Nea Räisänen

TIETOVERKKOUHAT JA NIILTÄ SUOJAUTUMINEN YRITYSVERKOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Räisänen, Nea
Tietoverkkouhat ja niiltä suojautuminen
Jyväskylä: Jyväskylän yliopisto, 2018, 56 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Hämäläinen, Timo

Verkottuvassa maailmassa yritykset ovat yhä enemmän riippuvaisia teknologiasta ja internetistä. Samalla kun se tuo mahdollisuuksia, aiheutuu siitä myös uhkia. Koska useiden yritysten merkittävin pääoma on tieto, on tärkeää suojata tiedot ulkopuolisilta. Myös lainsäädäntö ohjaa yrityksiä suojaamaan muun muassa henkilötiedot asianmukaisella tavalla. Usein yritykset turvautuvatkin tietoturvakatsauksiin arvioidakseen kykyään suojautua nykyisiltä tietoturvauhkilta. Tämän tutkimuksen tavoitteena oli käydä läpi viimeaikaisimpia hyökkäyksiä sekä keinoja niiltä suojautumiseen. Tutkimus toteutettiin tekemällä tietoturvakatsaus erään suomalaisen yrityksen toimistoverkkoon, ja katsauksesta laadittiin kohdeyritykselle raportti parannusehdotuksista. Tulokseksi saatiin useita haavoittuvuuksia, vaikkakin ne olivat melko vaikeasti hyväksikäytettäviä. Korjaavilla toimenpiteillä yritys voi suojautua paremmin nykyisiltä ja tulevaisuudenkin tietoverkkouhkilta.

Asiasanat: tietoturva, tietoverkko, uhka, haavoittuvuus

ABSTRACT

Räisänen, Nea
Network security threats and countermeasures
Jyväskylä: University of Jyväskylä, 2018, 56 pp.
Cyber security, Master's Thesis
Supervisor(s): Hämäläinen, Timo

In the networking world companies have become more dependent on technology and internet. It provides numerous possibilities but at the same time it poses threats. As information is the main asset for many companies, it is important to protect information from outsiders. There is also legislation for protecting information, for example, personal data. Companies conduct security audits often to evaluate their ability to protect their assets from security threats. The objective of this study is to present current security threats and their countermeasures. The study was conducted by doing a security audit to a Finnish company network and then, according to the findings, a report of recommendations was delivered to the company. During the audit, several vulnerabilities were found, however they seemed to be difficult to exploit. With the help of given recommendations, the company can improve its security and protect its assets better from current and future threats.

Keywords: information security, network, threat, vulnerability

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämän tutkielman aihepiirinä on tietoverkkouhat ja niiltä suojautuminen. Tutkielma tehdään toimeksiantona suomalaiselle yritykselle, jolla on useita toimipisteitä Suomessa. Yritys käsittelee toiminnassaan asiakkaiden tietoja sekä henkilötietoja, mistä syystä tietoturva on merkittävässä roolissa yrityksen toiminnassa. Yrityksen merkittävin pääoma on tieto, joten se pyrkii tietoturvan toimialalla yleisesti hyväksytyin keinoin suojaamaan tiedot. Koska yritys pyrkii kasvattamaan toimintaansa, on sen tietoturvaratkaisujen skaalauduttava kasvun tahdissa.

Tutkimuksen tarve tuli esille, kun yrityksen tietohallinnossa huomattiin tietoverkon turvallisuusratkaisujen ja -käytäntöjen päivittäminen ajankohtaiseksi. Tietohallinnossa todettiin, että nykyisiä ratkaisuja pitäisi päivitystä varten ensin tarkastella parannettavien kohtien löytämiseksi. Tämä pro gradu -tutkielma onkin tehty yrityksen päätöksestä toteuttaa verkkoaan koskeva tietoturvakatsaus. Aihe on yritykselle tärkeä, sillä vastaavanlaista tietoverkkoon kohdistuvaa käytännön tietoturvakatsausta ei yrityksessä ole vielä tehty.

Tämän tutkielman varsinaisia tutkimusongelmia onkin selvittää yrityksen verkon rakenne, millaisia uhkia verkkoon kohdistuu, ja keinoja, joilla uhkia voi vähentää. Näihin tutkimusongelmiin liittyy olennaisesti myös tietoturva-alan ja siihen liittyvien käsitteiden määrittely sekä katsaus viimeaikaisimpiin uhkiin. Käsitteiden määrittely ja katsaus viimeaikaisimpiin uhkiin toteutetaan kirjallisuuskatsauksella, missä käytetään lähteenä tietoturvan alan tilastoja, artikkeleita, konferenssijulkaisuja ja raportteja. Kirjallisuuskatsauksen avulla pyritään muodostamaan kokonaiskuva nykyisestä uhkaympäristöstä yrityksen ja loppukäyttäjän näkökulmasta.

Tutkielmassa käytetään konstruktiivista tutkimusmenetelmää, jonka lopputuloksena syntyy kohdeyritykselle raportti, joka sisältää suosituksia tietoverkon suojaamisen parantamiseksi. Raportti pohjautuu tietoturvakatsauksen tuloksiin sekä tietoturva-alan artikkeleihin hyökkäyksistä ja niiden vastatoimista.

Tietoturvakatsauksen tuloksena löydettiin useita haavoittuvuuksia, joista osa oli yrityksellä jo entuudestaan tiedossa. Entuudestaan tiedossa olevat haavoittuvuudet liittyivät samaan laitekokonaisuuteen. Muut löydetyt haavoittu-

vuudet liittyivät erityisesti avoinna oleviin ylimääräisiin portteihin, päivittämättömiin laitteisiin ja konfigurointiongelmiin. Tutkimuksessa suoritettiin myös kolmeen yrityksen tulostimeen hyökkäyksiä, joista osalle tulostimet olivat haavoittuvaisia. Tutkimuksen myötä havaittiin, että tulostimet ovat usein jo suunniteltu epäturvallisiksi, minkä vuoksi niiden turvallisuuden parantaminen on haastavaa.

Tietoturvakatsauksen tuloksista luodusta raportista yritys näkee tietoverkkonsa turvallisuuden tilan ja voi niitä hyödyntämällä ottaa käyttöön turvallisuutta entisestään parantavia menetelmiä. Samalla yritys voi varautua paremmin myös tulevaisuuden uhkiin. Koska vastaavanlaista tietoturvakatsausta ei ole aiemmin tehty yrityksen verkkoon, toimii tämän tutkielman tietoturvakatsauksen tulokset samalla pohjana yrityksessä tulevaisuudessa suoritettaville katsauksille.

Tutkielman rakenne on seuraavanlainen: Luvussa 2 määritellään tietoturvaan liittyvät keskeiset käsitteet, tietoturva, tietosuoja ja kyberturvallisuus sekä mikä ero näillä kolmella viimeiseksi mainitulla on. Luodaan luvussa 2 myös katsaus viimeaikaisimpiin hyökkäyksiin ja langattomien verkkojen turvallisuustilanteeseen, sillä myös yrityksessä käytetään langattomia verkkoja. Luvussa 3 käydään läpi tutkimuksen toteutuksen kannalta keskeiset asiat: tutkimusongelma, tutkimusmenetelmä, aineistonkeruumenetelmänä tietoturvakatsaus ja tutkimuksessa käytettävät työkalut. Menetelmissä kuvataan myös tietoturvakatsauksen prosessi. Luvussa 4 esitellään yrityksen tietoverkkoon tehtyjä hyökkäyksiä ja verkosta löydettyjä haavoittuvuuksia. Luku 5 sisältää tietoturvakatsauksen löydösten perusteella laadittuja suosituksia yritykselle, tulosten pohdinnan yrityksen näkökulma huomioiden ja tulosten validoinnin. Luvussa 6 on tutkimuksen johtopäätökset.

2 KIRJALLISUUSKATSAUS

Koska tietoturva liittyy olennaisesti tutkielman aihepiiriin, esitellään tässä luvussa tietoturvan käsite sekä muita siihen liittyviä käsitteitä. Esitellään myös tietoturvan kanssa osittain päällekkäisiä käsitteitä.

2.1 Tietoturvaan liittyviä käsitteitä

Tietoturva on laaja käsite. Siitä syystä tässä alaluvussa määritellään ennen tietoturvan määrittelyä tietoturvaan oleellisesti liittyviä käsitteitä. Näitä ovat tieto, tietojärjestelmä, uhka, haavoittuvuus ja riski.

2.1.1 Tieto

NIST (National Institute of Standards and Technology) (2017) käyttää tiedon määritelmänä faktoja ja ideoita, jotka voidaan esittää tai koodata datan useissa muodoissa. Tieto voi olla myös tietämystä, kuten dataa ja ohjeita, missä tahansa sellaisessa muodossa, jota voidaan välittää järjestelmän kokonaisuuksien välillä (NIST, 2017).

2.1.2 Tietojärjestelmä

Suomen kyberturvallisuusstrategiassa (2013) tietojärjestelmä määritellään ihmisistä, tietojenkäsittely- ja tiedonsiirtolaitteista ja ohjelmista koostuvaksi järjestelmäksi, jonka tarkoituksena on tehostaa tai helpottaa jotakin toimintaa tai tehdä se mahdolliseksi käsittelemällä informaatiota.

2.1.3 Uhka

NIST (2017) määrittelee uhkan olosuhteiksi tai tapahtumaksi, jolla on potentiaalia vaikuttaa haitallisesti organisaation toimintaan, omaisuuteen, työntekijöihin, muihin organisaatioihin tai kansakuntaan järjestelmän luvattoman käytön, tuhoamisen, paljastamisen ja tiedon muokkaamisen avulla tai estämällä järjestelmän käytön kokonaan. Valtionhallinnon tietoturvasanastossa (2008) uhka määritellään mahdollisesti toteutuvaksi haitalliseksi tapahtumaksi tai häiriöksi, joka tapahtuessaan voi aiheuttaa tiedoille, muulle omaisuudelle tai toiminnalle jotain ei-toivottua.

2.1.4 Haavoittuvuus

NIST (2017) määrittelee haavoittuvuuden heikkoudeksi tietojärjestelmässä, järjestelmän turvallisuustoimintatavoissa, sisäisessä valvonnassa tai toteutuksessa, jota uhka voi hyödyntää. Valtionhallinnon tietoturvasanastossa (2008) haavoittuvuus on ”alttius turvallisuutta uhkaaville tekijöille, puutteet ja heikkoudet turvatoimissa sekä suojauksissa”. CVE:n (Common Vulnerabilities and Exposures) mukaan haavoittuvuus on ohjelmistosta tai laitteiston komponenteista löytyvässä tietokonelogiikassa (esim. koodissa) oleva heikkous, jonka hyväksikäyttö aiheuttaa haittaa luottamuksellisuudelle, eheydelle tai saatavuudelle.

2.1.5 Riski

NIST (2017) määrittelee riskin uhkaavan tapahtuman aiheuttamien haittavaikutusten funktioksi ja todennäköisyydeksi, että uhkaava tapahtuma toteutuu. NIST:n (2017) mukaan järjestelmään liittyvät turvallisuusriskit ovat riskejä, jotka syntyvät tiedon tai järjestelmän luottamuksellisuuden, eheyden ja saatavuuden menetyksestä ja heijastavat potentiaalisia haittavaikutuksia organisaation toiminnalle. Riskin olemassaolo johtuu uhkien, haavoittuvuuksien ja omaisuuden arvon yhdistelmästä (Gerber & Von Solms, 2005).

2.2 Tietoturva

Valtionhallinnon tietoturvasanastossa sekä Suomen kyberturvallisuusstrategiassa (2013) tietoturva tarkoittaa järjestelyjä, joiden tavoitteena on varmistaa tiedon käytettävyys, eheys ja luottamuksellisuus. Sanastossa käytettävyys tarkoittaa, että tietoon oikeutetut voivat hyödyntää sitä haluttuna aikana. Eheys puolestaan tarkoittaa, että tieto on yhtäpitävä alkuperäisen tiedon kanssa, ja luottamuksellisuus tarkoittaa sitä, ettei tietoa saa kukaan ulkopuolinen.

Myös kansainvälinen standardi ISO/IEC 27002 (2005) määrittelee tietoturvan tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi.

Standardin mukaan tietoa voi olla monessa muodossa, kuten paperille tulostettuna ja elektronisena. (Von Solms & Van Niekerk, 2013.)

NIST (2017) tarkentaa määritelmää: tietoturva kattaa tiedon ja tietojärjestelmien suojaamisen luvattomalta pääsyltä, käytöltä, paljastamiselta, häiriöltä, muokkaamiselta tai tuhoamiselta. Suojaamisella pyritään turvaamaan luottamuksellisuus, eheys ja saatavuus. Whitman ja Mattord (2013, s. 4) vielä tarkentavat, että tiedon ja sitä käsittelevien järjestelmien suojaaminen tapahtuu tietoturvapolitiikan, koulutuksen, tietoisuusohjelmien ja teknologian avulla.

Von Solms ja Van Niekerk (2013) lisäävät, että tietoturvallisuus ei ole tuote tai teknologia vaan prosessi. Tietoturvallisuusprosessi saattaa edellyttää joidenkin tuotteiden käyttöä, mutta sitä ei voi suoraan ostaa. Tietoturvallisuus myös määritellään usein turvallisen tiedon ominaisuuksien suhteen. Näitä ominaisuuksia ovat useimmiten luottamuksellisuus, eheys ja saatavuus, mutta ominaisuuksia voi olla enemmänkin. (Von Solms & Van Niekerk, 2013.)

Laissa sähköisen viestinnän palveluista tietoturvalla tarkoitetaan ”hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä”. Sähköisen viestinnän palveluiden lain 247§:ään pohjaten Viestintävirasto erittelee palvelun tietoturvaan liittyen neljä tietoturvan osa-aluetta, joista yhteisötilaajalla, kuten yrityksellä tai oppilaitoksella, on velvollisuus huolehtia: toiminnan tietoturvallisuus, tietoliikenneturvallisuus, laitteisto- ja ohjelmistoturvallisuus sekä tietoaineistoturvallisuus. Vaikka yhteisötilaaja olisi ulkoistanut palveluidensa hoitamisen, se vastaa silti palveluidensa tietoturvasta ja lainmukaisuudesta. Kohtuuttomia toimia tietoturvan varmistamiseksi ei kuitenkaan yhteisötilaajalta edellytetä, vaan yhteisötilaaja voi suhteuttaa toimet kustannuksiin, uhkien vakavuuteen ja teknisen kehityksen tasoon sopiviksi. (Viestintävirasto.)

Viranomaisten auditointityökalussa Katakrissa (2015) tietoturvallisuus on jaettu turvallisuusjohtamiseen, fyysiseen turvallisuuteen ja tekniseen tietoturvallisuuteen, ja nämä kolme on jaettu vielä pienempiin osiin. Turvallisuusjohtamisen osa-alue on jaettu hallinnolliseen turvallisuuteen ja henkilöstöturvallisuuteen. Fyysinen turvallisuus -osio kattaa tilat ja laitteet, luvattoman pääsyn estämisen, salakatselulta ja salakuuntelulta suojaamisen ja toiminnan jatkuvuuden hallinnan. Teknisen tietoturvallisuuden alla puolestaan ovat tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuus.

Tietoturva määritellään siis usein juurikin tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi, perinteiseksi ”CIA-kolmioksi”. Tietoturva kattaa tiedon lisäksi myös sitä käsittelevät tietojärjestelmät ja teknisten toimien lisäksi tietoturvaan liittyy myös hallinnolliset toimet.

2.3 Tietosuoja

Koska tutkimuksen kohteena oleva yritys käsittelee toiminnassaan henkilötietoja, on syytä käydä läpi myös tietosuojan käsite. Näin voidaan tuoda esille tietoturvan ja tietosuojan välinen merkitysero.

Suomen kyberturvallisuusstrategiassa (2013) tietosuoja määritellään henkilön yksityisyyden suojaamiseksi oikeudettomalta tai henkilöä vahingoittavalta käytöltä. Strategiassa tietosuojan käsitteeseen kuuluvat myös ”ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.”

Tietosuoja Valtionhallinnon tietoturvasanastossa on määritelty ihmisen yksityisyyden suojaksi sekä muiksi sitä turvaaviksi oikeuksiksi käsiteltäessä henkilötietoja. Näitä oikeuksia ovat muun muassa ”1) tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen; 2) henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä”.

Tietosuoja liittyy siis henkilötietoihin. Suomessa on olemassa oma lakinsa, joka koskee henkilötietoja. Henkilötietolain 3§ määrittelee henkilötiedot kaikenlaisiksi luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan kuvaaviksi merkinnöiksi, joista hänet, hänen perheensä tai hänen kanssaan yhteidessä taloudessa elävät voidaan tunnistaa. Henkilötietolain tarkoituksena on ”toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista”. Henkilötietolain 2§:ssä sanotaan, että tätä lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Lakia sovelletaan myös muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sellaisen osa.

Suomen hallitus on kuitenkin esittänyt uutta kansallista tietosuojalakia täydentämään EU:n yleistä tietosuoja-asetusta, joka tuli voimaan 25.5.2016 ja jonka soveltaminen jäsenvaltioissa alkoi 25.5.2018. Hallitus ehdotti, että samalla kumottaisiin henkilötietolaki ja laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Ehdotettua lakia sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa. (Hallituksen esitys HE 9/2018 vp.2018.)

13.11.2018 eduskunta hyväksyi hallituksen esityksen mukaisen uuden tietosuojalain sekä siihen liittyvät muut lait muutettuna hallintovaliokunnan mietinnön mukaisesti (eduskunta.fi).

Tietoturvan ja tietosuojan eroksi voidaan niiden edellä mainituista määritelmistä päätellä, että tietosuoja liittyy vain henkilötietoihin, kun taas tietoturva voi liittyä myös muuhun tietoon. Tietoturva onkin käsitteenä laajempi kuin tietosuoja.

2.4 Kyberturvallisuus

Kyberturvallisuutta käytetään usein tietoturvan kanssa päällekkäin ikään kuin toisiaan vastaavina termeinä. Yhtymäkohtia näiden kahden termin välillä löytyy, mutta täysin samaa ne eivät tarkoita. Kyberturvallisuudessa on kyse myös muustakin kuin vain tiedon ja tietojärjestelmien suojaamisesta. Kyberturvallisuudessa on kyse myös sellaisten tietoa ja tietojärjestelmiä käyttävien ihmisten ja yhteiskuntien suojaamisesta, jotka altistuvat riskeille johtuen haavoittuvaisen tieto- ja viestintäteknologian käytöstä (Von Solms & Van Niekerk, 2013). Samankaltaisesti myös Suomen kyberturvallisuusstrategiassa (2013) määritellään kyberturvallisuus. Strategiassa kyberturvallisuus käsittää toimenpiteet, jotka kohdistuvat yhteiskunnan elintärkeisiin toimintoihin sekä kriittiseen infrastruktuuriin. Toimenpiteiden tavoitteena strategiassa on hallita ennakoivasti ja sietää kyberuhkia ja niiden vaikutuksia, ”jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle”.

