 2008, s. 1). Järjestelmä on kuitenkin vain yhtä tehokas, kuin sille määritetyt säännöt, joten täysin uudenlaiset hyökkäyskuviot voivat luonnollisesti päästä järjestelmän ohi huomaamatta.

4.2 Tietomurtoon vastaaminen

Yhdysvaltojen terveys- ja sosiaalipalveluministeriön ohjeistuksen mukaan tietomurtoon vastaavat toimenpiteet ovat: Murron varmistaminen, tapahtumaan vastaavan tiimin kokoaminen ja koordinointi, murron arviointi, murron laajuuden ja tyypin määrittäminen, todistusaineiston kerääminen ja murrosta kommunikointi datan omistajien kanssa (USHHS 2015, s. 5—6).

Tietomurron sattuessa tulee luoda tiimi, johon kuuluu henkilöitä organisaation kaikista osa-alueista ja heidän tehtävänsä on tietomurron selvityksen ja hallinnan toimenpiteiden suorittaminen. Tärkeää on estää valtuuttamattomat yhteydet, ja lisävuotojen mahdollisuus. Toinen tärkeä vaihe on vuodon perimmäisen syyn etsiminen ja korjaaminen. Samalla tiedon kulkua ja julkista viestintää murrosta tulee koordinoida. Kaikki todistusaineisto murtoon liittyen, kuten lokitiedostot, murron vastaamiseen tehdyt toimenpiteet ja vaikutusten lievittämisen keinot tulee dokumentoida myöhempää analysointia varten (USHHS 2015, s. 5—6).

Euroopan yleisen tietosuoja-asetuksen mukaan on henkilötietoja koskevasta tietoturvaloukkauksesta ilmoitettava viipymättä toimintavaltaiselle valvontaviranomaiselle, kuitenkin enintään 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta. Kuitenkin perustelluin syin, voidaan 72 tunnin aikaikkuna ylittää (Tietosuoja-asetus 2016, Luku 33 kohta 1).

4.3 Murron jälkeiset toimenpiteet

Murron jälkeiset toimenpiteet keskittyvät dokumentointiin, viestintään ja arviointiin. Tietomurto tulee systemaattisesti dokumentoida, ja sen vastaamiseen käytetyt toimenpiteet tulee arvioida. Murtoon vastanneiden tiiminjäsenien palautetta tulee kuunnella ja ne tulee sisällyttää riskin minimoinnin strategioiden arviointiin. Tietomurron perimmäinen syy tulee korjata, ja sen vaikutuksia tulee minimoida erilaisilla aikaisempiin murtoihin perustuvilla strategioilla (USHHS 2015, s. 6).

Dokumentoinnin arvioinnista opittuja asioita tulee soveltaa tietomurtoon valmistautuvissa toimenpiteissä, ja toimenpiteitä tulee muuttaa tarpeen mukaan. Murrosta on lopuksi ilmoitettava asianomaisille ja viranomaisille, ja auttaa murrossa uhreiksi joutuneita tarpeen mukaan (USHHS 2015, s. 6).

5 Yhteenveto

Tietomurrot ovat jokapäiväinen ongelma, ja niiden kustannukset yhteiskunnalle ovat valtavat. Ylivoimaisesti suurin osa kaikista tietomurroista jakautuu vain viidelle hyökkäysvektorille ja kaikista hyökkäyksistä käyttäjätunnukset liittyvät reilusti yli kolmasosan (ITRC 2022; IBM 2022).

Tietomurtoja voidaan kuitenkin ehkäistä oikeanlaisella varautumisella ja hyvillä käytännöillä, kuten esimerkiksi Zero-trust mallia ja hyvää salasanahygieniaa hyödyntämällä. Kaikesta varautumisesta huolimatta, on todennäköistä, että organisaatio tulee kokemaan tietomurron jossain kohtaa elinkaartaan. Tämän takia on myös varauduttava ja luotava menetelmät tietomurron käsittelemiseen, ja sen jälkeisiin toimenpiteisiin. Tutkielmassa tarkastellut menetelmät ja riskit ovat kuitenkin vasta murto-osa alan haasteiden kirjosta. Organisaatioilla tulee olla suunnitelmat valmiina tätä skenaariota varten, ja olla tietoisia kaikista liiketoimintaan pätevistä tietoturvaan liittyvistä laeista (USHHS 2015). Erityisesti Euroopassa toimivien organisaatioiden tulee olla tietoisia Euroopan yleisen tietosuoja-asetuksen määrityksistä paikallisen lainsäädännön ohella (Tietosuoja-asetus 2016).

Tietomurron sattuessa tärkeintä on: sulkea kaikki valtuuttamattomat yhteydet, estää lisävuotojen tapahtuminen ja löytää murron perimmäinen syy pikimmiten. Kaikki toimenpiteet tulee dokumentoida ja todistusaineiston kerääminen ja suojaaminen on tehtävä. Tietomurrosta on ilmoitettava asianomaisille ja erityisesti maasta ja lainsäädännöstä riippuen viranomaisille (USHHS 2015).

