Haaga-Helia
ammattikorkeakoulu Oy

Hakkerien rooli yritysten tietoturvan parantelussa

Asaf Shamaa

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Asaf Shamaa

Koulutusohjelma
Tietojenkäsittely - Päivätoteutus

Opinnäytetyön nimi
Hakkerien rooli yritysten tietoturvan parantelussa

Sivu- ja liitesivumäärä
24

Tämän opinnäytetyön tarkoitus on kertoa hakkerien roolista yritysten näkökulmasta sekä niiden tuomista hyödyistä ja haitoista. Erityisesti työn aihe keskittyy niin sanottuihin valkohattuihin, joiden tehtävänä on testata olemassa olevaa tietoturvaa ja löytää siitä heikkoja kohtia tai muuta parannettavaa.

Työn tulokset pohjautuvat yhdistelmään yksilöhaastattelua ja itsenäistä tutkimusta, jotka suoritettiin keväällä 2020. Yritysten lisäksi asiantuntijoita on useampi, joista suurin osa on työskennellyt valkohattuna aiemmin.

Tutkimuksen ja haastattelun avulla selvitetään, mitä hyötyä hakkereista on yrityksille, mitkä ovat yritysten odotukset tämänlaisten hakkereitten suhteen ja kohtaavatko nämä odotukset. Haastattelu keskittyi ammattilaisen omiin kokemuksiin näissä töissä ja niiden avulla voidaan arvioida työn tuomaa käytännön hyötyä.

Opinnäytetyön perusteella yritykset voivat arvioida, onko valkohattuhakkerin palkkaaminen tietoturvan testaamiseen investoinnin arvoista ja kuinka paljon hyötyä siitä tulee käytännössä heille, mikäli tämä henkilö löytää vakavia puutteita yrityksen tietoturvasta.

Kyselyn ja tutkimuksen jäljiltä yleiskuva valkohattuhakkerin toiminnasta ei näyttäisi poikkeavan vahvasti normaalista tietoturvaekspertin työstä. Suurin ero on siinä, kuinka paljon valkohattu tietää hakkeroinnista kokemuksen kautta, ja mahdollisesti henkilön omasta historiasta hakkerina.

Suurin osa näkee valkohatut ja heidän toimintansa hyvänä asiana yritysten kannalta, antaen tietoturvaan liittyviin asioihin näkökulmia ja työkaluja, joita normaalilla tietoturvavastaavalla ei välttämättä olisi.

Asiasanat
Tietoturva, hakkeri, yritystoiminta.

Sisällys

1 Johdanto

Tietoturva on aina ollut tärkeä tekijä yritysmaailmassa, erityisesti IT-alalla. Hakkerit ja muut pahantahtoiset tekijät voivat tuoda massiivisia tappioita firmoille, olkoot ne sitten viruksen, tietovuodon tai brändin imagolle aiheuttamia vahinkoja. Tiedot, joita yritykset säilyttävät, ovat syystäkin tarkasti valvottuja ja hyvin suojattuja.

Päivitykset, virustentorjuntaohjelmat, ja muut tietoturvatoimet ovat jatkuvasti kehityksen tarpeessa, sillä tavat kalastella tietoa tai murtautua tietojärjestelmiin kehittyvät nopeasti hakkerien ja muiden tietoturvamurtoja tekevien henkilöitten toimesta.

On kuitenkin olemassa hakkereita, jotka käyttävät näitä taitoja muuhun kuin ihmisten tietojen keräämiseen oman hyödyn vuoksi. Tämän opinnäytetyön tavoitteena on kertoa näistä hakkereista, joita yleensä kutsutaan valkohatuiksi, ja heidän toiminnastansa sekä niiden hyödyistä yritysten näkökulmasta.

Keskeisinä tutkimuskysymyksinä ovat seuraavat:

- Mitä valkohattuhakkerit ovat?
- Millä tavoin valkohattuhakkerit toimivat?
- Mitä työkaluja valkohattuhakkereilla on käytettävissään?
- Miten yritykset hyödyntävät valkohattuhakkerien työkaluja ja taitoja?

Tutkimus on luonteeltaan laadullinen ja lähestymistapa on kuvaileva, kun taas tutkimusmateriaali on osittain kyselyyn perustuva. Loput tutkittavasta tulee aiheen kirjallisuudesta, ja vaikka rikolliset hakkerit ovat aiheeseen liittyvä tekijä, tutkimus on suurimmalta osin rajattu valkohattuhakkereihin ja heidän toimintaansa.