Kyberturvallisuus siis sisältää tietoturvallisuuden ja on sitä laajempi käsite siten, että se kattaa myös ihmisten ja yhteiskuntien turvallisuuden. Toinen ero näiden kahden käsitteen välillä on myös, että ihmisiä ja yhteiskuntaa voidaan vahingoittaa laajassa mittakaavassa kyberturvallisuushyökkäyksillä, kun taas tietoturvallisuudessa haitta yleensä on epäsuoraa (Von Solms & Van Niekerk, 2013).

2.5 Viimeaikaisimpia hyökkäyksiä

Luomalla katsaus viimeaikaisimpiin uhkiin tilastojen avulla saadaan käsitys siitä, mitkä uhkat ovat esillä nykyään, missä määrin ja mitä vaikutuksia niillä voi olla. Tuodaan esille, millaisia puolustautumiskeinoja näitä uhkia vastaan on olemassa. Käydään myös läpi, mitä tekijöitä voi olla uhkien taustalla ja mistä syistä.

Haittaohjelmat muodostavat keskeisen (kyber)uhkan yrityksille, hallituksille ja yksilöille (Choo, 2011b). Uhkatilastoissa korostuvatkin erityisesti erilaiset haittaohjelmat (AV-TEST, 2018; Chebyshev, Sinitsyn, Liskin & Kupreev, 2018; McAfee, 2018; Symantec, 2018). Muita KasperskyLabin vuoden 2018 toisen neljännesvuoden tilastoissa eriteltyjä uhkia ovat hyökkäykset IoT-laitteisiin, pankkitroijalaiset, kiristyshaittaohjelmat, kryptovaluutan louhijat, web-lähteistä tulevat hyökkäykset ja haavoittuvaiset sovellukset (Chebyshev ym., 2018).

Internetin alettua levitä laajasti 1990-luvulla (Castells, 2002) haittaohjelmien lukumäärä on kasvanut voimakkaasti. Esimerkiksi vuonna 1996 DOS-pohjaisia viruksia oli luotu 10 000 (Nachenberg, 1997). Nykyään esimerkiksi AV-TEST Instituutti rekisteröi joka päivä yli 350 000 uutta haittaohjelmaa ja potentiaalisesti haitallista sovellusta (engl. potentially unwanted applications, PUA).

AV-TESTin tilastossa näkyy haittaohjelmien vuosittainen lisääntyminen kymmeneltä edelliseltä vuodelta lähtien. Vuonna 2018 AV-TEST rekisteröi 856,62 miljoonaa haittaohjelmaa.

Haittaohjelmat hyväksikäyttävät haavoittuvuuksia web-palveluissa, selaimissa ja käyttöjärjestelmissä tai käyttävät sosiaalista manipulointia saadakseen käyttäjät ajamaan haitallista koodia haittaohjelmien levittämiseksi (Gandotra, Bansal & Sofat, 2014).

On olemassa useita eri tyyppisiä haittaohjelmia, kuten viruksia, troijalaisia, matoja, takaovia, vakoilu- ja mainosohjelmia sekä bottiverkkoja. Nämä luokat eivät poissulje toisiaan, mikä tarkoittaa, että haittaohjelmassa voi olla piirteitä useista eri luokista samaan aikaan. (Gandotra ym., 2014.)

Kun suurin osa haittaohjelmista hyväksikäyttää käyttöjärjestelmien haavoittuvuuksia Karyotiksen ja Khouzanin (2016) mukaan, markkinaosuudella on väliä. Hakkerit luovat haittaohjelmia sinne, missä käyttäjät ovat, ja tämä taas määräytyy käyttöjärjestelmän markkinaosuuden mukaan. (Arce, 2018.)

Statcounterin tilaston mukaan henkilökohtaisten tietokoneiden käyttöjärjestelmissä Windows johtaa n. 76% osuudella ja MacOs toisena n. 13% osuudella (Statcounter GlobalStats, 2018). Älypuhelinmarkkinoilla puolestaan johtaa Android n. 75% osuudella ja iOS on toisena 22% osuudella (Statcounter GlobalStats, 2018). AV-TESTin tilastoista nähdäänkin, että vuonna 2018 haittaohjelmia Windowsille löydettiin 76,84 miljoonaa, Androidille 2,94 miljoonaa ja MacOs:lle 86 660. AV-TESTin tilastossa (2018) uhkien jakaumassa haittaohjelmia oli 74,62% ja potentiaalisesti haitallisia sovelluksia 25,38%.

2.5.1 Mobiilihaittaohjelmat

Samalla kun mobiililaitteiden käyttö on lisääntynyt, on lisääntynyt myös niille kohdistetut haittaohjelmat. Vuodesta 2015 vuoteen 2016 haittaohjelmienlukumäärä Androidille lisääntyi 1,98 miljoonasta 4,36 miljoonaan, eli yli kaksinkertaistui (AV-TEST, 2018). Symantecin tilastoissa vuonna 2017 keskimäärin 24 000 haitallista mobiilisovellusta estettiin joka päivä (Symantec, 2018).

Koska Android-laitteet ovat saavuttaneet johtavan markkinaosuuden mobiilikäyttöjärjestelmissä, on käyttöjärjestelmän suosittuus ja siihen liittyvät rahalliset hyödyt vetäneet puoleensa myös haittaohjelmien tekijöitä. Androidin suosittuus johtuu Androidin avoimesta arkkitehtuurista ja sen sovelluskehitysrajapintojen (engl. application programming interface) suosittuudesta kehittäjäyhteisössä. (Faruki ym., 2015.)

Kun uhkat lisääntyvät, tilannetta pahentaa vanhentuneiden käyttöjärjestelmien jatkuva käyttö. Erityisesti Androidin uusinta versiota käyttää vain 20% Android-laitteista ja vain 2,3% käyttää Androidin viimeisintä pienempää julkaisua (engl. minor release). (Symantec, 2018.)

Myös KasperskyLabin vuoden 2018 toisen neljännesvuoden tilastoissa näkyy mobiilihaittaohjelmien kohdistuminen ennen kaikkea Androidille. KasperskyLab havaitsi 1 744 244 haitallista mobiilisovellusten asennuspakettia (engl. installation package), mikä on 421 666 enemmän kuin edellisessä vuosi-

neljänneksessä. KasperskyLab myös erittelee näiden mobiilisovellusten tyyppejä: nämä olivat muun muassa erilaisia riskityökaluja, mainosohjelmia ja eri tyyppisiä troijalaisia. (Chebyshev ym., 2018.)

Mobiilipankkitroijalaisten asennuspaketteja KasperskyLab havaitsi vuoden 2018 toisella vuosineljänneksellä 61 045, mikä on 3,2 kertaa enemmän kuin edellisellä neljänneksellä. Kaksi yleisintä mobiilipankkitroijalaista hyödyntävät kalasteluikkunoita varastaakseen käyttäjän pankkikortti- ja verkkopankkitunnuksia. Lisäksi ne varastavat rahaa SMS-palveluiden väärinkäytöksillä. Mobiilikiristyshaittaohjelmatroijalaisten asennuspaketteja Kaspersky havaitsi 14119, mikä on puolet enemmän kuin edellisellä neljänneksellä. (Chebyshev ym., 2018.)

Mobiilihaittaohjelmat voivat levitä esimerkiksi linkkejä sisältävien tekstiviestien avulla, saastuneen verkkosivun (La Polla, Martinelli & Sgandurra, 2013) ja sovelluskauppojen kautta (He, Chan & Guizani, 2015).

Mobiilihaittaohjelmilta voi suojautua lataamalla sovelluksia vain virallisista sovelluskaupoista, päivittämällä ja pitämällä varmuuskopiot ajan tasalla. Älypuhelinta ei kannata myöskään niin sanotusti ”jailbreakata” tai ”rootata”, sillä se laskee puhelimen suojaustasoa merkittävästi ja lisää haittaohjelmariskiä. On suositeltavaa myös asentaa virustorjuntaohjelmistot Android-mobiililaitteille. (IOS-laitteisiin virustorjuntaohjelmistoja ei ole saatavilla.) Virustorjuntaratkaisu voi olla käytännöllinen varsinkin pk-yrityksille, joilla on rajallinen IT-henkilöstön määrä ja pieni IT-budjetti. (Harris & Patten, 2014.)

2.5.2 Hyökkäykset IoT-laitteisiin

KasperskyLabin (2018) ”hunajapurkkien” datan perusteella Telnet-salasanojen murtaminen raaka voima -tyyppisesti on yleisin metodi IoT-laitteiden haittaohjelmien leviämiseen (Chebyshev ym., 2018). Nämä uhat vaikuttavat yleensä Linux-pohjaisiin järjestelmiin (McAfee, 2018), mikä näkyy myös KasperskyLabin (2018) tilastossa kymmenestä yleisimmästä haittaohjelmatyypistä, jotka on ladattu IoT-laitteisiin Telnet-hyökkäysten yhteydessä (Chebyshev ym., 2018). McAfee (2018) havaitsi uusia IoT-haittaohjelmia vuonna 2017 noin 59 000 ja vuonna 2018 noin 116 000. Symantec (2018) puolestaan havaitsi 600% nousun kaikissa IoT-hyökkäyksissä vuonna 2017. IoT-laitteisiin hyökkäämisen taustalla on bottiverkkojen rakentaminen.

Bottiverkko on joukko haittaohjelmalla tartutettuja koneita, niin sanottuja zombeja, joita hallitaan keskitetysti ja etänä. Bottiverkon hallitsija voi laittaa zombikoneet suorittamaan haitallisia ja rikollisia toimia, kuten lähettämään roskapostia, suorittamaan palvelunestohyökkäyksiä tai varastamaan henkilökohtaista dataa kuten sähköposti- tai pankkitunnuksia. Arviolta 80% sähköpostiliikenteestä on roskapostia ja suurin osa tästä on lähetetty bottiverkkojen avulla. (Hoque, Bhattacharyya & Kalita, 2015.)

Vaikka internet-palveluntarjoajat (ISP) ovat keskeisessä roolissa bottiverkkojen estämisessä (Asghari, van Eeten & Bauer, 2015) myös loppukäyttäjät voivat tehdä osansa estääkseen laitteidensa kaappaamisen osaksi bottiverkkoja.

Laitteiden oletussalasanat tulisi aina vaihtaa, sillä niitä hyödynnetään raakavoima -tyyppisissä hyökkäyksissä.

Käyttäjän tulisi olla huolellinen ladatessaan uusia ohjelmia, ettei tule ladanneeksi vahingossa haittaohjelmaa. Tekstit verkkosivulla tulisi lukea ennen painikkeiden klikkaamista. On suositeltavaa käyttää virustorjuntaohjelmistoja ja varmuuskopioida säännöllisesti. Käyttäjän pitäisi myös päivittää laitteitaan säännöllisesti. Järjestelmänvalvoja puolestaan voi ehkäistä bottiverkkohyökkäyksiä päivittämällä järjestelmää ja pysymällä ajan tasalla viimeisimmistä haavoittuvuuksista. Lisäksi lokien analysointi on tärkeää poikkeamien havaitsemiseksi. (Liu, Xiao, Ghaboosi, Deng & Zhang, 2009.)

2.5.3 Pankkitroijalaiset

KasperskyLabin (2018) tilastossa pankkitroijalaiset kuvaillaan ohjelmiksi, jotka varastavat salasanoja, pankkitunnuksia ja pankkikorttitietoja eri toimintaperiaatteita hyödyntäen. Jotkut pankkitroijalaiset esimerkiksi kaappaavat käyttäjän liikennettä injektoidakseen haitallisia skriptejä uhrin vierailemille verkkopankkisivuille tai ohjaamalla uhri väärennetylle verkkopankkisivulle (Chebyshev ym., 2018). Varastettujen tunnusten avulla pyritään varastamaan rahaa uhrien tileiltä.

Ylipäätään troijalaiset mukailevat autenttisen ohjelman toimintaa, mutta oikeasti varastavatkin tietoa, tarkkailevat järjestelmää tai turmelevat dataa (Vinod, Jaipur, Laxmi & Gaur, 2009). Vuonna 2018 pankkitroijalaisten jatkuva uhka säilyi ennallaan, ja niitä levitettiin tehokkaasti roskapostikampanjoiden avulla (McAfee, 2018).

Kiwia, Dehghantanha, Choo ja Slaughter (2018) mainitsevat pankkitroijalaisen ehkäisykeinoiksi virustorjuntaohjelmistot, verkon IPS:ien ja palomuurien käytön ja organisaation työntekijöiden kouluttamisen. Näiden lisäksi organisaatiossa on suositeltavaa olla varasuunnitelma tartunnan varalle, jotta järjestelmä voidaan palauttaa normaaliin tilaan mahdollisimman nopeasti ja estää haittaohjelman leviäminen.

2.5.4 Kiristyshaittaohjelmat

Vuoden 2018 toisella vuosineljänneksellä KasperskyLab esti lähes 159 000 käyttäjän koneelle kohdistettua kiristyshaittaohjelmahyökkäystä. Toisen vuosineljänneksen aikana kiristyshaittaohjelmien aktiivisuus laski 70 577:stä 63 804:ään. (Chebyshev ym., 2018.) Myös McAfeen raportissa (2018) näkyy kiristyshaittaohjelmien väheneminen: Uusien kiristyshaittaohjelmien näytteiden lukumäärä kasvoi joka neljännesvuodella vuonna 2017, mutta vuonna 2018 uusien näytteiden määrä laski yli 2,25 miljoonasta alle 1,5 miljoonaan.

Kiristyshaittaohjelma tyypistään riippuen joko lukitsee saastuneen koneen työpöydän tai salaa kaikki sen tiedostot (Kharraz, Arshad, Mulliner, Robertson & Kirda, 2016). Jotkut kiristyshaittaohjelmat puolestaan salaamisen (encryption)

sijaan poistavat käyttäjän kaikki tiedostot, mikäli käyttäjä ei maksa lunnaita (Kharraz, Robertson, Balzarotti, Bilge & Kirda, 2015).

Kiristyshaittaohjelmat leviävät, kun käyttäjä huijataan klikkaamaan haitallista linkkiä tai avaamaan sähköpostin haitallinen liitetiedosto (Sittig & Singh, 2016). Jotkut kiristyshaittaohjelmat hyödyntävät lisäksi tietoverkkopalveluiden (engl. network services) haavoittuvuuksia, jolloin ne pystyvät leviämään lähiverkossa (Huang ym., 2018).

Kiristyshaittaohjelmat pyytävät lunnaita käyttäjän datan palauttamiseksi. Yleinen suositus kuitenkin on olla maksamatta, sillä mikään ei takaa, että uhri saisi tiedostonsa takaisin maksettuaan lunnaat (Viestintävirasto, 2016). Lunnaiden maksaminen vain rohkaisee kyberrikollisia entisestään levittämään kiristyshaittaohjelmia (Cabaj & Mazurczyk, 2016). Symantecin (2018) arvion mukaan vuonna 2017 59% kiristyshaittaohjelmista kohdistui yrityksiin, mikä johtui suurelta osin WannaCry-kiristyshaittaohjelmasta, joka kohdistui pääosin yrityksiin eikä kuluttajiin.

Yritykset ja instituutiot voivatkin olla houkuttelevampi kohde, sillä yrityksen työpöydät ja palvelimet sisältävät todennäköisemmin arkaluontoista tai kriittisiä tietoja, kuten asiakastietokantoja, liiketoimintasuunnitelmia ja lähdekoodia. Mitä arvokkaampaa data on, sitä korkeammat lunnaat ja mahdollisuus lunnaiden maksamiselle. (Cabaj & Mazurczyk, 2016.)

Richardson ja North (2017) suosittelevat neljää vaihetta kiristyshaittaohjelmien ehkäisyssä: varmuuskopiointi, sähköpostin linkkien ja liitetiedostojen avaamisen välttäminen, päivittäminen ja saastuneen koneen irrottaminen verkosta. Organisaatioille he ehdottavat lisäksi kiristyshaittaohjelmien aiheuttamien riskien arviointia ja nykyisten käytäntöjen ja politiikkojen päivittämistä.

Nadir ja Bakhshi (2018) esittävät vastakeinoiksi seuraavia: Varmuuskopioiden ottaminen tiedostoista mahdollistaa tiedostojen palauttamisen. Virustorjuntaohjelmistot ovat tärkeä työkalu kiristyshaittaohjelmien havaitsemisessa ja ehkäisemisessä, vaikka voivatkin yleensä havaita vain ennestään tunnettuja uhkia. Ohjelmistojen ja käyttöjärjestelmien päivittämisellä voidaan paikata löydettyjä ja hyväksikäytettäviä haavoittuvuuksia. Sähköpostin kunnollinen suodatus voi estää kiristyshaittaohjelmia sisältäviä sähköposteja päätymästä perille. (Nadir & Bakhshi, 2018.)

Myös käyttäjien kouluttaminen on tärkeää, jotta he eivät lataa tuntemattomilta lähettäjiltä tulleita tiedostoja tai linkkejä. Pääsynhallinnalla voidaan vaikuttaa yrityksessä siihen, että käyttäjillä on vain tarvittavat oikeudet. Myös käyttäjillä, joilla on laajemmat oikeudet, tulisi olla käytössään käyttäjätunnus vähemmillä oikeuksilla, sillä myös he voivat tehdä virheitä. Järjestelmänvalvojan kannattaa sallia vain luotetut sovellukset päivityksiä ja muita järjestelmään kohdistuvia muutoksia varten, mikä vähentää haittaohjelmien lataamisen mahdollisuutta. Mikäli kiristyshaittaohjelma pääse salaamaan tiedostot eikä sen käyttämä salaus ole tarpeeksi vahva, voi vastakeinona hyödyntää vapaasti saatavilla olevia salauksen purkutyökaluja tiedostojen palauttamiseksi. Jos kiristyshaittaohjelma pääsee poistamaan tiedostot, voi tiedostot yrittää vielä palauttaa palautustyökalun avulla. (Nadir & Bakhshi, 2018.)