Lähteet

Apache. 2022. *Log4j.* https://logging.apache.org/log4j/2.x/, viitattu 10.11.2021.

BBC. 2012. *Anonymous hackers 'cost PayPal £3.5m'.* Uutisartikkeli BBC:n sivuilla https://www.bbc.com/news/uk-20449474, viitattu 9.11.2022.

———. 2014. *Edward Snowden: Leaks that exposed US spy programme.* Uutisartikkeli BBC:n sivuilla https://www.bbc.com/news/world-us-canada-23123964, viitattu 9.11.2022.

Bonner, Lance. 2012. "Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches". *Wash. UJL & Pol'y* 40:257.

Bošnjak, L, J Sreš ja Bosnjak Brumen. 2018. "Brute-force and dictionary attack on hashed real-world passwords". Teoksessa *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro),* 1161–1166. IEEE.

Brito, Jerry. 2011. *'We Do It for the Lulz': What Makes LulzSec Tick?* Artikkeli TIME Magazinen sivuilla https://techland.time.com/2011/06/17/we-do-it-for-the-lulz-what-makes-lulzsec-tick/, viitattu 9.11.2022.

CERT, Insider Threat Center. 2011. "Insider Threat Control: Using a SIEM signature to detect potential precursors to IT Sabotage". *Software Engineering Institute, Carnegie Mellon University Carnegie Mellon University,* https://resources.sei.cmu.edu/asset_files/WhitePaper/2011_019_001_53433.pdf.

———. 2017. *CERT Insider Threat Center Brochure.* saatavilla pdf-muodossa, https://resources.sei.cmu.edu/asset_files/Brochure/2017_015_001_452233.pdf, viitattu 10.11.2022.

Cova, Marco, Christopher Kruegel ja Giovanni Vigna. 2008. "There Is No Free Phish: An Analysis of"Free"and Live Phishing Kits." *WOOT* 8:1–8. https://www.usenix.org/legacy/events/woot08/tech/full_papers/cova/cova.pdf.

CVE. 2022a. *CVE Program.* Tietokanta etsittävissä ja ladattavissa internetistä, https://www.cve.org, viitattu 10.11.2022.

CVE. 2022b. *CVE Program.* log4j hakutulokset CVE tietokannasta, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=log4j, viitattu 10.11.2022.

Das, Anupam, Joseph Bonneau, Matthew Caesar, Nikita Borisov ja Xiaofeng Wang. 2014. "The Tangled Web of Password Reuse". Teoksessa *Proceedings of NDSS 2014.* Tammikuu. https://doi.org/10.14722/ndss.2014.23357.

Dmitrienko, Alexandra, Christopher Liebchen, Christian Rossow ja Ahmad-Reza Sadeghi. 2014. "On the (in) security of mobile two-factor authentication". Teoksessa *International Conference on Financial Cryptography and Data Security,* 365–383. Springer.

F-Secure. 2022a. *Mitä on tietojenkalastelu?* Artikkeli F-Securen omilla sivuilla https://www.f-secure.com/fi/home/articles/what-is-phishing, viitattu 8.11.2022.

———. 2022b. *What is a data breach?* Artikkeli F-Securen omilla sivuilla https://www.f-secure.com/us-en/home/articles/what-is-a-data-breach, viitattu 3.11.2022.

Guardian. 2013. *NSA collecting phone records of millions of Verizon customers daily.* Uutisartikkeli Guardianin sivuilla https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, viitattu 9.11.2022.

Gupta, Pranshu, ja Ramon A Mata-Toledo. 2016. "CYBERCRIME: IN DISGUISE CRIMES." *Journal of Information Systems & Operations Management* 10 (1).

Harper, Allen, Ryan Linn, Stephen Sims, Michael Baucom, Daniel Fernandez, Huáscar Tejeda ja Moses Frost. 2022. *Gray hat hacking: the ethical hacker's handbook.* McGraw-Hill Education.

IBM, International Business Machines Corporation. 2019. *Cost of a Data Breach Report 2019.* Saatavilla PDF-muodossa, https://www.ibm.com/downloads/cas/RDEQK07R, viitattu 8.11.2022.

———. 2020. *Cost of a Data Breach Report 2020.* Saatavilla PDF-muodossa, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1CostofaDataBreachReport2020.pdf, viitattu 8.11.2022.

IBM, International Business Machines Corporation. 2021. *Cost of a Data Breach Report 2021.* Saatavilla PDF-muodossa, https://www.dataendure.com/wp-content/uploads/2021_Cost_of_a_Data_Breach_-2.pdf, viitattu 8.11.2022.

———. 2022. *Cost of a Data Breach Report 2022.* Saatavilla PDF-muodossa, https://www.ibm.com/downloads/cas/3R8N1DZJ, viitattu 5.10.2022.

ITRC, Identity Theft Resource Center. 2022. *2021 Data Breach Annual Report.* Saatavilla PDF-muodossa, https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf, viitattu 21.10.2022.