2.5.5 Kryptolouhijat

Vaikka KasperskyLabin (Chebyshev ym., 2018), Symantecin (2018) ja McAfeen (2018) tilastoissa kiristyshaittaohjelmat on listattu, näkyy niissä kuitenkin kiristyshaittaohjelmien väheneminen. Sen sijaan kryptovaluuttalouhijoiden lukumäärä on alkanut kasvaa. Kyberrikolliset, jotka ovat aiemmin keskittyneet kiristyshaittaohjelmiin ja niistä saataviin tuloihin, ovat nyt alkaneet siirtyä kryptovaluutan louhintaan (Symantec, 2018; McAfee, 2018).

KasperskyLab havaitsi vuoden 2018 toisella vuosineljänneksellä 13 948 uutta louhijan muunnosta ja Kasperskyn ohjelmistojen käyttäjistä yli 2,2 miljoonaa sai koneelleen louhijatartunnan (Chebyshev ym., 2018). Symantec (2018) havaitsi vuoden 2017 aikana 8500% kasvun havaituissa louhijoissa. Symantec (2018) arvioi IoT-hyökkäystenkin lisääntymisen liittyvän louhintaan, kun kyberrikolliset voivat siten hyödyntää suurta määrää kaapattuja laitteita louhintaan.

Selainpohjainen kryptolouhinta tarkoittaa rahayksiköiden (engl. monetary units) luomista käyttämällä selaimia kuten Firefoxia, Chromea ja Internet Exploreria. Kryptovaluutan realisointi vaatii tietyn määrän työtä (engl. proof-of-work), jotta digitaalinen valuutta voidaan laskea liikkeelle (engl. issue). Työ käsittää monimutkaisten matemaattisten ja kryptografisten algoritmien laskentaa. (Vukolić, 2015, Zimba, Wang, Mulenga & Odongo, 2018 mukaan.) Tämä vaatii runsaasti CPU -resursseja. Toisin kuin kiristyshaittaohjelmissa, missä tulojen saaminen riippuu uhrin halusta tai kyvystä maksaa lunnaat, kryptolouhinnassa tulot siirtyvät automaattisesti hyökkääjälle. Hyökkääjän tehtävä on strategisesti valita sellainen vilkas web-palvelin tai jokin yritysverkon web-palvelin, jossa on paljon käyttäjiä päivittäin. (Zimba ym., 2018.)

Symantecin (2018) arvion mukaan ainakin vuonna 2017 louhijahyökkäykset kohdistuivatkin enemmän kuluttajiin kuin yrityksiin. Tämä voi johtua siitä, että louhijat toimivat parhaiten sivuilla, joilla käyttäjät viihtyvät kauan aikaa, kuten videoiden suoratoistopalvelusivustoilla. Tällaista tapahtuu todennäköisemmin kuluttajien kuin yritysten koneilla. (Symantec, 2018.)

Louhinta siis vaikuttaa ennen kaikkea suorituskykyyn: se hidastaa koneita ja ylikuumentaa akkuja. Yritysverkot ovat sulkemisriskin alla, kun louhijat leviävät niiden ympäristössä. Louhijat saattavat vaikuttaa organisaatioihin myös taloudellisesti, mikäli organisaatioita laskutetaan pilven CPU:n käytöstä. (Symantec, 2018.)

Yritysten tai organisaatioiden verkkoon päästyään louhijat saattavat toki aiheuttaa muutakin vahinkoa, kuin koneiden ja palvelinten hidastumista.

Esimerkiksi Lahden kaupungin it-järjestelmiin pääsi helmikuussa 2018 kryptovaluuttaa louhiva haittaohjelma, jonka vuoksi terveysasemien potilastietojärjestelmät lakkasivat toimimasta. Tämä häiritsi vakavasti hammashoitoloiden ja terveysasemien toimintaa: Laboratoriovastauksia ei saatu, eikä röntgenkuvia tai verikokeita voitu ottaa häiriön aikana. Potilaskertomuksien tiedot eivät näkyneet, eivätkä sähköiset reseptitkään toimineet. (Vänskä, 2018.)

Selainpohjaiseen louhintaan liittyviä potentiaalisia vastatoimia ovat (selaimen puolelta) estää asiakkaan puolella tapahtuvaa skriptausta, varoittamalla käyttäjiä heidän puolellaan tapahtuvasta raskaasta skriptauksesta ja estämällä tunnettujen louhintaskriptien lähteitä. Näiden haasteena on kuitenkin löytää sopiva raja resursseja runsaasti kuluttavan legitiimin sovelluksen ja louhinnasta johtuvan resurssien kulutuksen välille, jotta käyttäjä voi päättää, salliiko resurssien kulutuksen vai ei. (Eskandari, Leoutsarakos, Mursch & Clark, 2018.)

Suomen Kyberturvallisuuskeskus (2018) puolestaan on julkaissut ohjeistuksen ylläpitäjille WannaMine-haittaohjelmalta suojautumiseen. Ohjeisiin lukeutuvat Windows-työasemien ja -palvelinten päivittäminen, vahvojen ja eri salasanojen käyttö ja tunkeilijan havaitsemisjärjestelmien käyttö (IDS). Ohjeissa kehotetaan tarkistamaan, löytyykö palvelimelta outoja WMI Autorun entryjä tai käynnistyviä tehtäviä. Lisäksi suositellaan verkon segmentointia, jolla voi rajoittaa mahdollisuuksia liikkua sisäverkossa.

2.5.6 Web-lähteistä tulevat hyökkäykset

KasperskyLabin vuoden 2018 toisen vuosineljänneksen uhkatilastoissa esitellyt web-lähteistä tulevat hyökkäykset perustuvat saastuneilta verkkosivuilta ja murretuilta legitiimeiltä sivuilta ladattuihin haitallisiin objekteihin. KasperskyLab torjui noin 963 miljoonaa webresursseista ympäri maailmaa tulevaa hyökkäystä. Noin 352 miljoonaa uniikkia web-osoitetta tunnistettiin haitalliseksi. Web-hyökkäysten suurin lähde oli USA (45,87%), toisena Alankomaat (25.74%) ja kolmantena Saksa (5,53%). (Chebyshev ym., 2018.)

McAfeen raportissa (2018) puolestaan web-uhkat on eritelty epäilyttäviin web-osoitteisiin, haitallisiin web-osoitteisiin, haitallisiin lataustiedostoja sisältäviin web-osoitteisiin ja kalastelusivustoihin. Vuoden 2018 toisella neljänneksellä McAfee havaitsi epäilyttäviä osoitteita noin 17,5 miljoonaa, haitallisia sivustoja yli 7 miljoonaa, haitallisia lataustiedostoja sisältäviä sivustoja noin 900 000 ja kalastelusivustoja yli 200 000.

Haitallisiin sivuihin liiittyy drive-by -lataushyökkäyksiä (engl. drive-by download attack). Drive-by -lataushyökkäyksessä käyttäjä huijataan haitalliselle verkkosivulle, jonka kautta haittaohjelma latautuu käyttäjän koneelle. Roskaposti on yleinen tapa houkutella käyttäjiä hyökkääjien haitallisille sivustoille. Roskaposti voi esimerkiksi sisältää linkin, joka johtaa haitalliselle sivustolle. Sivusto voi olla hyökkääjän omistama tai hyökkääjien murtama legitiimi sivusto, johon suuri määrä käyttäjiä luottaa jo valmiiksi. (Le, Welch, Gao & Komisarczuk, 2013.)

Hyökkääjien lisäämä sisältö heidän murtamalleen sivulle on usein linkki, joka uudelleenohjaa käyttäjän haitalliselle sivustolle (Mavrommatis & Monrose, Moheeb Abu Rajab Fabian, 2008). Sivu sisältää koodia, tyypillisesti JavaScriptillä kirjoitettua, joka hyväksikäyttää haavoittuvuuksia käyttäjän selaimessa, selaimen lisäosissa tai käyttöjärjestelmässä (Cova, Kruegel & Vigna, 2010; Le ym., 2013). Yleisiä selainten lisäosia ovat Adobe Acrobat, Adobe Flash Player, Apple QuickTime ja Microsoft ActiveX -ohjaimet (Le ym., 2013). Kun komentorivi-

koodi ottaa käyttäjän koneen haltuun, hyökkääjät pääsevät suorittamaan haitallisia toimia. Tämä voi tarkoittaa käyttäjän tietojen varastamista ja niiden lähettämistä hyökkääjille. Yleistä on kuitenkin ladata ja asentaa käyttäjän koneelle haittaohjelma. (Le ym., 2013.) Usein koneesta tuleekin bottiverkon osa (Cova ym., 2010).

Sood ja Zeadally (2016) neuvovat käyttäjiä olemaan avaamatta outoja viestejä tai niiden sisältämiä linkkejä. On suositeltavaa myös käyttää selaimessa vahvoja turvallisuuslisäosia, jotka rajoittavat ei-toivottujen verkkosivujen tai ponnahdusikkunoiden avautumista (Sood & Zeadally, 2016). Ylipäätään kannattaa välttää epäilyttäviä verkkosivuja tai sähköpostin mukana tulevia linkkejä.

Yrityksiä neuvotaan rajoittamaan tietoliikennettä epäilyttäville verkkosivuille. Kaikki luvattomat yhteydet ulkopuolisille verkkosivuille pitäisi keskeyttää välittömästi, kun asiakas yrittää yhdistää niihin. Kriittistä liiketoimintaa varten voi olla hyvä listata vain luotetut verkkosivut (engl. whitelist). Lisäksi keskitetysti hallitut virustorjuntaohjelmistot ja verkkosivujen estotyökalut tulisi asentaa käyttäjien laitteille rajoittamaan pääsyä ulkopuolisille verkkosivuille ja palvelimille. Käyttäjien oikeudet tulee myös olla minimaaliset. (Sood & Zeadally, 2016.)

Laitteille ei tule asentaa tarpeettomasti kolmannen osapuolen ohjelmistoja, kuten Javaa ja Adobe Flash playeria. Näitä haavoittuvia ohjelmia voidaan hyödyntää drive-by -hyökkäyksissä ja se voi johtaa tietomurtoihin. Yritykset voivat hyödyntää myös valmiita kolmannen osapuolen drive-by -hyökkäyksiä havaitsevia ohjelmistoratkaisuja. (Sood & Zeadally, 2016.)

2.5.7 Haavoittuvaiset sovellukset

KasperskyLabin vuoden 2018 toisen neljännesvuoden tilaston mukaan kyberrikollisten hyödyntämät haavoittuvaiset sovellukset olivat jakaumaltaan seuraavanlaisia: Office 67%, Android 13%, selain 12%, Adobe Flash 5%, Java 3% ja PDF 0%. KasperskyLabin havainnon mukaan vuonna 2018 2. vuosineljänneksellä Microsoft Officen osuus kyberrikollisten käyttämistä haavoittuvaisista sovelluksista tuplaantui edelliseen vuosineljännekseen nähden ja nelinkertaistui vuoden 2017 keskimäärään nähden. Kasvu johtui ensisijaisesti roskapostikampanjasta, jossa levitettiin haavoittuvuutta CVE-2017-11882 hyväksikäyttäviä dokumentteja. (Chebyshev ym., 2018.) Kyseinen haavoittuvuus mahdollistaa mielivaltaisen koodin suorittamisen nykyisen käyttäjän kontekstissa, kun Microsoft Office -ohjelmisto epäonnistuu käsittelemään kunnolla objekteja muistissa. Haavoittuvuuden hyväksikäyttö vaatii, että käyttäjä avaa tiedoston haavoittuvaisella Microsoft Office -versiolla. (Microsoft, 2017a.) Haavoittuvuuden CVSS-pisteytys on 9.3 (CVE-Details).

Haavoittuvuus liittyi jokaisesta Microsoft Office -versiosta löytyneeseen vanhentuneeseen Equation Editor -komponenttiin. Lisäksi se sallii useita piilokeinoja (engl. obfuscations) suojauksen ohittamiseen. Nämä kaksi tekijää tekivät tästä haavoittuvuudesta suosituimman työkalun rikollisten käsissä toisella neljännesvuodella. (Chebyshev ym., 2018.)

Kasperskyn tilaston (2018) mukaan myös Microsoft Officen kautta hyväksikäytettävien Adobe Flash-exploittien lukumäärä on noussut. Toisen neljännesvuoden aikana löytyi uusi nollapäivähaavoittuvuus CVE-2018-5002. Sen exploit levisi XLSX-tiedostossa ja käytti huonosti tunnettua tekniikkaa, joka salli exploitin latauksen etälähteestä sen sijaan, että se olisi ollut itse dokumentissa mukana. (Chebyshev ym., 2018.) Haavoittuvuuden CVSS-pisteytys on korkein mahdollinen eli 10.0 (CVE-Details).

Toisella vuosineljänneksellä Kaspersky havaitsi myös kasvua tietoverkkohyökkäyksissä. Nämä liittyivät suurimmaksi osin niiden haavoittuvuuksien hyväksikäyttämiseen, jotka paikattiin tietoturvapäivityksellä MS17-010. (Chebyshev ym., 2018.) Kyseiset haavoittuvuudet liittyivät siihen, miten Windows SMB -palvelin käsittelee tiettyjä pyyntöjä. Haavoittuvuuksien hyväksikäyttö mahdollisti koodin suorittamisen kohdepalvelimella. (Microsoft, 2017b.)

Haavoittuvaisten sovellusten aiheuttamia uhkia voi ehkäistä päivittämällä sovellukset aina viimeisimpään versioon. Käyttäjien on syytä noudattaa varovaisuutta käsitellessään sähköpostien mukana tulevia dokumentteja, jotta eivät tule ladanneeksi haitallisia dokumentteja.

2.5.8 Uhkien tausta ja seurauksia

Symantecin (2018), McAfeen (2018) ja Kasperskyn (Chebyshev ym., 2018) tilastoissa uhkien taustalla mainitaan yleisesti ”kyberrikolliset”. Tämän tutkielman kannalta ei ole olennaista jakaa kyberrikollisia edelleen mahdollisiin alaryhmiin.

Kyberrikollisten motiivina voi olla itse hakkerointi, uteliaisuus, vallan hankkiminen ja ryhmään kuuluminen (Van Beveren, 2000, Hua & Bapna, 2013 mukaan) tai hauskanpito tai tunnustuksen saaminen vertaisiltaan (Sabillon, Cano, Cavaller & Serra, 2016).

Yksi keskeinen motivaatiotekijä kyberrikollisten taustalla on kuitenkin raha. Aiemmin edistyneimmät rikollisryhmät myivät tavaroita (engl. goods) kuten varastettua dataa tai tietokoneviruksia, mutta tässä on tapahtunut siirtyminen kyberrikospalveluiden muodostamiseen. Kyberrikollisten palvelutarjonnasta on tullut laaja: Heiltä voi esimerkiksi tilata haittaohjelmia, palvelunestohyökkäyksiä ja ylipäätään hakkerointipalveluja, ja näitä voi ostaa kuka vain: hallitukset, aktivistit, terroristit ja rikolliset. (Filshtinskiy, 2013.)

Haittaohjelmien muuttumisesta yhä monimutkaisemmiksi onkin nähtävissä, kuinka motivaatio uteliaisuudesta ja julkisuuden tai jännityksen hakemisesta on muuttunut motivaatioksi laittomasta rahallisesta hyödystä (Choo, 2011a). Lisäksi avoimesti saatavilla olevien helppokäyttöisten työkalujen myötä haittaohjelmien tekeminen ei vaadi enää ammattilaistason ohjelmointi- tai hakkerointiosaamista (Choo, 2011b).

Useista tässä luvussa luetelluista haittaohjelmista voikin nähdä, että ne ovat tehty tuomaan tekijöilleen tai käyttäjilleen rahaa uhrien kustannuksella: kirityshaittaohjelmat lunnaiden avulla, pankkitroijalaiset varastettujen pankkitunnusten avulla ja kryptovaluutan louhijat uhrien koneiden kapasiteetin avulla.

Kybermaailmassa yritykseen kohdistuvalla hyökkäyksellä voi olla vakavia seurauksia yritykselle. Hyökkäyksen aiheuttamien jälkien korjaaminen vie yrityksen resursseja, kuten aikaa ja rahaa ja voi vaikuttaa liiketoiminnan kulkuun.

Lisäksi kyberhyökkäys voi tuhota liiketoiminnan taloudellisesti pankkitunnusten menettämisen myötä ja materiaalisesti tiedollisen omaisuuden tai asiakasdatan menettämisen myötä (Valli, Martinus & Johnstone, 2014). Asiakkaiden henkilökohtaisten tietojen paljastuminen voi puolestaan aiheuttaa asiakkaiden joutumisen identiteettivarkauksien uhreiksi (Valli ym., 2014).

Kyberhyökkäyksen uhriksi joutuminen voi aiheuttaa yrityksen maineelle suurta vahinkoa. Suorien kyberrikoksen aiheuttamien kustannusten lisäksi yrityksen asiakkaat voivat menettää luottamuksensa yritykseen. Näin yritys voi menettää myös tulevaisuuden kauppoja. Haavoittuvuus kyberhyökkäyksille voi vähentää yrityksen markkina-arvoa. Kyberrikoksen uhriksi joutuminen voi laskea myös osakkeen arvoa, varsinkin jos tapauksesta kerrotaan uutisissa. (Smith, K. T., Smith, M. & Smith, J. L., 2011.)

2.6 Langattomat verkot turvallisuusnäkökulmasta

Langattomat verkot (IEEE 802.11 standardeihin pohjautuva WLAN) on suosittu teknologia niiden liikkuvuuden, skaalautuvuuden ja helppokäyttöisyyden vuoksi (Nikbakhsh, Manaf, Zamani & Janbeglou, 2012). Burns, Wu, Du ja Zhu (2017) väittävätkin Wi-Fi:n olevan itse asiassa yleisin teknologia internettiin pääsemiseksi. Wi-Fi-yhteensopivat laitteet yhdistävät WLAN:iin Wi-Fi-tukiaseman avulla. Samalla näistä langattomista verkoista kuitenkin aiheutuu tietoturvaongelmia. WLAN:ien käyttö lisää potentiaalisia uhkia niiden käyttäjiä, kuten kotikäyttäjiä ja yrityksiä kohtaan (Waliullah & Gan, 2014). Myös tutkimuksen kohteena olevassa yrityksessä on WLAN käytössä, joten käydään tässä alaluvussa läpi, mitä haavoittuvuuksia niiden salauksista löytyy ja mitä hyökkäyksiä niihin liittyy.

2.6.1 Langattomien verkkojen salaukset

Ensinnäkin WLAN:in salausprotokollat kuten WEP ja WPA/WPA2 ovat haavoittuvaisia. Vuonna 1999 kehitettiin WEP-salaus (Wired Equivalent Privacy), jonka tarkoitus nimensä mukaisesti oli tarjota samanlainen yksityisyyden taso kuin langallisessa verkossa. Pian kuitenkin todettiin, että WEP:iin liittyi vakavia tietoturvaongelmia. WEP ei tarjonnut tehokasta tekniikkaa avainten hallintaan ja sen käyttämä salausalgoritmi RC4 oli riittämätön. WEP:n tietoturva-aukot pyrittiin paikkaamaan IEEE 802.11i tietoturvastandardilla, WPA:lla (Wi-Fi protected access) viisi vuotta myöhemmin vuonna 2004. Vaikka WPA:ta pidetään turvallisempana kuin WEP:tä, siinä on silti käytetty uudelleen WEP:n algoritmia. Siksi WPA on haavoittuvainen nelikättely (engl. 4-way handshake) pro-

tokollaan kohdistuville sanakirja- ja raakavoima -hyökkäyksille ja palvelunestohyökkäyksille (Stimpson ym., 2012, Waliullah & Gan, 2014 mukaan.)

WPA:ssa käytetty TKIP (Temporary key integrity protocol) on WPA-2:ssa korvattu CCM-protokollalla (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). RC4 puolestaan on WPA-2:ssa korvattu AES:lla (Advance Encryption Standard). Vaikka WPA-2-AES koetaan turvallisena, on se silti haavoittuvainen palvelunesto-, sanakirja– ja sisäisille hyökkäyksille (Wang, Srinivasan & Bhattacharjee, 2011, Waliullah & Gan, 2014 mukaan.)

Vuonna 2017 uutisoitiin laajasti WPA-2:sta löytyneestä haavoittuvuudesta, joka mahdollistaa hyökkääjälle pääsyn salattuun Wi-Fi-verkkoon eli KRACK-hyökkäyksen. KRACK-hyökkäys kohdistuu WPA:n nelitiekättelyyn. Siinä huijataan uhri asentamaan uudelleen jo käytetty tai käytössä oleva avain manipuloimalla ja toistamalla kryptografisia kättelyviestejä. (Fehér & Sandor, 2018.)

Haavoittuvuus on tehokas erityisesti Linuxissa ja Androidissa. Windowsissa ja Macissa tarvitaan suurempi määrä paketteja haavoittuvuuden hyödyntämiseksi. (Realpe, Parra & Velandia, 2018.)

Uusin salausprotokolla on WPA-3, joka julkaistiin kesäkuussa 2018. Se on suunniteltu vahvistamaan Wi-Fi verkkojen turvallisuutta ja korjaamaan edellisten versioiden ongelmia. WPA-3 käyttää salasanaan pohjautuvaa SAE-tekniikkaa (Simultaneous Authentication of Equals) autentikoimaan asiakas tukiasemaan. Protokolla käyttää ”dragonfly” -kättelyä hyödyntääkseen diskreettiä logaritmista ja elliptisten käyrien kryptografiaa. Kättelyssä syntyy PMK (Pairwise Master Key), jota käytetään WPA-2:ssakin käytetyssä nelitiekättelyssä. SAE-protokolla käyttää jaettua salasanaa vain todennukseen, ei PMK:n johtamiseen. Vaikka WPA-3 suojaa useilta hyökkäyksiltä, joille aiemmat protokollat ovat alttiita, ei WPA-3 suojaa tämän hetken tiedon mukaan kaikilta hyökkäyksiltä. Esimerkiksi evil twin -, SSL stripping -, ja DNS spoofing -hyökkäyksille WPA-3 on altis. Haavoittuvuus ARP spoofing- ja Rogue Access Point -hyökkäyksille on lisäksi ratkaistu vain osittain. (Kohlios & Hayajneh, 2018.)

2.6.2 Langattomien verkkojen hyökkäyksiä

Langattomien verkkojen ongelma on niiden ulottuminen haluttujen rajojen ulkopuolelle. Vaikka tukiasemien ja antennien sijaintiin voi vaikuttaa, on haastavaa täysin estää verkon ulottuminen esimerkiksi yrityksen toimitilojen ulkopuolelle. (Waliullah & Gan, 2014.) Tästä niiden luonteesta johtuen ne ovatkin alttiita erilaisille hyökkäyksille.

Langattomiin verkkoihin liittyvät hyökkäykset voidaan luokitella eri tavoin. Esimerkiksi Waliullah ja Gan (2014) jakavat hyökkäykset WLAN-teknologiaa kohtaan passiivisiin ja aktiivisiin hyökkäyksiin. Lisäksi Waliullah ja Gan (2014) luokittelevat hyökkäyksiä vielä niiden vaikutuksen mukaan: hyökkäykset voivat kohdistua verkon luottamuksellisuuteen, eheyteen, saatavuuteen, pääsyn hallintaan ja todennukseen (engl. authentication). Tällaisessa jaottelussa ongelmana on, että hyökkäyksen vaikutus voi ulottua useampaankin

tietoturvavaatimukseen kuin vain yhteen ja vaikutuksen arviointi voi olla lisäksi tulkinnanvaraista.

Toinen tapa jaotella langattomiin verkkoihin liittyviä hyökkäyksiä on käyttää OSI-mallia, sillä langattomat verkon noudattavat yleisesti OSI-mallia koostuen sovellus-, kuljetus-, verkko-, siirtoyhteys- ja fyysisestä kerroksesta. Jokaisella OSI-kerroksella on sille ominaiset tietoturvahaasteet, sillä eri kerroksissa on käytössä eri protokollia. (Zou, Zhu, Wang & Hanzo, 2016.)

Fyysisen kerroksen hyökkäyksiin lukeutuvat esimerkiksi salakuuntelu ja häirintä (Zou ym., 2016). Salakuuntelussa on kyse pääsystä verkkoliikenteeseen ja viestien sisällön lukemisesta (Waliullah & Gan, 2014). Erityisesti salaamattomat käyttäjätunnukset ja salasanat ovat kiinnostavaa tietoa (Noor & Hassan, 2013). Vaikka liikenne olisi salattua, voi hyökkääjä onnistua murtamaan salatutkin viestit (Waliullah & Gan, 2014). Häirintähyökkäys, tai myös nimeltään palvelunestohyökkäys, puolestaan tarkoittaa tilannetta, jossa hyökkääjä häiritsee tahallaan verkon käyttäjien välistä viestintää. Häirinnällä pyritään estämään käyttäjiä pääsemästä verkon resursseihin. (Zou ym., 2016.)

Siirtoyhteyskerrokseen (MAC-layer) kohdistuvia hyökkäyksiä ovat esimerkiksi MAC:in väärennös, välimieshyökkäys ja verkkoinjektio. MAC:in väärennöksessä hyökkääjä muuttaa oman MAC-osoitteensa, mikä mahdollistaa hyökkääjän identiteetin piilottamisen tai jonkin toisen verkkonoodin esittämisen. Verkkoinjektiossa pyritään estämään verkkolaitteiden, kuten reitittimien ja kytkinten toiminta injektoimalla väärennettyjä verkon uudelleenkonfigurointikomentoja. Tällä tavoin koko verkko voi lamaantua, minkä jälkeen tarvitaan uudelleenkäynnistys tai jopa laitteiden uudelleenohjelmointia. (Zou ym., 2016.)

Välimieshyökkäyksellä viitataan tyypillisesti tilanteeseen, missä hyökkääjä salakuuntelee liikennettä kaapatakseen kahden keskenään kommunikoivan noodin MAC-osoitteen. Sitten hyökkääjä esittää näitä kahta uhria, jolloin hyökkääjä pääsee toimimaan uhrien välissä. Uhreille tilanne vaikuttaa siltä, kuin he kommunikoisivat suoraan toistensa kanssa yksityisesti. (Zou ym., 2016.) Hyökkääjä voi esimeriksi esiintyä käyttäjälle tukiasemana ja tukiasemalle oikeana käyttäjänä (Waliullah & Gan, 2014). Toisaalta Wang ja Wyglinski (2016) mukaan välimieshyökkäykselle ei ole annettu selkeää määritelmää ja se voi olla myös yhdistelmä eri hyökkäyksiä, kuten evil twin- ja rogue access point -hyökkäys.

Evil twin on yksi rogue access point -tyyppinen hyökkäys (Alotaibi & Elleithy, 2016). Evil twin -tukiasema on aitoa tukiasemaa esittävä mutta hyökkääjän hallussa oleva tukiasema. Usein sen SSID on sama kuin aidon tukiaseman. Näin käyttäjät voivat vahingossa yhdistää väärennettyyn tukiasemaan. (Wang, Le & Wyglinski, 2016.) Varsinkin monilta julkisilta paikoilta löytyvät avoimet tukiasemat ovat haavoittuvaisia evil twin -hyökkäykselle (Burns ym., 2017).

Rogue access point voi myös olla esimerkiksi valtuutettuun verkkoon yhdistetty väärennetty tukiasema, jota hyökkääjä voi käyttää takaovena. Takaovi verkossa auttaisi hyökkääjää ohittamaan esimerkiksi palomuurin ja IPS:n. (Wang, Le & Wyglinski, 2016.)

Verkkokerroksen hyökkäyksiin voidaan sisällyttää IP:n väärennös ja kaappaus sekä Smurf-hyökkäys. IP:n väärennöksellä hyökkääjä pyrkii piilottamaan oikean identiteettinsä tai esittämään toista verkkonoodia suorittaessaan luvattomia toimia. IP:n kaappauksessa kaapataan toisen käyttäjän IP-osoite. Mikäli hyökkääjä onnistuu kaappauksessa, hän pystyy sulkemaan oikean käyttäjän pois verkosta ja luomaan uuden yhteyden verkkoon esiintyen oikeana käyttäjänä. Tämä voi mahdollistaa hyökkääjälle pääsyn luottamukselliseen tietoon. Smurf-hyökkäys puolestaan on palvelunestohyökkäys, missä lähetetään uhrille suuri määrä ICMP-paketteja, joiden lähde IP-osoite on väärennetty. Uhrin vastaanottaessa ICMP-pyynnöt hän joutuu lähettämään ICMP-vastaukset, mikä johtaa suureen määrään liikennettä uhrin verkossa. Suuri määrä ICMP-pyyntöjä voi lamauttaa uhrin verkon. Smurf-hyökkäyksen yksi vastakeino on varmistaa, etteivät käyttäjät ja reitittimet jatkuvasti vastaa ICMP-pyyntöihin. Toisaalta myös palomuurin voi asettaa hylkäämään haitalliset paketit. (Zou ym., 2016.)

Kuljetuskerrokseen liittyy TCP ja UDP -protokolliin kohdistuvat hyökkäykset: TCP ja UDP ”flooding” ja TCP sekvenssinumeroiden ennustus. TCP flooding -hyökkäys on palvelunestohyökkäys, missä hyökkääjä lähettää suuren määrän ping-pyyntöjä, kuten ICMP echo -pyyntöjä uhrinoodille, ja uhri vastaa ping-vastauksilla. TCP sekvenssien ennustus -hyökkäys puolestaan pyrkii ennustamaan lähettävän noodin TCP-pakettien sekvenssi indeksin (engl. sequence index) ja sitten väärentämään noodin TCP-paketit. Tämä vaikuttaa datan eheyteen. UDP on TCP:n tavoin altis flooding-hyökkäyksille, joissa on kyse UDP-pakettien lähettämisestä suurina määrinä. Kohde joutuu vastaamaan paketteihin ja näin sitä eivät pysty enää muut verkon noodit saavuttaa. UDP flooding -hyökkäystä voidaan ehkäistä rajoittamalla UDP-pakettien vastaustiheyttä ja suodattamalla palomuurin avulla haitallisia UDP-paketteja. (Zou ym., 2016.)

Sovelluskerroksessa toimivat protokollat HTTP, FTP ja SMTP ovat myöskin alttiita hyökkäyksille. Keskeiset HTTP-hyökkäykset sisältävät haittaohjelmahyökkäykset, kuten troijalaiset ja virukset, SQL-injektio- ja XSS-hyökkäykset. FTP:hen liittyy FTP bounce- ja directory traversal -hyökkäykset. FTP bounce -hyökkäys hyödyntää PORT -komentoa saadakseen pääsyn portteihin uhrinoodin kautta, toimien näin välimiehenä. Directory traversal -hyökkäyksessä pyritään saamaan luvaton pääsy tiedostojärjestelmään hyödyntämällä haavoittuvuutta käyttäjän asettamien tiedostonimien validoinnin aikana. SMTP-hyökkäyksiin lukeutuvat salasanojen kaappaus, SMTP-virukset ja -madot sekä sähköpostin väärennös. SMTP ei salaa tietoja, kuten käyttäjätunnuksia, salasanoja eikä itse STMP-palvelinten ja asiakkaiden välillä kuljetettuja sähköpostiviestejä. Sovelluskerroksen hyökkäyksiä voi ehkäistä virustorjuntaohjelmistoilla ja palomuureilla. (Zou ym., 2016.)

2.6.3 WLAN:in suojauskeinoja

Edellä mainitut hyökkäykset osoittavat, kuinka tärkeää yritykselle ja myös tavalliselle kotikäyttäjälle on suojata langaton verkko. Vaikka kaikilta hyökkäyk-

siltä ei voikaan täysin suojautua, on silti keinoja, joilla uhkia voi vähentää. (Waliullah & Gan, 2014.) Huomattavaa on myös, että eri hyökkäysten havaitsemista tai ehkäisemistä on tutkittu runsaasti ja niihin esitetty useita keinoja. Esimerkiksi rogue access point -hyökkäyksen havaitsemista on tutkittu sekä asiakkaan puolella että järjestelmänvalvojan puolella. (Noor & Hassan, 2013.)

Hyvä käytäntö WLAN:in suojaamiseen on käyttää WPA-2:ta WEP:in tai WPA:n sijaan. WPA-2:sta käyttäessä tulee tietysti käyttää pitkiä ja vahvoja salasanoja. Suuremmat yritykset voivat myös harkita sertifikaattipohjaista autentikointimekanismeja tai RADIUS:ta. (Waliullah & Gan, 2014.)

Valmistajien oletus-SSID:t, käyttäjätunnukset ja salasanat ovat helposti internetistä löydettävissä, joten ne tulisi vaihtaa laitteita käyttöönotettaessa. SSID:ksi kannattaa asettaa nimi, joka antaa mahdollisimman vähän tietoa omistajastaan. Näin hyökkääjä ei välttämättä pysty tunnistamaan verkon tarkkaa sijaintia. SSID:n piilottaminen ei kuitenkaan ole tehokas suojauskeino, sillä valmiilla työkaluilla SSID:n voi helposti selvittää. (Waliullah & Gan, 2014.)

Noor ja Hassan (2013) ehdottavat suojauskeinoksi verkon segmentointia, jotta voidaan välttää luvattomien käyttäjien pääsy ydinverkkoon. Tätä varten yritysverkossa voidaan hyödyntää VLAN:ia (Virtual Local Area Networks), jonka avulla voidaan ohjata LAN -kehykset verkossa oikeaan paikkaan ja näin estää esimerkiksi vieraiden pääsy yrityksen dataan ja palveluihin (Waliullah & Gan, 2014).

Yhdessä VLAN:in kanssa voidaan käyttää vielä NAC:ta (Network Access Control), joka on autentikointiteknologia. NAC:in avulla hallitaan käyttäjän pääsyä verkon resursseihin perustuen lähettäjän käyttäjäidentiteettiin, käyttäjän laitteen tilaan ja asetettuun politiikkaan. (Waliullah & Gan, 2014.)

Suositeltavaa on myös ottaa käyttöön murtautumisen havaitsemis- ja estämisjärjestelmiä. Näiden avulla voidaan tunnistaa murtautumiset ja ilmoittaa siitä järjestelmänvalvojille. (Waliullah & Gan, 2014.)

3 TUTKIMUKSEN TOTEUTUS

Tässä luvussa käydään läpi tutkimuksen toteuttamisen kannalta keskeisiä asioita: Määritellään tutkimusongelma, esitellään tutkimusmenetelmä sekä aineistonkeruumenetelmänä tietoturvakatsaus.

3.1 Tutkimusongelma

Tutkimusongelma on kohdeyrityksen verkon tutkiminen tietoturvauhkien varalta sekä se, millaisilla keinoilla voidaan parantaa nykytilannetta. Tutkimusongelmaan liittyy verkon rakenteen selvittäminen ja tietoturvan ja siihen liittyvien muiden käsitteiden määritteleminen. Tutkielma pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

- Millainen on kohteena olevan yrityksen verkon rakenne?
- Millaisia tietoturvauhkia kohdistuu yrityksen verkkoon?
- Millaisilla keinoilla voidaan vähentää verkkoon kohdistuvia uhkia?

3.2 Tutkimusmenetelmä

Tutkielmassa käytetään konstruktiivista tutkimusotetta. Sillä luodaan teorian avulla tosielämän ongelmaan ratkaisuehdotus ja siten tuotetaan kontribuutiota sille tieteenalalle, jossa sitä sovelletaan (Kasanen, Lukka & Siitonen, 1991).

Tässä tutkimusotteessa on ydinroolissa abstrakti käsite konstruktio, joka voi olla mikä tahansa ihmisen luoma artefakti, kuten muun muassa suunnitelma, malli, diagrammi ja organisaatiorakenne. Konstruktioita ei löydetä, vaan ne keksitään tai kehitetään. Kun kehitetään jo kaikesta olemassa olevasta poikkeava konstruktio, luodaan samalla aivan uutta, jolloin konstruktio itsessään kehittää uutta todellisuutta. (Kasanen ym., 1991.)

Konstruktiivinen tutkimusote soveltuu empiirisiin tutkimuksiin ja se on kehitetty liiketaloustieteen alalla, mutta sitä sovelletaan myös esimerkiksi tietojärjestelmätieteiden ja lääketieteen alalla (Kasanen ym., 1991).