Kost, Edward. 2022. *Data Breach vs. Data Leak: What's the Difference?* Blogi UpGuardin sivuilla https://www.upguard.com/blog/data-breach-vs-data-leak, viitattu 3.11.2022.

Ledesma, Josue. 2022. *What Is a Data Leak? Definition and Prevention.* Blogi Varoniksen sivuilla https://www.varonis.com/blog/data-leaks, viitattu 3.11.2022.

Mojang. 2022. *Security Vulnerability in Minecraft: Java Edition.* Artikkeli Minecraftin omilla sivuilla, https://help.minecraft.net/hc/en-us/articles/4416199399693-Security-Vulnerability-in-Minecraft-Java-Edition, viitattu 10.11.2021.

PCMagazine. 2022. *Critical Apache Log4j Exploit Demonstrated in Minecraft.* PCMag artikkeli, https://www.pcmag.com/opinions/critical-exploit-for-apache-log4j2-could-be-far-reaching-proves-real-in, viitattu 10.11.2021.

Ponemon-Institute. 2018. *2018 Cost of Insider Threats: Global.* saatavilla pdf-muodossa, https://www.insiderthreatdefense.us/pdf/PonemonInstitute2018Report-TheTrueCostOfInsiderThreatsRevealed.pdf, viitattu 10.11.2022.

Raman, Preeti, Hilmi Güneş Kayacık ja Anil Somayaji. 2011. "Understanding data leak prevention". Teoksessa *6th Annual Symposium on Information Assurance (ASIA'11),* 27. Citeseer. https://people.scs.carleton.ca/~soma/pubs/raman-asia2011.pdf.

Rikoslaki. 1889/39. *Suomen rikoslaki.* https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001, viitattu 3.11.2022.

Rose, Scott, Oliver Borchert, Stu Mitchell ja Sean Connelly. 2020. *Zero trust architecture.* Tekninen raportti. National Institute of Standards ja Technology.

Roza, Michael, Frank Guanco, Neha Thethi, Victor Chin, Jon-Michael Brook, Zoran Lalic, Vic Hargrave ym. 2019. “Top Threats to Cloud Computing: The Egregious Eleven”. *Cloud Security Alliance.*

Salah, K, ja A Qahtan. 2008. “Boosting throughput of Snort NIDS under Linux”. Teoksessa *2008 International Conference on Innovations in Information Technology,* 643–647. IEEE.

Shahzad, Muhammad, Muhammad Zubair Shafiq ja Alex X Liu. 2012. “A large scale exploratory analysis of software vulnerability life cycles”. Teoksessa *2012 34th International Conference on Software Engineering (ICSE),* 771–781. IEEE.

Suomisanakirja. 2022. *Konfiguroinnin määritelmä.* https://www.suomisanakirja.fi/konfigurointi, viitattu 10.11.2022.

Thomas, Kurt, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki ym. 2017. “Data breaches, phishing, or malware? Understanding the risks of stolen credentials”. Teoksessa *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security,* 1421–1434.

Tietosuoja-asetus. 2016. *EU 2016/679; jatkossa TSA.* https://gdpr-text.com/fi, viitattu 25.11.2022.

TIME, Doug Aamoth. 2010. *Operation Payback: Who Are the WikiLeaks ‘Hactivists’?* Artikkeli TIME Magazinen sivuilla https://techland.time.com/2010/12/09/operation-payback-who-are-the-wikileaks-hactivists/, viitattu 9.11.2022.

USHHS, Administration for Children & Families, United States Department of Health & Human Services. 2015. *State and Tribal Child Welfare Information Systems, Information Security Data Breach Response.* Sivu 2. Saatavilla PDF-muodossa, https://www.acf.hhs.gov/sites/default/files/documents/cb/im1504.pdf, viitattu 3.11.2022.

WatchGuard. 2021. *RISK-BASED AUTHENTICATION: A Critical Element to Any Zero-Trust Deployment.* Huhtikuu. Viitattu 8. marraskuuta 2022. https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/watchguard/ebook-risk-based-auth-us.pdf.

Weidman, Georgia. 2014. *Penetration testing: a hands-on introduction to hacking*. No starch press.

VICE, Lorenzo Franceschi-Bicchierai. 2016. *Hacker Tries To Sell 427 Milllion Stolen MySpace Passwords For 2,800 Dollars.* VICE News artikkeli Vicen omilla sivuilla https://www.vice.com/en/article/pgkk8v/427-million-myspace-passwords-emails-data-breach, viitattu 9.11.2022.

Wood, K, ja E Pereira. 2011. “Impact of Misconfiguration in Cloud–Investigation into Security Challenges”. *International Journal Multimedia and Image Processing* 1 (1).

Zeng, Peng, Guanjun Lin, Lei Pan, Yonghang Tai ja Jun Zhang. 2020. “Software vulnerability analysis and discovery using deep learning techniques: A survey”. *IEEE Access* 8:197158–197172.