Lukka (2006) sanoo Piiraisen ja Gonzalezin (2013) mukaan perusehtojen konstruktiiviselle tutkimukselle olevan: 1) Se keskittyy todellisen elämän ongelmiin, jotka tarvitsevat ratkaisemista; 2) Se tuottaa innovatiivisen konstruktion, jonka tarkoitus on ratkaista ongelma; 3) Se sisältää yrityksen toteuttaa konstruktio, jotta voidaan testata sen käyttökelpoisuus; 4) Se sisältää tiivistä yhteistyötä tutkijan ja ammatinharjoittajien välillä; 5) Se on huolellisesti linkitetty olemassa olevaan teoreettiseen tietoon; 6) Se pyrkii luomaan teoreettista kontribuutiota.

Tutkielman lähtökohtana on kohdeyrityksen tietohallinnossa huomattu tarve tietoverkon turvallisuusratkaisujen ja -käytäntöjen päivittämiseksi ajankohtaiseksi, mutta ei ole tarkkaa tietoa, mitä kohtia pitäisi päivittää tai kehittää. Tavoitteena on ratkaista tämä tekemällä kohdeyrityksen verkkoon tietoturvakatsaus, jolla saadaan selville verkon nykytilanne. Katsauksen tulosten perusteella kohdeyritykselle laaditaan raportti, joka sisältää parannusehdotuksia ja suosituksia nykytilanteen parantamiseksi. Vastaavanlaista katsausta ja siitä johdettua raporttia ei ole kohdeyrityksessä aiemmin tehty. Näin ollen tämä katsaus toimii samalla pohjana mahdollisesti tulevaisuudessa tehtäville katsauksille yrityksessä.

Konstruktio on siis tässä tapauksessa kohdeyritykselle laadittava raportti suosituksista, joiden avulla kohdeyritys voi suojata verkkoaan paremmin sekä sisä- että ulkopuolelta kohdistuviin uhkiin. Raportin tavoite on parantaa yrityksen verkon tietoturvallisuutta, parantaa sen vastustuskykyä tietoverkkouhkille. Raportin käyttökelpoisuutta lopulta arvioidaan yrityksen toiminnan kannalta. Raportti validoidaan kohdeyrityksen yhteyshenkilöiden avulla. Validoinnissa esitellään tietoturvakatsauksen tulokset ja niistä laaditut suositukset, ja pyydetään yhteyshenkilöltä lausunto siitä, ovatko tulokset kuvattu oikein. Mikäli yrityksessä ollaan sitä mieltä, että tulokset ovat kuvattu oikein, tulokset ovat validoitu.

3.3 Tietoturvakatsaus

Tässä tutkielmassa aineistonkeruumenetelmänä käytetään tietoturvakatsausta (engl. security audit). Tietoturvakatsausprosessia ja tietoturvakatsauksen tekemistä käytännössä on tutkittu monipuolisesti. Tietoturvakatsauksen avulla voidaan arvioida organisaation kykyä suojella omaisuuttaan (Onwubiko, 2009).

Pereira ja Santos (2010) tarkentavat, että katsausprosessin avulla saadaan todisteita organisaation tietojärjestelmien turvallisuuspolitiikan tehokkuudesta ylläpitää omaisuuden luottamuksellisuutta, eheyttä ja saatavuutta, jotka ovat tyypillisiä (tieto)turvallisuustavoitteita.

Bin Baharin, Din, Jamalundin ja Tahir (2003) ehdottavat tutkimuksessaan kolmannen osapuolen tietoturvakatsaus -mallia, joka keskittyy yhteen osa-

alueeseen, kuten palomuuriin. Bin Baharin ym. (2003) mukaan katsaus on sykli, johon kuuluu seuraavat vaiheet: potentiaalisten haavoittuvuuksien tunnistaminen, haavoittuvuuksien arviointi, vastatoimien arviointi, vastatoimien käyttöönotto, testaaminen (hyökkäyksen simulointi), seuraaminen (todisteet hyökkäyksestä), ajan tasalla pysyminen uusien haavoittuvuuksien varalta ja prosessin toistaminen.

Tietoturvakatsauksen tekoon ei ole yhtä oikeaa lähestymistapaa, vaan sopiva näkökulma voidaan valita tapauskohtaisesti. Esimerkiksi Lo ja Marchand (2004) kuvaavat artikkelissaan katsauksen toteuttamista käytännössä: He valitsivat ylhäältä alaspäin suuntautuvan lähestymistavan tietoturvakatsauksen suorittamiseksi yritykseen. He aloittivat porttiskannauksella ulkopuolelta ja etenivät yrityksen sisäpuolelle sekä organisatorisessa että teknologisessa mielessä. He ottivat huomioon myös käyttäjien roolin tietoturvan toteutumisessa.

Tietoturvakatsausten tulisi olla säännöllisiä: niitä ei tulisi käyttää pelkästään silloin, kun ei-toivottu tapahtuma on jo sattunut, vaan niitä tulisi käyttää myös ennakoivasti arvioimaan organisaation nykyisiä turvallisuuskäytäntöjä. Hyökkäysten, uhkien ja haavoittuvuuksien jatkuva tutkiminen on tärkeää, sillä ne kehittyvät jatkuvasti ja niillä voi olla merkittäviä vaikutuksia organisaatioon. (Pereira & Santos, 2010.)

Tässä tutkielmassa tietoturvakatsaus suoritettiin sovitusti kohdeyrityksen kanssa. Määriteltiin alussa ne osa-alueet, joita sai tutkia ja millaisilla työkaluilla. Sovittiin, että mikäli tutkimuksessa löytyy merkittäviä haavoittuvuuksia, niistä raportoidaan välittömästi, jotta ne voidaan paikata mahdollisimman nopeasti. Ottaen huomioon, että tietoturvakatsauksella voi paljastua yrityksestä arkaluontoisia tietoja, tuli yrityksen kanssa sopia liian paljastavien tietojen naamioinnista tutkielman julkaistavassa versiossa.

Kuten tietoturvakatsausta määriteltäessä todettiin, sopiva lähestymistapa katsauksen tekoon voidaan valita tapauskohtaisesti. Tässä tutkielmassa tietoturvakatsaukseen valittiin lähiverkon näkökulma. Lähdettiin liikkeelle langattoman lähiverkon ulkopuolelta ja pyrittiin murtautumaan sen läpi sisäverkkoon. Sisäverkossa suoritettiin porttiskannauksia, sillä porttiskannaus auttaa löytämään avoinna olevat portit, joihin voi kohdistaa hyökkäyksiä. Muodostettiin myös kuva sisäverkon rakenteesta skannausten tulosten perusteella. Skannausten avulla voitiin paikantaa verkosta haavoittuvia laitteita. Kun haavoittuvuudet oli tunnistettu, saatiin vielä suorittaa yksinkertaisia hyökkäyksiä yrityksen osoittamiin laitteisiin. Lopulta löydökset koottiin yritykselle laadittavaan raporttiin. Laadittiin myös lista suosituksista, joiden avulla yritys voi parantaa verkkonsa tietoturvaa.

3.4 Käytettävät työkalut

Tämän tutkielman katsausosuudessa käytetään kannettavaa tietokonetta, jossa on käyttöjärjestelmänä Kali Linux. Kali Linuxista löytyy valmiina monia penetraatiotestaukseen liittyviä työkaluja, joita hyödynnetään tässä tutkielmassa.

Tässä tutkimuksessa käytettäviä työkaluja ovat muun muassa aircrack-ng, arpscan, Zenmap, Nmap, Metasploit Framework, PRET, arpspoof, urlsnarf, driftnet ja sslstrip.

Työkalut valittiin sillä perusteella, että ne ovat tutkielman tekijälle entuudestaan tuttuja ja ne ovat aiemmassa käytössä hyviksi ja toimiviksi havaittuja.

4 YRITYKSEN VERKON HAAVOITTUVUUKSIA

Yrityksen verkon haavoittuvuuksien kartoittaminen aloitettiin langattomien verkkojen tutkimisella. Pyrittiin saamaan selville verkon salasana, jotta saataisiin pääsy yrityksen sisäverkkoon. Sisäverkossa tehtiin porttiskannauksia verkkotopologian saamiseksi ja haavoittuvien laitteiden löytymiseksi. Tutkittiin myös tulostimia ja suoritettiin yksinkertainen välimieshyökkäys. Välimieshyökkäyksen toteutustapa valittiin sillä perusteella, että se oli kohdennettavissa vain tiettyyn uhriin.

Verkkojen tutkimisessa käytetyt työkalut ja menetelmät hyväksytettiin etukäteen yrityksen yhteyshenkilöllä.

Tutkimus tehtiin käyttämällä yritykseltä saatua tietokonetta. Tietokone oli aiemmin ollut käytössä, mutta siitä oli poistettu käyttöjärjestelmä. Tutkimusta varten koneeseen asennettiin Kali Linux 2019.1.

4.1 Langaton lähiverkko

Aloitettiin yrityksen verkon tutkiminen kartoittamalla lähistöllä olevat langattomat lähiverkot. Tämä tehtiin laittamalla verkkokortti monitorointitilaan komennolla airmon-ng start wlan0, joka mahdollistaa kaikkien ilmassa liikkuvien pakettien kuuntelun.

Komennolla airodump-ng wlan0mon saatiin näkyviin lähistöllä olevat verkot. Seurattiin liikennettä kaksi minuuttia, jonka kuluttua havaittiin 46 eri verkkoa. Näiden joukossa olivat yrityksen toimistoverkko, vierasverkko ja kaksi muuta verkkoa. Kaikkien ssid:t olivat näkyvillä. Kaksi verkoista käyttää kanavaa 11, yksi kanavaa 2 ja yksi kanavaa 3.

Seuraavaksi asetettiin airodump-ng kuuntelemaan yrityksen toimistoverkkoa komennolla airodump-ng -c 2 -w yrityswlan --bssid BSSID wlan0mon. Havaittiin, että verkkoon oli kytkeytynyt 9 laitetta, joista yksi oli tutkielman tekijän matkapuhelin.

Kohdistettiin deautentikointihyökkäys kyseiseen matkapuhelimeen komennolla aireplay-ng -0 1 -a BSSID -c MAC wlan0mon, jotta saataisiin kaapattua verkkoon liittymisen kättely. Kaapatun kättelyn avulla voidaan yrittää selvittää verkon salasanaa. Aireplay-ng -komennon jälkeen toiseen terminaaliin (jossa käynnissä airodump-ng) ilmestyi WPA Handshake: (BSSID). Tämä tarkoitti, että kättely saatiin taltioitua.

Verkon salasanan murtamiseen liittyen mainittakoon ensimmäiseksi, että oli tiedossa, ettei salasana esiinny salasanalistoissa eikä sanakirjoissa edes osittain. Tästä syystä jätettiin tekemättä sanakirjahyökkäykset. Yrityksen puolelta haluttiin kuitenkin selvittää, olisiko salasana murrettavissa kohtuullisessa ajassa eri maskivariaatioiden avulla. Maskit perustuivat siihen, millä tavalla salasanan voi rakentaa verkon ssid:n perusteella.

Yritettiin siis verkon salasanan murtamista Hashcat-työkalulla. Muutettiin aluksi kättelyn sisältävä tiedosto hashcatille sopivaan muotoon. Ajettiin hashcat -m 2500 -a 3 --force wlan.hccapx (maski), missä maskina käytettiin eri variaatioita. Hashcatin käynnistyttyä tarkastettiin sen tila, ja todettiin, että tutkimuskone ei ole tarpeeksi tehokas brute force -yrityksiin, sillä salasanan murtamiseen menisi Hashcatin arvion mukaan noin kolme kuukautta. Tehokkaammalla laitteistolla salauksen saisi purettua kohtuullisemmassa ajassa.

4.2 Skannaukset sisäverkossa

Skannauksia varten liityttiin yrityksen langattomaan verkkoon yhteyshenkilöltä saadun salasanan avulla. Saatiin osoitteeksi 192.168.1.100, netmask 255.255.255.0 ja broadcast 192.168.1.255.

4.2.1 Arp-kysely

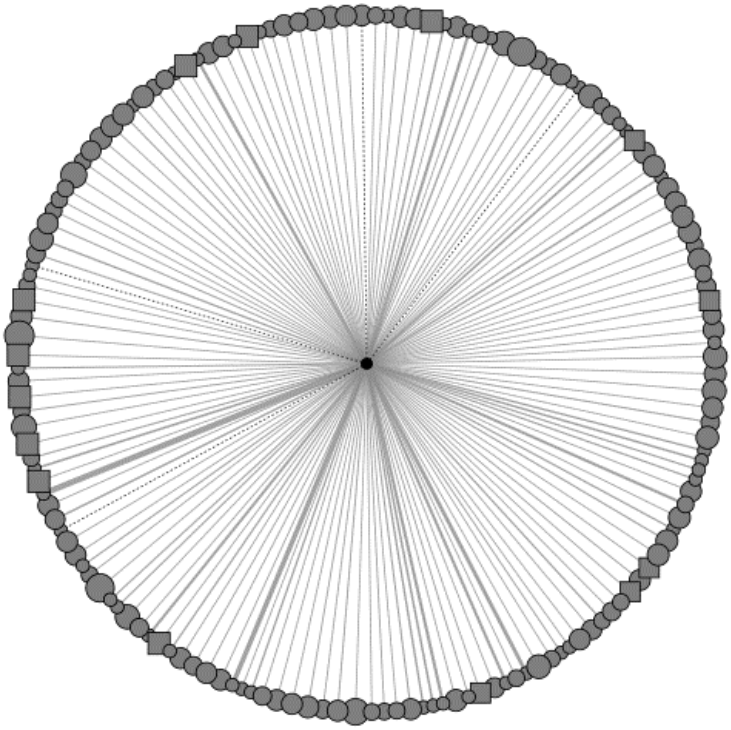
Tehtiin ensimmäiseksi arp-kysely koko verkkoon komennolla arp-scan 192.168.1.0/24. Arp-scan on ARP-pakettiskanneri, joka näyttää jokaisen aktiivisen IPv4 -laitteen aliverkossa, vaikka niissä olisi palomuuri. Arp-kyselyyn vastasi 167 laitetta.

4.2.2 Zenmap ja Nmap

Tehtiin sisäverkon skannaus Zenmapissa. Zenmap on Nmapin graafinen käyttöliittymä, joka tarjoaa useita toimintoja skannausten tutkimiseen ja tallentamiseen (nmap.org).

Skannattiin verkkoa --traceroute -valinnalla ja selvitettiin samalla myös laitteiden ohjelmisto- ja käyttöjärjestelmäversiot -sV ja -O -valinnoilla. Tarkasteltiin verkon topologiaa Zenmapin piirtämän kuvaajan avulla (KUVIO 1). Kuvaajan ja Zenmapissa suoritetun nmapin tulosten perusteella kaikki verkon laitteet ovat yhden hypyn päässä toisistaan ja samassa segmentissä. Verkko on

siis ”litteä”: Jos päästään yhdelle laitteelle verkossa, voidaan saavuttaa loputkin verkon laitteet.



KUVIO 1 Zenmapin piirtämä kuvaaja verkon rakenteesta

4.2.3 FTP

Löydettiin 4 avointa ftp-palvelua portista 21: palvelimesta ja kolmesta tulostimesta. Tilassa ”closed” oli 38 porttia ja tilassa ”filtered” 70 porttia. Selvitettiin, saisiko Metasploit frameworkin avulla ftp-versiot selville niistä neljästä laitteesta, joissa ftp-palvelu oli avoinna. Metasploit antoi tarkat tiedot kahden tulostimen osalta, yhden tulostimen ja palvelimen tiedot puolestaan jäivät vajaiksi.

Tarkastettiin vielä Metasploitin avulla, salliiko ftp-palvelu anonyymin kirjautumisen. Tulokseksi saatiin, että tulostimet sallivat anonyymin kirjautumisen lukuoikeuksin, mutta palvelin ei.

Otettiin vielä ftp-yhteys tulostimiin. Yhteen tulostimista yhteydenotto onnistui, mutta sillä saatiin pääsy vain yhteen tyhjään hakemistoon.

4.2.4 Telnet

Avoimia telnet -palveluita portissa 23 löytyi seitsemän, joista kuusi kuuluu kytkimille. Yksi avoin telnet-portti kuului tulostimelle, jonka osoite on 192.168.1.6. Yhteydenotto telnet-palveluun kesti pitkään. Kun yhteys oli muodostettu, kokeiltiin kirjautumista telnet-palveluun ja huomattiin sen vastaavan nopeasti kirjautumisyrityksiin. Yhteys katkaistiin kolmen epäonnistuneen yrityksen jälkeen.

Avoimen telnet-portin sisältävä tulostin on merkiltään HP:n tulostin. Vuonna 2016 HP päätti alkaa sulkea oletuksena auki olevat telnet ja ftp-portit uusista tulostimistaan (Shah, 2016) niiden turvallisuusriskien vuoksi.

4.2.5 SSH

Tarkasteltiin skannausten tuloksista avoinna olevia ssh-palvelimia. Saatiin selville, että 12 laitteessa ssh-palvelu oli avoimena. Suurin osa näistä laitteista oli kytkimiä ja langattoman verkon tukiasemia, mutta mukana oli myös hallintasovellus ja testikoneita.

Uusin käytössä oleva versio oli OpenSSH 7.5, joka on noin kaksi vuotta vanha. Uusin versio on tämän tutkielman tekohetkellä 7.9 (OpenSSH). Vanhin käytössä oleva oli OpenSSH 4.3 laitteessa osoitteessa 192.168.1.10. OpenSSH 4.3 on 13 vuotta vanha versio (OpenSSH).

4.3 -versioon löytyy ainakin 18 haavoittuvuutta, joista vakavin on CVSS-luokitukseltaan 9.3 ja aiheuttaa palveluneston ja mahdollisesti myös mielivaltaisen koodin ajamisen (CVE Details). Kyseistä versiota käyttävässä laitteessa on käyttöjärjestelmäversiona Linux kerneliversio 3.2-4.9, eli ainakin kolme vuotta, jopa 7 vuotta vanha (kernel.org). Tuolla välillä oleviin kerneleihin on löydetty useita CVSS 10-tason haavoittuvuuksia, jotka mahdollistavat esimerkiksi palveluneston tai puskurin ylivuotovirheen (CVE Details). Yhteyshenkilön mukaan kyseessä on testikone, jonka käyttötarve ei mahdollista jatkuvaa päivittämistä.

4.2.6 Palvelimet

Skannaustuloksista löydettiin yhteensä neljä palvelinta osoitteista .2, .3, .4 ja .5. Koska skannaus oli tehty -O ja -sV -valinnoilla, saatiin tuloksista selville myös palvelinten käyttöjärjestelmäversiot. Huomattiinkin, että käytössä olevat käyttöjärjestelmäversiot olivat vanhentuneita, eikä niitä enää valmistajan sivujen mukaan tueta.

Etsittiin vielä haavoittuvuuksia palvelinten käyttöjärjestelmäversioihin CVE Details-sivustolta. Löydettiin satoja raportoituja haavoittuvuuksia palvelinversiota kohden ja useita kymmeniä kriittisiä haavoittuvuuksia, jotka muun muassa mahdollistavat koodin suorittamisen etänä laitteella.

Kysyttiin yhteyshenkilöltä tarkemmin palvelinten käytöstä ja tilanteesta ja saatiin tietää, että palvelinten käyttötarve ei mahdollista jatkuvaa päivittämistä. Korjausta tähän ollaan kuitenkin tämän tutkielman tekohetkellä tekemässä. Yhteyshenkilöllä oli siis tiedossa, että palvelinten käyttöjärjestelmät ovat vanhentuneita ja sitä kautta haavoittuvaisia lukuisille hyökkäyksille.

4.2.7 TCP 80

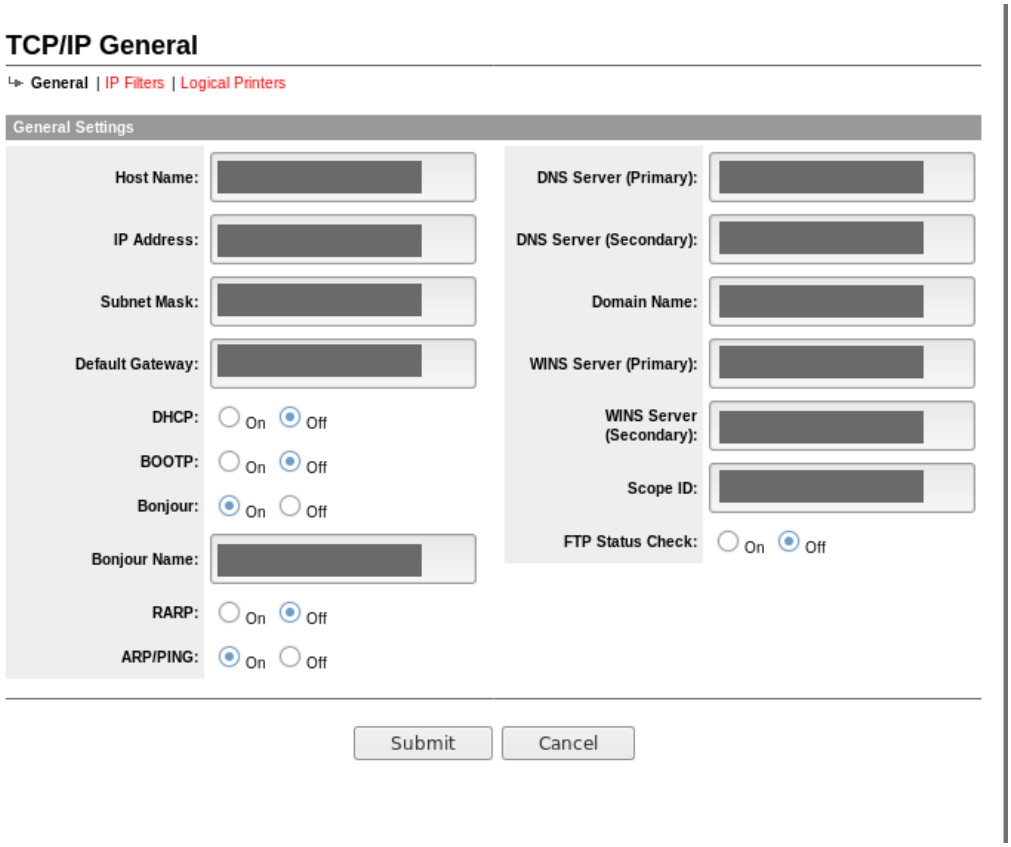
Skannausten tuloksista havaittiin myös, että useilla laitteilla oli www-palvelu portissa TCP/80 avoimena. Selaimella näitä laitteita tutkimalla päästiin niiden kirjautumis- tai hallintasivuille. Laitteiden joukossa oli tulostimia, palvelin ja hallintasovellus.

Palvelimen ja hallintasovelluksen osalta oli tiedossa, että niihin oli oletussalasanat vaihdettu, ja lisäksi kirjautumisyritykset palvelimeen tallentuvat lokiin. Näiden versiot olivat tosin vanhentuneita, ja niihin löytyi useita kriittisen tason haavoittuvuuksia CVE Details-sivustolta. Nämä haavoittuvuudet mahdollistavat muun muassa pääsyrajoitusten kiertämisen etänä ja koodin ajamisen etänä. Palvelin ja hallintasovellus jätettiin kuitenkin tutkimatta tarkemmin tässä tutkimuksessa.

Löydettiin myös laite osoitteesta .19, jossa selaimella avautui Apache2-palvelimen testisivu. Palvelimen versio on 2.4.18, joka on vanhentunut ja johon löytyy useita matalan tason ja keskitason haavoittuvuuksia. Viimeisin versio on tämän tutkielman tekohetkellä 2.4.38, johon mennessä löydetyt haavoittuvuudet on paikattu. (Apache; CVE Details.) Laitteessa oli avoinna myös MySQL-palvelu versiolla 5.7.16 portissa tcp/3306. Kyseinen versio on julkaistu vuonna 2016 ja viimeisin versio 2019 (mysql.com). Laitteessa on käyttöjärjestelmäversiona Linux kerneliversio 3.2-4.9, eli ainakin kolme vuotta, jopa 7 vuotta vanha (kernel.org). Kysyttiin laitteen tarkoitusta yhteyshenkilöltä, joka tiesi laitteen olevan testikone, muttei kuitenkaan ollut tietoinen avoimesta, keskeneräisestä www-palvelimesta.

4.2.8 Tulostimet

Tutkittiin selaimella tarkemmin tulostimia, joilla www-palvelu oli avoinna portissa TCP/80. Ensimmäiseksi havaittiin, että kaikkien tulostinten asetuksia pystyi tarkastelemaan selaimella ilman kirjautumista. Kokeiltiin kirjautua tulostinten www-käyttöliittymiin tulostinmallien oletustunnuksilla, mutta ne olivat vaihdettu. Yhteydenotto selaimella tulostimien www-käyttöliittymiin kuitenkin osoitti, että verkossa käytetään salaamatonta liikennettä huolimatta siitä, että www-käyttöliittymät vaativat käyttäjätunnusta ja salasanaa asetusten muuttamiseksi. Huomattiin myös, että osoitteessa .7 sijaitseva tulostin ei vaadi www-käyttöliittymässä kirjautumista ollenkaan asetusten muuttamiseksi (KUVIO 2), eikä koko kirjautumisvaihtoehtoa edes löydy sivulta. Sivulta löytyi kyllä toiminto, jolla voi vaihtaa salasanan. Toiminnon yhteydessä lukee, että järjestelmänvalvojan salasanalla pääsee laitteen konfiguraatioon, mutta ilmeisestikään salasana ei koske www-käyttöliittymää. Löydettiin asetuksista myös kenttä, johon oli kirjattu SMTP-palvelun salasana. Selaimen inspect element -toiminnolla voitiin nähdä kentän arvo.



KUVIO 2 Tulostimen asetuksia voi muuttaa ilman kirjautumista

Löydettiin kahdesta tulostimista, osoitteista .6 ja .7 toiminto, jolla voitiin tulostaa haluttu tiedosto suoraan käyttäjän tietokoneelta. Myös tulostimista osoitteista .20-.26 löydettiin tulostustoiminto, jolla pystyi vain tulostamaan tulostimen tietoja. Tällaisella toiminnolla voi ainakin pitää tulostimen kiireisenä ja tuhlata paperia.

Tulostimissa .24-.26 oli suoraan selaimella pääsy tulostustietoihin, joissa näkyi muun muassa tulostetun tiedoston nimi, käyttäjätunnus, tulostusaika ja sivumäärä. Selaimella päästiin tarkastelemaan myös tulostimen osoitekirjaa, jossa näkyi käyttäjän etu- ja sukunimi sekä sähköpostiosoite. Listassa näkyi työntekijöiden työsähköpostiosoitteita, joita ei ole julkisesti näkyvillä yrityksen verkkosivuilla. Huomattiin myös, että ilman kirjautumista osoitekirjaan pystyi lisäämään käyttäjiä, muokkaamaan tai poistamaan niitä. Esimerkiksi käyttäjän takana olevan sähköpostiosoitteen muuttaminen oli mahdollista. Osoitekirjan avulla työntekijät voivat tulostaa suoraan sähköpostiinsa.

Yhteen tulostimista löydettiin CVE Details -sivulta CVSS-luokitukseltaan tason 10 haavoittuvuus. Haavoittuvuus liittyy oletuksena sallittuun RFU-toimintoon (Remote Firmware Update) ja se mahdollistaa mielivaltaisen koodin ajamisen lataamalla muunnellun firmwaren päivityksen portin TCP/9100 kautta. Muunneltu firmware voi vaikuttaa laitteelle lähetettävän datan eheyteen, luottamuksellisuuteen ja saatavuuteen. Tarkistettiin laitevalmistajan sivulta, että laitteelle on saatavissa firmware -päivitys kyseisen haavoittuvuuden paikkaamiseksi. Tästä yritykselle suosituksena kyseisen laitteen päivitys.

4.3 Tulostimet PRET-työkalulla

Vaikka tietoverkkoturvallisuuteen kuuluvat olennaisesti myös päätelaitteet, kuten tietokoneet, puhelimet ja tulostimet, ei tässä tutkielmassa voitu keskittyä kaikkiin laitteisiin. Tutkimuksessa tuli huomioida, että tutkimus ei saa aiheuttaa haittaa työntekijöille eikä heidän työlleen. Näin ollen saatiin lupa tutkia kolmea eri tulostinta PRET-työkalulla (Printer Exploitation Toolkit), joka on tulostinten turvallisuuden testaamiseen tarkoitettu työkalu. Tulostimiin voi työkalun avulla kokeilla laajaa skaalaa erilaisia hyökkäyksiä (hacking-printers.net). Näistä tuli kuitenkin tutkimusta varten valita sellaiset, jotka ovat relevantteja kohdeympäristössä ja jotka eivät mahdollisesti onnistuessaan aiheuta tulostimelle pysyvää haittaa. Esimerkiksi fyysistä tuhoa aiheuttavat ja haittaohjelmia lataavat hyökkäykset jätettiin tutkimatta. Samasta syystä kokeiltiin vain esimerkkihyökkäyksiä, joissa niiden vaikutukset ja peruutustavat oli esitetty.

PRET:iä voi ajaa kolmessa eri tilassa: PS, PJL ja PCL, jotka ovat lyhennyksiä yleisistä tulostinkielistä.

PJL (Printer Job Language) on yksi tulostustehtävien hallintakieli, jolla voi hallita asetuksia, kuten paperin kokoa, nykyiselle tulostustehtävälle. PJL:ää voidaan myös käyttää vaihtamaan näytön tekstiä tai lukemaan tai kirjoittamaan laitteella olevia tiedostoja. PCL (Printer Command Language) on minimalistinen sivun kuvauskieli, jotka monet valmistajat ja laitteet tukevat. Se on kuitenkin niin rajoitettu, että sitä on vaikeaa hyväksikäyttää tietoturvallisuuden näkökulmasta. PS (PostScript) on yksi sivun kuvauskieli, joka määrittelee dokumentin ulkonäön. PostScript on itse asiassa melko kattava ohjelmointikieli; pääsy tulostimen PostScript-tulkkiin voidaan tulkita koodin suorittamiseksi, sillä mikä tahansa algoritminen funktio voidaan teoriassa toteuttaa PostScriptillä. (Müller, Schwenk, Somorovsky & Mladenov, 2016.)

Tutkielmassa testatut tulostimet olivat osoitteissa .6, .17 ja .21. Tulostimet ovat keskenään eri merkkisiä ja eri ikäisiä.

Otettiin yhteys tulostimiin PRET-työkalun kolmen eri tilan avulla ja koottiin taulukkoon tulostimien tukemat tilat (TAULUKKO 1). Merkattiin taulukkoon (TAULUKKO 1) tila tuetuksi, jos yhteys saatiin muodostettua, ja ei-tuetuksi, jos tulostin ei antanut palautetta.

TAULUKKO 1 Tulostimien tukemat tilat

Tulostimen osoite	**PS**	**PJL**	**PCL**
.6	kyllä	kyllä	kyllä
.17	kyllä	kyllä	kyllä
.21	ei	kyllä	kyllä

Koottiin myös taulukkoon ne hyökkäykset, jotka tehtiin tulostimiin osoitteissa .6, .17. ja .21 (TAULUKKO 2).

TAULUKKO 2 Taulukko käytetyistä hyökkäyksistä

Hyökkäys	Tila	Komennot
Offline-tila	pjl	offline
Tulostustehtävän säilytys	ps, pjl	hold
Tulostustehtävän kaappaus	ps	capture
Dokumentin sisällön manipulointi	ps	cross, orverlay
Dokumentin sisällön korvaus	ps	replace
Pääsy tiedostojärjestelmään	ps, pjl	ls, find, traversal…
Tunnusten paljastus	ps, pjl	lock, unlock

4.3.1 Tulostin osoitteessa .6

Tulostin .6 tuki kaikkia kolmea tilaa: PS, PJL ja PCL. PJL-tilassa saatiin ls-komennolla tiedostojärjestelmä auki. Kun edettiin tiedostojärjestelmässä, yhteys tulostimeen katkeili toistuvasti, eikä PRET pystynyt palauttamaan yhteyttä automaattisesti. Jouduttiin odottamaan useita minuutteja, ennen kuin saatiin muodostettua yhteys uudestaan PJL-tilaan. Koska ei löydetty suoraan syytä yhteyden katkeiluun ja koska tutkimukseen käytettävissä oleva aika oli rajallinen, todettiin saadut löydökset tiedostojärjestelmästä riittäviksi.

Ylipäätään tulostimien ei koskaan tulisi sallia suoraa pääsyä tiedostojärjestelmään: Mikäli hyökkääjällä on pääsy tiedostoihin, hän voi mahdollisesti nähdä luottamuksellista tietoa, kuten tallennettuja tulostustehtäviä. Tiedostojen muokkaaminen puolestaan voi johtaa koodin suorittamiseen etänä. (Müller ym., 2016.) Tulostimeen .6 muista kokeilluista hyökkäyksistä onnistui vielä näytön tekstin muuttaminen halutuksi (KUVIO 3).

KUVIO 3 Tulostimen näytön teksti saatiin vaihdettua

4.3.2 Tulostin osoitteessa .17

Tulostin .17 tuki ensimmäisillä yhteydenotoilla kaikkia kolmea tilaa: PS, PJL ja PCL. Kun alettiin ajaa hyökkäysten komentoja PS-tilassa, tulostin ajautui toistuvasti virhetilaan. Virhetilan ollessa päällä tulostaminen ei onnistunut ja se vaati manuaalisen tulostimen ohjauspaneelissa olevan napin painalluksen virhetilan pois saamiseksi. Todettiin, ettei ainakaan TAULUKKO 2 mukaisten PS-tilan hyökkäysten ajaminen onnistu tulostimessa.

PJL-tilassa onnistuttiin murtamaan tulostimessa oleva PIN-koodi. Laitteen manuaalista eikä yhteyshenkilöltä kysyttäessä käynyt kuitenkaan selväksi, mitä varten PIN-koodi oli laitteessa. PRET:n wikisivun mukaan PJL tarjoaa mahdollisuuden asettaa salasanan, jolla lukitaan pääsy tulostimen kovalevylle tai ohjauspaneeliin (control panel). Salasanan asettaminen ei kuitenkaan välttämättä tarkoita, että se oikeasti lukitsisi levyn tai paneelin. PRET:n wikisivun mukaan vain harva tulostin käyttää salasanaa lukitsemiseen, ja salasanalla voi olla omanlaisensa merkitys tulostimissa tai sitten se on turha muuttuja.

Kokeiltiinkin PIN:in murtamisen jälkeen pääsyä muun muassa tiedostojärjestelmään, mutta se ei antanut tuloksia. Sen sijaan saatiin tulostin offline-tilaan ja näyttämään ruudussa haluttu teksti. Tulostin ei vastaanottanut tulostustehtäviä offline-tilassa, joten tulostin jouduttiin käynnistämään uudestaan manuaalisesti ohjauspaneelin nappia painamalla. Samalla näytöllä näkyvä muokattu teksti katosi.

4.3.3 Tulostin osoitteessa .21

Osoitteessa .21 oleva tulostin oli melko uusi malli, johon PRET:llä sai yhteyden PJL- ja PCL -tiloilla. PS-tilalla kokeiltaessa saatiin yhteys muodostettua, mutta palaute oli puutteellista.

Kokeiltiin kaikkia TAULUKKO 2 mukaisia hyökkäyksiä ja huomattiin, ettei niistä yksikään tuottanut haluttua lopputulosta. Voitiin todeta tulostimen olevan vastustuskykyinen ainakin näillä komennoilla tehdyille hyökkäyksille.

4.3.4 Huomioita PRET-työkalusta

Ylipäätään PRET-työkalua käyttäessä yhteys katkeili hyvin usein. Esimerkiksi aluksi saatiin yhteys PS-tilaan, mutta hyökkäykseen liittyvä komento katkaisi yhteyden, eikä yhteyttä saatu muodostettua uudelleen vähään aikaan.

Yhteyden katkeamista havaittiin myös PJL-tilassa. Tämä saattoi johtua käytetystä työkalusta, tai sitten tulostin ei osannut käsitellä sille lähetettyä komentoa, jolloin yhteys kaatui. PJL-hyökkäysten toimimattomuuteen saattoi lisäksi vaikuttaa se, että PJL:stä on Müllerin (2016) mukaan olemassa ”murteita”. Tämä tarkoittaa, että valmistajilla on taipumus tukea vain osaa PJL-referenssissä olevista komennoista ja lisäksi ne saattavat lisätä omia komentojaan (Müller ym., 2016).

4.4 Yksinkertainen välimieshyökkäys

Kun oli päästy sisäverkkoon, toteutettiin yksinkertainen välimieshyökkäys ARP-väärennöksen avulla. ARP:ia (Address Resolution Protocol) käytetään muuntamaan IP-osoite fyysiseksi osoitteeksi. ARP-väärennöksessä hyökkääjä pyrkii liittämään MAC-osoitteensa toisen hostin IP-osoitteeseen, minkä tuloksena IP-osoitteeseen tarkoitettu liikenne lähetetään hyökkääjälle. Välimieshyökkäys mahdollistaa useita hyökkäyksiä verkkoon. Sen avulla voitaisiin esimerkiksi kaapata käyttäjätunnuksia ja salasanoja ja muokata uhrin näkemiä sivuja. Hyökkäystä varten otettiin ylös osapuolten IP-osoitteet: Uhrin IP-osoite oli 192.168.1.168 ja laite kannettava tietokone, jossa oli Windows 10 käyttöjärjestelmä. Gatewayn IP-osoite oli 192.168.1.1.

Ensimmäiseksi sallittiin Kalissa pakettien välitys, koska välimieshyökkäyksessä Kalin tulee toimia välittäjänä oikean reitittimen/gatewayn ja uhrin välissä. Ilman pakettien välitystä uhrin verkkoyhteys katkeaa.

Pakettien välitys toteutettiin komennolla echo ”1” > /proc/sys/net/ipv4/ip_forward. Seuraavaksi asetettiin arpspoof uhrin ja gatewayn väliin komennolla arpspoof -i wlan0 -t 192.168.1.168 192.168.1.1, ja gatewayn ja uhrin väliin komennolla arpspoof -i wlan0 -t 192.168.1.1 192.168.1.168. Tässä vaiheessa huomattiin, että uhrin verkkoyhteys katkesi (request timeout). Koska uhri ei päässyt vierailemaan verkkosivuilla, ei voitu hyödyntää myöskään esimerkiksi urlsnarfia eikä driftnetiä. Urlsnarf näyttää uhrin vierailemat verkkosivut ja driftnet näyttää kuvia uhrin vierailemilta verkkosivuilta.

Tarkistettiin iptables-säännöt, eikä havaittu ylimääräisiä estäviä sääntöjä. Kokeiltiin tehdä vastaavilla komennoilla arpspoof-väärennös myös matkapuhelimeen, mutta lopputulos oli sama, eli uhrin verkkoyhteys katkesi. Kysyttiin yhteyshenkilöltä tarkemmin käytössä olevasta gatewaysta, mutta saatujen tietojen pohjalta todettiin, ettei yhteyden katkeaminen todennäköisesti johdu siitä. Sen sijaan arpspoofin toimimattomuus saattoi johtua käytössä olleen tukiaseman ominaisuuksista.

Päätettiin yrittää välimieshyökkäystä vielä uudelleen käyttämällä langallista yhteyttä. Tämä mukailisi tilannetta, missä hyökkääjällä on fyysinen pääsy yrityksen toimitiloihin. Yrityksen verkkopistorasiat eivät ole lukittuja, joten kuka tahansa sopivan verkkokaapelin omaava voi kytkeä laitteensa yrityksen verkkoon. Tässä tapauksessa löydettiin ylimääräinen verkkokaapeli käyttämättömän työpisteen pöydältä. Yhdistettiin hyökkääjän tietokone verkkopistorasiaan ja saatiin IP-osoitteeksi 192.168.1.219. Tehtiin arpspoof samoilla komennoilla käyttäen tällä kertaa interfacena eth0 wlan0:n sijaan. Tällä kertaa uhrin verkkoyhteyteen ei kohdistunut palvelunestotila.

Käynnistettiin urlsnarf kuuntelemaan uhrin liikennettä. Uhrin vierailtua salaamattomilla verkkosivuilla urlsnarf näytti uhrin vierailemien sivujen osoitteen ja selaimen tiedot. Uhrin vieraillessa salatuilla verkkosivuilla mitään tietoja ei saatu.

Käynnistettiin myös driftnet verkkosivuilla olevien kuvien kaappaamiseksi, mutta tämä ei tuottanut toivottua lopputulosta. Kuvia ei saatu salaamattomilta sivuilta ja salatuilta sivuilta löytyvistä kuvista saatiin vain virheilmoitus driftnetiin.

Päätettiin kokeilla, saataisiinko uhri käyttämään verkkosivujen salaamatonta versiota SSLstrip-työkalun avulla. Kyseinen työkalu pakottaa uhrin selaimen kommunikoimaan http-yhteyden kautta; se ikään kuin muuttaa https:n http:ksi. Lisättiin iptables:iin uudelleenohjaussääntö porttiin 10000, jota SSLstrip kuuntelee oletuksena. Käynnistettiin SSLstrip. Uhri vieraili useilla varmasti https:ää tukevilla sivuilla, mutta sivustot eivät muuttuneet http:ksi, eikä näin ollen saatu mahdollisuutta päästä kaappaamaan suojaamattoman yhteyden yli lähetettyjä salasanoja.

On huomioitava, että selainten tietoturva on parantunut runsaasti. Tässäkin tapauksessa HSTS todennäköisesti aiheutti sen, ettei tämä hyökkäys toiminut halutulla tavalla. HSTS, eli HTTP Strict Transport Security, on mekanismi, joka sallii verkkosivujen ilmoittaa olevansa saatavilla vain suojatun yhteyden yli. Käyttäjät voivat myös ohjata selaimensa olemaan vuorovaikutuksessa verkkosivuihin vain suojatun yhteyden yli. (Jackson, Barth & Hodges, 2012.)

Toisaalta käyttäjätunnusten tai salasanojen kaappaamista varten olisi mahdollista luoda uskottava kalastelusivusto hyökkääjän omistamalla väärennetyllä sertifikaatilla. Sertifikaatin avulla hyökkääjä voisi purkaa liikenteen salauksen ja sillä voitaisiin mahdollisesti kiertää myös selaimien varoitukset. Tätä ei kuitenkaan ollut mahdollista toteuttaa tässä tutkimuksessa.

5 TULOKSET

Tämän tutkielman lopputuloksia ovat tietoturvakatsauksen löydöksistä laaditut suositukset yritykselle. Suositukset sisältävät toimenpiteitä, joiden avulla yritys voi parantaa verkkonsa turvallisuutta.

Tietoturvakatsauksen lopuksi esiteltiin katsauksen löydökset ja sitten niistä laaditut suositukset yritykselle. Alaluvussa 5.1 esitellään nämä suositukset ja alaluvussa 5.2 käydään läpi tuloksia yrityksen näkökulmasta sekä tulosten validisuutta.

5.1 Suosituksia yritykselle

Ensinnäkin yrityksen verkko on suojattu ulkopuolisilta palomuurin avulla ja langattomassa verkossa käytetään WPA-2 -salausta vahvalla salasanalla. Tutkimuksessa kuitenkin havaittiin, että sisäverkkoon päästessä hyökkääjällä on paljon hyökkäyspinta-alaa, sillä kaikki verkon laitteet ovat välittömästi saavutettavissa.

Tutkimuksessa havaittiin haavoittuvuuksia ja puutteita, jotka korjatessaan yritys voi parantaa verkkonsa tietoturvallisuutta.

Verkosta löydettiin useita päivityksen tarpeessa olevia laitteita. Toisaalta osa näistä laitteista oli syystä jätetty päivittämättä. Verkosta löydettyjen palvelimien vanhentuneesta tilanteesta yhteyshenkilö oli jo valmiiksi tietoinen ja korjausta niihin ollaan tekemässä tutkielman tekohetkellä. Tästä syystä palvelimiin liittyvät havainnot rajattiin pois yritykselle laadituista suosituksista. Muussa tapauksessa olisi suositeltu kiireellistä palvelimien päivittämistä ja niissä avoinna olevien palveluiden tarkastamista ylimääräisten varalta.

Muut löydetyt haavoittuvuudet liittyivät ylimääräisiin avoinna oleviin portteihin ja tulostimiin.

Käydään läpi tässä alaluvussa suositukset, jotka laadittiin tutkimuksen löydösten perusteella.

5.1.1 Laitteiden kytkeminen verkkoon

Tutkimuksessa huomattiin, että verkkoon pystyi liittymään vapaasti myös yritykselle kuulumattomilla laitteilla langattoman verkon salasanalla tai kytkemällä verkkokaapelin verkkopistorasiaan yrityksen toimitiloissa. Tällä tavoin sai suoraan pääsyn yrityksen sisäverkkoon ja sen kaikille laitteille.

Suosituksena yritykselle vain yrityksen erikseen hyväksymien laitteiden salliminen verkkoon MAC-osoitteiden perusteella, jotta verkkoon ei pysty liittymään hallitsemattomasti millä tahansa laitteella. Tällä keinolla voidaan ehkäistä myös työntekijöitä kytkemästä vapaasti verkkoon laitteita ja avaamasta niihin tarpeettomia portteja. Tästä esimerkkinä tutkimuksessa löydetty laite, jonka käyttöjärjestelmäversiosta ja avoinna olevista palveluista yhteyshenkilö ei ollut tietoinen.

5.1.2 Päivitykset

Tutkimuksessa löydettiin yli sata aktiivista laitetta, joista osa käytti vanhentuneita käyttöjärjestelmiä ja ohjelmistoja. Monet näistä vanhentuneista laitteista olivat kuitenkin jo yhteyshenkilöllä tiedossa. Nämä muodostavat oman kokonaisuutensa, jota käsitellään verkon segmentointiin liittyvässä suosituksessa luvussa 5.3. Siispä päivityssuositus liittyy tutkimuksessa löydettyihin vanhentuneisiin tulostimiin. Yhteen tulostimista löytyikin kriittinen haavoittuvuus, joka oli paikattavissa päivityksellä.

Suosituksena yritykselle tulostinten päivitys ja lisäksi niiden tuominen aktiivisen päivittämisen piiriin työasemien tavoin. Haavoittuvaan tulostimeen on ollut valmistajan verkkosivujen mukaan päivitys saatavilla joulukuusta 2017, mutta sitä ei ollut yrityksessä tutkielman tekohetkellä vuoden 2019 alussa vielä päivitetty.

5.1.3 Verkon segmentointi ja valvonta

Tämän hetken tilanne yrityksessä on, että verkko on vertauskuvallisesti kova pinnalta mutta pehmeä sisältä. Verkon reunalla on palomuuri sekä tunkeutumisen havaitsemisjärjestelmä (IDS), jotka valvovat sisään tulevaa liikennettä, mutta sisäverkkoon päästessä hyökkääjä voi vapaasti tutkia verkkoa ja tehdä hyökkäyksiä. Verkon ”litteys” mahdollistaa myös haittaohjelmien leviämisen verkossa.

Tutkimuksessa löydettiin useita vanhentuneita laitteita, joiden tilasta yhteyshenkilö oli tietoinen, sillä niiden käyttötarve ei mahdollista jatkuvaa päivittämistä. Verkossa on siis normaalin ylläpitorutiinin ulkopuolella oleva testilaitekanta, joita ei voi päivittää ja suojata samojen turvallisuusstandardien mukaisesti kuin muita laitteita.

Verkon tietoturvallisuuden parantamiseksi suositellaankin yritykselle verkon segmentointia testiympäristön osalta. Tällä tavoin hyökkääjälle on vai-

keampaa tehdä hyökkäyksiä koko verkkoon. Samalla voidaan rajoittaa myös käyttäjien pääsyä tiettyihin verkon resursseihin.

Suositellaan yritykselle myös sisäverkon valvontaa tunkeutumisen havaitsemisjärjestelmän (IDS) avulla epäilyttävän liikenteen havaitsemiseksi. Tässä tutkimuksessa tehdyistä toimista mikään ei näkynyt yhteyshenkilölle.

5.1.4 Tulostimet

Tutkimuksessa havaittiin, että yrityksessä on käytössä vanhoja tulostimia, joiden tietoturva on puutteellinen. Ylipäätään tulostimet ovat verkossa hyökkääjille mielenkiintoinen kohde, koska niitä ei ole suunniteltu tietoturvallisiksi ja niille lähetetään tulostettavaksi hyvinkin arkaluontoisia tietoja sisältäviä dokumentteja.

Müller ym. (2016) suosittelevat ylipäätään tulostimien tietoturvan parantamiseksi portin 9100/tcp sulkemista, mikäli porttia ei tarvita. Yksi vaihtoehto olisi myös eristää (sandbox) kaikki tulostimet erilliseen VLAN:iin, johon on pääsy vain tulostuspalvelimella (Costin, 2012, Müller ym., 2016 mukaan).

Tutkimuksessa löydettiin tulostin, joka ei vaadi kirjautumista asetuksien muuttamiseksi. Tästä suosituksena yritykselle selvitys siitä, voiko asetusten muuttamiseen saada tunnistautumisen käyttöön.

5.1.5 SMTP-tunnukset

Tutkimuksessa löydettiin selaimen avulla erään tulostimen web-käyttöliittymästä SMTP-palvelun käyttäjätunnus ja salasana. Salasana-kentän merkit pystyttiin paljastamaan selaimen inspector-työkalulla.

Varmistettiin tunnusten paikkansapitävyys yrityksen yhteyshenkilön avulla. Saatiin selville, että tunnusten löytyminen tulostimen web-käyttöliittymästä oli yritykselle erityisen mielenkiintoinen ja tärkeä löydös.

Ottaen huomioon, mihin löydetyillä tunnuksilla on yrityksessä pääsy, suositellaan yritykselle tunnusten vaihtoa ja tunnusten rajaamista järjestelmien ulkopuolelle. Jos tulostin tarvitsee SMTP:tä, suositellaan sen selvittämistä, saako tunnukset pois näkyviltä tulostimen web-käyttöliittymästä. Mikäli tulostin ei tarvitse SMTP:tä, suositellaan koko toiminnon poistamista tulostimesta.

5.1.6 Avoimet portit laitteissa

Tutkimuksessa löydettiin yksi testikäytössä oleva laite, jossa oli avoimena Apache2-palvelimen testisivu. Yhteyshenkilö ei ollut tietoinen laitteen kaikista avoinna olevista porteista ja niiden palveluista. Lisäksi löydettiin varsinkin tulostimista avoimia telnet- ja ftp-portteja.

Suositellaan yritykselle avoimien porttien sulkemista, mikäli niitä ei tarvita. Avoimet portit lisäävät ylipäätään hyökkäyspinta-alaa, ja varsinkin telnet- ja ftp-palvelut ovat haavoittuvaisia niiden salauksen puutteen vuoksi.

5.2 Tulosten pohdinta ja validointi

Kun suositukset oli laadittu, käytiin ne läpi yrityksen yhteyshenkilön kanssa. Käydään tässä alaluvussa tarkemmin läpi yrityksen näkökulmia laadittuihin suosituksiin.

Langattoman verkon hyökkäyksen osalta on totta, että verkon salauksen voi purkaa jopa kohtuullisessa ajassa tehokkaammalla laitteistolla. Langattoman verkon salasanan tulisikin olla vahvempi.

Verkkoon pääsyssä yritys tunnisti MAC-suodatuksen hyväksi suojauskeinoksi ja se on yksi suojaustaso lisää. Täysin pitävähän MAC-suodatus ei ole, sillä MAC-osoitteen voi väärentää. Yrityksessä oltiin myös sitä mieltä, että MAC-suodatuksen käyttöönottoon liittyy haasteita. Se saattaa lisätä työtä entisestään, mikäli sitä ei saada kerralla toimimaan oikein. MAC-suodatusta käyttöönottaessa tulisikin olla erityisen huolellinen.

Skannausten perusteella luotu kuva verkon rakenteesta pitää paikkansa. On totta, että koko verkko on yhtä VLAN:ia ja segmentointi on hyvä keino suojata verkkoa. Hallinnollisesta näkökulmasta tulee kuitenkin aina olla aina perustelut verkon segmentointiin, sillä segmentointi monimutkaistaa verkon ylläpitoa. Yrityksen tapauksessa erityisesti tunnistettu testilaitekanta kannattaa segmentoida. Osa löydetyistä haavoittuvuuksista liittyykin juuri tähän testilaitekokonaisuuteen, mukaan lukien tutkimuksessa löydetty vanhentunut Linux-kone, johon oli palvelimen testisivu jäänyt auki.

Avoimet telnet-, ssh-, ja ftp-portit ovat yrityksen näkökulmasta hyviä huomioita ja ne toimivat hyvänä muistutuksena. Yritys myönsi, että tulostimet tulisikin pitää vakioylläpidon puolella ja niiden turvallisuutta tulisi parantaa. Kun laitteita alkaa olla paljon, kuten yrityksessä tällä hetkellä, on yhä haastavampaa pysyä ajan tasalla kaikista laitteista. Vaikka tulostimen avointa telnet-porttia ei voisikaan suoraan hyödyntää hyökkäyksessä, on silti hyvän hallintotavan mukaista pitää laitteet minimipääsyssä.

SMTP-tunnusten löytyminen tulostimen web-käyttöliittymästä oli yritykselle mielenkiintoinen löytö, joka korjattiin nopeasti. Tunnukset muutettiin ja niiden oikeuksia rajattiin. Alettiin myös selvittää, saako tunnusten näkymistä tulostimen käyttöliittymässä jotenkin estettyä.

Tulostimen mallista selvästi riippuu, mitä tietoja ne näyttävät suoraan. Tulostimissa .24-.26 on pääsy tulostimen osoitekirjaan, missä näkyy työntekijöiden nimiä ja sähköposteja. Vaikka yrityksen työntekijöiden nimet eivät ole kovin suojattuja, ei niiden silti ole tarpeen olla helposti näkyvillä. Vaihtelevaa näyttää olevan myös tulostimiin tehtävät hyökkäykset. Yrityksen kannalta erityisen kiinnostavaa olisi ollut päästä tulostustehtäviin kiinni, mitä ei kuitenkaan tässä tutkimuksessa saavutettu.

Arpspoofilla toteutettua välimieshyökkäystä ei saatu toimimaan niin, että olisi voitu kaapata käyttäjätunnuksia tai salasanoja. Wlan-interfacessa tehty arpspoof ei toiminut todennäköisesti siksi, koska wlan-tukiasemassa oli sisäänrakennettuna suojaus, joka aiheutti arspoofissa palvelunestotilanteen uhrille.

Tämän tutkimuksen jälkeen tilanne yrityksessä päivitettiin, minkä myötä suojaus välimieshyökkäystä vastaan parani yrityksessä entisestään.

Kaiken kaikkiaan yhteyshenkilö totesi saatujen tulosten olevan oikein kuvattu, joten tulokset saatiin näin validoitua. Tulokset olivat hyödyllistä tietoa yritykselle, ja yritys pyrkiikin tulosten myötä lisäämään kerroksellisuutta verkkonsa suojaukseen ja huomioimaan jatkossa paremmin verkon laitteilla avoinna olevat palvelut.

6 JOHTOPÄÄTÖKSET

Tämän tutkielman lähtökohtana oli kohdeyrityksessä huomattu tarve päivittää heidän tietoverkkonsa turvallisuusratkaisuja ja -käytäntöjä. Päivitettävät kohdat päätettiin selvittää tekemällä verkkoon tietoturvakatsaus, jonka tulosten perusteella laadittaisiin yritykselle raportti parannusehdotuksista. Tutkimusmenetelmäksi valittiin konstruktiivinen tutkimusote ja aineistonkeruumenetelmäksi tietoturvakatsaus. Tutkielman tavoitteeksi muodostui selvittää kohdeyrityksen verkon rakenne, mitä tietoturvauhkia verkkoon kohdistuu ja miten uhkia voidaan vähentää.

Tutkielman käytännön osuutta pohjustettiin kirjallisuuskatsauksella. Tutkielman aiheen kannalta oli oleellista aluksi esitellä tietoturvaan liittyviä käsitteitä ja sen jälkeen määritellä tietoturva, tietosuoja ja kyberturvallisuus. Oli oleellista tuoda esille, mitä eroa on tietoturvan, tietosuojan ja kyberturvallisuuden käsitteillä. Todettiin, että tietoturva koskee tiedon ja tietojärjestelmien suojaamista, kun taas tietosuoja liittyy vain henkilötietoihin. Kyberturvallisuus puolestaan kattaa myös ihmisten ja yhteiskunnan turvallisuuden ja ulottuu näin ollen tämän tutkielman laajuuden ulkopuolelle.

Kirjallisuuskatsaus-osiossa esiteltiin myös viimeaikaisia hyökkäyksiä tilastojen avulla, jotta saataisiin kuva, millaisia uhkia käyttäjiin kohdistuu nykyään.

Tilastojen mukaan viimeaikaisimpia hyökkäyksiä ovat erilaiset haittaohjelmat sekä työpöytä- että mobiililaitteille, hyökkäykset IoT-laitteisiin, drive by download -hyökkäykset ja haavoittuvaisten, tunnettujen sovellusten hyväksi käyttäminen. Esitetiin myös yrityksen ja loppukäyttäjän näkökulmasta joitakin keinoja, joilla näiltä hyökkäyksiltä voi suojautua. Viimeaikaisten hyökkäysten takana ovat tilastojen ja tutkimuksien mukaan kyberrikolliset, jotka pyrkivät hyötymään hyökkäyksistä varsinkin taloudellisesti.

Koska tietoturvakatsaus kohdistui yrityksen verkkoon, kirjallisuuskatsaus -osiossa käytiin läpi myös langattomia verkkoja niiden turvallisuusnäkökulmasta. Todettiin, että WLAN:ien salausprotokollat ovat haavoittuvaisia useille hyökkäyksille, eikä uusin WPA-3-salausprotokollakaan suojaa kaikilta tunnetuilta hyökkäyksiltä. WLAN:ien suojaamiseen löytyi alan tutkimuksissa kuiten-

kin useita keinoja. Näistä esiteltiin ne, jotka ovat pienehkön tai keskisuuren yrityksen kannalta mahdollisia toteuttaa.

Verkkoon tehdystä tietoturvakatsauksesta saatiin kartoitettua useita uhkia, vaikkakin osa uhkista jäi varmasti löytymättä. Tutkielman tulokset voidaankin nähdä pohjana tulevaisuudessa tehtäville katsauksille.

Kuten tietoturvaa määriteltäessä kävi ilmi, tietoturva on prosessi eikä valmis, ostettavissa oleva tuote. Verkon tietoturvan parantaminen edellyttää yritykseltä ajantasaista tietoa nykyisestä infrastruktuurista ja säännöllisiä tietoturvakatsauksia. Tekemällä lisää tietoturvakatsauksia voidaan myös löytää tässä tutkimuksessa löytämättä jääneet uhkat. Tutkimuksessa oli nähtävissä, että verkon tietoturvallisuus ei ollut täysin pysynyt yrityksen kasvun mukana, vaikkakin yleisesti ottaen verkon tietoturva vaikutti olevan hyvällä tasolla.

Tietoturvakatsauksen tuloksista voitiin johtaa useita toimia, joiden avulla yritys voi parantaa verkkonsa turvallisuustasoa. On syytä kuitenkin huomata, että suositukset eivät ole kaiken kattava lista, sillä uhkia jäi varmasti löytymättä. Suosituksia laatiessa huomioitiin niiden toteutettavuus, sillä yrityksellä ensisijaisena vaihtoehtona on hankkia turvallisuusratkaisut luotettavalta toimittajalta sen sijaan, että yritys rakentaisi järjestelmänsä itse. Yrityksen päätettäväksi kuitenkin jää suositeltujen toimien vaikutusten arviointi ja toimien toteuttamisjärjestys. Ottaen huomioon verkon koon ei voida olettaa, että suositellut toimenpiteet saataisiin tehtyä nopealla aikataululla.

Tämän tutkielman tietoturvakatsauksesta johdetut suositukset eivät luonnollisestikaan ole suoraan yleistettävissä kaikkiin yrityksiin, sillä suositusten taustalla on vain yhden yrityksen tilanne. Tuloksilla voi olla kuitenkin merkitystä myös muille yrityksille. Mikäli tässä tutkimuksessa esiteltyjä haavoittuvuuksia löytyy myös toisesta yrityksestä, voi se koettaa parantaa tilannetta tässä tutkielmassa esitellyillä suosituksilla. Tarkempi haavoittuvuuksien kartoittaminen edellyttää kuitenkin aina jonkinlaista tietoturvakatsausta.

Vaikka tässä tutkielmassa keskityttiin verkon tekniseen puoleen, saatiin myös huomata, että osa suosituksista liittyi osittain myös hallinnolliseen puoleen. Yrityksen tulisi päivittää laitepolitiikkaansa ja kehittää keinoja, joiden avulla se voisi välttää ylimääräisten laitteiden kytkemisen verkkoon jatkossa. Yrityksessä tulisi olla myös ajan tasalla oleva dokumentaatio verkon laitteista ja niissä olevista palveluista. Hallinnollista tietoturvaa ei muuten tutkittu tässä tutkielmassa, vaikka silläkin on oma roolinsa teknisen tietoturvan rinnalla kokonaisvaltaisessa tietoturvassa.

Tietoturvakatsaus voi olla hyvinkin laaja prosessi riippuen mukaan otettavien näkökulmien määrästä, eikä ole olemassa vain yhtä tapaa suorittaa tietoturvakatsaus. Koska pro gradu -tutkielma on kuitenkin luonteeltaan melko suppea tutkimus, tuli tässäkin tehdä useita rajauksia. Tässä tutkielmassa ei esimerkiksi tutkittu fyysistä turvallisuutta, joka sekin on keskeinen osa yrityksen tietoturvallisuutta. Myös tutkittavien laitteiden määrä oli rajattu. Tutkimuksessa noudatettiin varovaisuutta, mikä osaltaan myös rajasi tutkimusta. Ei esimerkiksi voitu mielivaltaisesti tutkia tiiviissä käytössä olevia palvelimia eikä mitä

tahansa tulostinta, sillä tutkimuksen teko ei saanut häiritä muiden työntekijöiden työtä. Tutkimus tuli pitää mahdollisimman ”piilossa” muilta työntekijöiltä.

Kaiken kaikkiaan tutkimus antoi pohjan tulevaisuuden katsauksille yrityksessä. Jatkotutkimuksena olisi mielenkiintoista tehdä vastaavanlainen katsaus verkkoon sen jälkeen, kun yritys on tehnyt parannuksia nykytilanteeseen, ja verrata sen tuloksia tämän tutkielman tuloksiin. Olisi myös mielenkiintoista tallentaa ja analysoida yrityksen liikennettä muita haavoittuvuuksia varten.

LÄHTEET

Alotaibi, B. & Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications, 90*(3), 1261-1290.

Apache HTTP server 2.4 vulnerabilities. Haettu osoitteesta httpd.apache.org/security/vulnerabilities_24.html

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity, 4*(1), tyy010.

Asghari, H., van Eeten, M. J. & Bauer, J. M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy, 13*(5), 16-23.

AV-Test. Malware. Haettu osoitteesta https://www.av-test.org/en/statistics/malware/

bin Baharin, K. N., Din, N. M., Jamaludin, M. Z. & Tahir, N. M. (2003). Third party security audit procedure for network environment. (s. 26-30) IEEE.

Burns, A., Wu, L., Du, X. & Zhu, L. (2017). A novel traceroute-based detection scheme for wi-fi evil twin attacks. (s. 1-6) IEEE.

Cabaj, K. & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: The case of cryptowall. *IEEE Network, 30*(6), 14-20.

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society* Oxford University Press on Demand.

Chebyshev, V., Sinitsyn, F., Liskin, A. & Kupreev, O. (2018, elokuu 6,). IT threat evolution Q2 2018. statistics. Haettu osoitteesta securelist.com/it-threat-evolution-q2-2018-statistics/87170/

Choo, K. R. (2011a). Cyber threat landscape faced by financial and insurance industry.

Choo, K. R. (2011b). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Costin, A. (2012). PostScript: Danger ahead?! *Hack in Paris,*

Cova, M., Kruegel, C. & Vigna, G. (2010). Detection and analysis of drive-by-download attacks and malicious JavaScript code. (s. 281-290) ACM.

CVE Common Vulnerabilities and Exposures. Haettu osoitteesta https://cve.mitre.org/about/terminology.html

CVE Details. Haettu osoitteesta cvedetails.com

Eskandari, S., Leoutsarakos, A., Mursch, T. & Clark, J. (2018). A first look at browser-based cryptojacking. (s. 58-66) IEEE.

EU:N yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano – uusi tietosuojalaki. Haettu osoitteesta https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M. & Rajarajan, M. (2015). Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys & Tutorials, 17*(2), 998-1022.

Fehér, D. J. & Sandor, B. (2018). Effects of the WPA2 KRACK attack in real environment. (s. 239) IEEE.

Filshtinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air? *Communications of the ACM, 56*(6), 28-30.

Gandotra, E., Bansal, D. & Sofat, S. (2014). Malware analysis and classification: A survey. *Journal of Information Security, 5*(02), 56.

Gerber, M. & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30.

Hacking printers wiki. Haettu osoitteesta hacking-printers.net

Hallituksen esitys HE 9/2018 vp. (2018, 1 Maaliskuu,). Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

Harris, M. & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

He, D., Chan, S. & Guizani, M. (2015). Mobile application security: Malware threats and defenses. *IEEE Wireless Communications, 22*(1), 138-144.

Henkilötietolaki 22.4.1999/523

Hoque, N., Bhattacharyya, D. K. & Kalita, J. K. (2015). Botnet in DDoS attacks: Trends and challenges. *IEEE Communications Surveys and Tutorials, 17*(4), 2242-2270.

Hua, J. & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems, 22*(2), 175-186.

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., . . . McCoy, D. (2018). Tracking ransomware end-to-end. (s. 618-631) IEEE.

Index of /pub/linux/kernel/v3.x/. Haettu osoitteesta mirrors.edge.kernel.org/pub/linux/kernel/v3.x/

ISO/IEC. (2005). *ISO/IEC 27002: Code of practice for information security management*

Jackson, C., Barth, A. & Hodges, J. (2012). Http strict transport security (hsts).

Karyotis, V. & Khouzani, M. (2016). *Malware diffusion models for modern complex networks: Theory and applications.* Morgan Kaufmann.

Kasanen, E., Lukka, K. & Siitonen, A. (1991). *Konstruktiivinen tutkimusote liiketaloustieteessä* (3)

Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K. & Kirda, E. (2016). UNVEIL: A large-scale, automated approach to detecting ransomware. (s. 757-772)

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. (s. 3-24) Springer.

Kiwia, D., Dehghantanha, A., Choo, K. R. & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking trojans for evolutionary computational intelligence. *Journal of Computational Science, 27*, 394-409.

Kohlios, C. & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for wi-fi and WPA3. *Electronics, 7*(11), 284.

Kyberturvallisuuskeskus. (2018, helmikuu 13,). WannaMine-haittaohjelma louhii, varastaa tunnuksia, leviää tehokkaasti ja osaa piiloutua. Haettu osoitteesta

https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802131503.html

La Polla, M., Martinelli, F. & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE Communications Surveys & Tutorials, 15*(1), 446-471.

Laki sähköisen viestinnän palveluista 7.11.2014/917

Le, V. L., Welch, I., Gao, X. & Komisarczuk, P. (2013). Anatomy of drive-by download attack. (s. 49-58) Australian Computer Society, Inc.

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H. & Zhang, J. (2009). Botnet: Classification, attacks, detection, tracing, and preventive measures. *EURASIP Journal on Wireless Communications and Networking, 2009*(1), 692654.

Lo, E. C. & Marchand, M. (2004). Security audit: A case study [information systems]. (s. 193-196) IEEE.

Lukka, K. (2006). Konstruktiivinen tutkimusote: Luonne, prosessi ja arviointi. *Teoksessa Rolin-Kakkuri-Knuuttila-Henttonen (Toim.) Soveltava Yhteiskuntatiede Ja Filosofia.Gaudeamus Kirja Oy, Hakapaino Oy, Helsinki*, 111-133.

Mavrommatis, N. P. P. & Monrose, Moheeb Abu Rajab Fabian. (2008). All your iframes point to us. (s. 1-16)

McAfee. (2018). *McAfee labs threats report.*

Metasploit. Haettu osoitteesta metasploit.com

Microsoft. (2017a, marraskuu 14). CVE-2017-11882 | Microsoft Office Memory Corruption Vulnerability.

Microsoft. (2017b, maaliskuu 14). Microsoft security bulletin MS17-010 - critical. Haettu osoitteesta docs.microsoft.com

Müller, J., Schwenk, J., Somorovsky, J. & Mladenov, V. (2016). Exploiting network printers.

MySQL 5.7 release notes. Haettu osoitteesta https://dev.mysql.com/doc/relnotes/mysql/5.7/en/

Nachenberg, C. (1997). Computer virus-antivirus coevolution. *Communications of the ACM, 40*(1), 46-51.

Nadir, I. & Bakhshi, T. (2018). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. (s. 1-7) IEEE.

Nikbakhsh, S., Manaf, A. B. A., Zamani, M. & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. (s. 684-687) IEEE.

NIST. (2017). *An introduction to information security*

Noor, M. M. & Hassan, W. H. (2013). Wireless networks: Developments, threats and countermeasures. *International Journal of Digital Information and Wireless Communications (IJDIWC), 3*(1), 119-134.

Onwubiko, C. (2009). A security audit framework for security management in the enterprise. (s. 9-17) Springer.

OpenSSH release notes. Haettu osoitteesta www.openssh.com/releasenotes.html

Pereira, T. S. M. & Santos, H. (2010). A security framework for audit and manage information system security. (s. 29-32) IEEE.

Piirainen, K. A. & Gonzalez, R. A. (2013). Seeking constructive synergy: Design science and the constructive research approach. (s. 59-72) Springer.

Puolustusministeriö. (2015). Katakri - tietoturvallisuuden auditointityökalu viranomaisille. Haettu osoitteesta https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Realpe, L. F. E., Parra, O. J. S. & Velandia, J. B. (2018). Use of KRACK attack to obtain sensitive information. (s. 270-276) Springer.

Richardson, R. & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10-21.

Sabillon, R., Cano, J., Cavaller, V. & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165.

Shah, A. (2016, Dec 5,). HP shutting down default FTP, telnet access to network printers. *PC World*. Haettu osoitteesta www.pcworld.com

Sittig, D. F. & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics, 7*(2), 624.

Smith, K. T., Smith, M. & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal,*

Sood, A. K. & Zeadally, S. (2016). Drive-by download attacks: A comparative study. *IT Professional, 18*(5), 18-25.

Statcounter GlobalStats. (2018). OS market share. Haettu osoitteesta http://gs.statcounter.com

Stimpson, T., Liu, L., Zhang, J., Hill, R., Liu, W. & Zhan, Y. (2012). Assessment of security and vulnerability of home wireless networks. (s. 2133-2137) IEEE.

Suomen kyberturvallisuusstrategia. (2013, tammikuu 24,). Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Symantec. (2018). *Internet security threat report volume 23.*

Valli, C., Martinus, I. C. & Johnstone, M. N. (2014). Small to medium enterprise cyber security awareness: An initial survey of western australian business.

Valtiovarainministeriö. (2008). *Valtionhallinnon tietoturvasanasto*. Helsinki: Edita Prima Oy.

Van Beveren, J. (2000). A conceptual model of hacker development and motivation. *Journal of E-Business, 1*(2), 1-9.

Vänskä, O. (2018, Feb 9,). Lahden it-katastrofin syy: Järjestelmät laitettiin louhimaan bitcoineja. Haettu osoitteesta www.tivi.fi

Viestintävirasto. Palvelun tietoturva. Haettu osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/yhteisotilaajienoikeudetjavelvollisuudet/palveluntietoturva.html

Viestintävirasto. (2016). Selviytymisopas kiristyshaittaohjelmia vastaan - kokemuksia kiristyshaittaohjelmista suomessa ja neuvoja niistä selviytymiseen. Haettu osoitteesta www.kyberturvallisuuskeskus.fi/fi/ohjeet

Vinod, P., Jaipur, R., Laxmi, V. & Gaur, M. (2009). Survey on malware detection methods. (s. 74-79)

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. (s. 112-125) Springer.

Waliullah, M. & Gan, D. (2014). Wireless LAN security threats & vulnerabilities. *International Journal of Advanced Computer Science and Applications, 5*(1)

Wang, L. & Wyglinski, A. M. (2016). Detection of man-in-the-middle attacks using physical layer wireless security techniques. *Wireless Communications and Mobile Computing, 16*(4), 408-426.

Wang, L., Srinivasan, B. & Bhattacharjee, N. (2011). Security analysis and improvements on WLANs. *Journal of Networks, 6*(3), 470.

Whitman, M. E. & Mattord, H. J. (2013). *Management of information security* (4) Cengage Learning.

Zenmap. Haettu osoitteesta nmap.org/zenmap

Zimba, A., Wang, Z., Mulenga, M. & Odongo, N. H. (2018). Crypto mining attacks in information systems: An emerging threat to cyber security. *Journal of Computer Information Systems,* , 1-12.

Zou, Y., Zhu, J., Wang, X. & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104*(9), 1727-1765.