1.1 Käsitteet

Tutkimukselle relevanttien käsitteitten määritelmät:

Hakkeri
Perinteisesti terminä hakkerilla on kuvailtu syvällisesti tietotekniikkaan perehtynyttä ihmistä. Ajan myötä sen merkitys alkoi muuttumaan, ja siitä tuli synonyymi krakkereille, jotka ovat tietoturvaan murtautuvia henkilöitä (Haasio 2017, 68-69).

Erilaiset hakkerit ovat saaneet omat variantit, jotka erottavat toisistaan väreillä sekä yleisesti heidän käytöksestänsä tietoturvaan murtautumisen suhteen. Yleisiä esimerkkejä ovat mustahatut, valkohatut ja harmaahatut (Haasio 2013, 100).

Valkohattu

Hakkeri, joka murtautuu normaalin hakkerin tapaan yleensä luvatta tietojärjestelmiin, mutta pyrkii välttämään vahinkoja sekä antaa vihjeitä järjestelmän omistajille, esimerkiksi osoittaen tietoturvassa olevat puutteet tai haavoittuvaisuudet (Haasio 2013, 100.) Nämä hakkerit ovat vastakohta ns. mustahatuille, jotka varastavat tietoa tai muuten toimivat rikollisissa aikeissa muiden tietoverkoissa.

Valkohattuja löytyy sekä yritystoiminnassa että sen ulkopuolella. Ensimmäinen ryhmä sopii erikseen asiakkaan kanssa, joka voi olla yritys tai yksityishenkilö siitä, mitä toimenpiteitä turvallisuustestaukseen käytetään, kun taas toinen ryhmä satunnaisesti tunkeutuu järjestelmiin mutta ilmoittaa löytämistään haavoittuvaisuuksista tunkeutumisen kohteelle koskematta itse tietoihin, joita hän pystyy näkemään.

Mustahattu

Henkilö, joka murtautuu tietojärjestelmiin ilman lupaa ja pyrkii joko myymään niistä kerättyä tietoa eteenpäin tai hyödyntämään sitä itse rikollisiin tarkoituksiin (Haasio 2013, 100). Niin sanottu tavanomainen hakkeri nykykontekstissa.

Esimerkkinä tästä on hakkeri, joka onnistuu murtautumaan nettikaupan sivuille ja keräämään siellä asioivien asiakkaitten pankkitietoja, joita hän sitten itse käyttää luvattomasti maksamaan omat ostoksensa internetissä.

Krakkeri

Tietoturvajärjestelmiin luvattomasti tunkeutuva henkilö. Terminä krakkeri on yleensä sekoittunut yhteen hakkerin kanssa, ja etenkin mustahattuhakkereista puhuttaessa voi yhtä hyvin puhua myös krakkereista, mikäli toimintatavat henkilöillä täsmäävät (Haasio 2017, 68-69).

Tietoturva

Käsitteenä tietoturvan vaatimukset ovat, että tieto säilyy eheänä (turvassa luvattomilta muutoksilta), saatavilla tarvittaessa ja luottamuksellisena, jos käyttäjän mielestä sitä tarvitaan. Tähän määritelmään lukeutuu myös tietoa säilyttävien koneitten ja palveluitten käytettävyys ja toimivuus. (Järvinen 2012, 10.)

Esimerkiksi salasanat, joita vaaditaan oman sähköpostitilin tarkastelua varten, ovat keskeinen osa tietoturvaa eheyden ja luottamuksellisuuden osalta, sillä oletuksena vain kyseistä tiliä käyttävä henkilö tietäisi salasanan, ja täten hän on myös ainoa henkilö, joka pääsee katsomaan tilin tietoja.

Kyberturvallisuus

Turvallisuuden osa-alue, joka kattaa yhteiskunnassa toimivat tietoverkot, kuten internetin ja muut tietoverkot. Kyberturvallisuuden sanastossa termin määritelmä on: ”Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan” (Sanastokeskus TSK ry 2018, 22).

Tunkeutumistestaus

Toiselta nimeltään penetraatiotestaus, tämä on tapa katsoa tietoturvaa siitä näkökulmasta, että siinä olevia haavoittuvaisuuksia voidaan hyödyntää tilanteissa, joissa järjestelmään yritetään murtautua (Engebretson 2013, 1).

Red Team- testaus

Simulaatio tietoturvaan kohdistuvasta hyökkäyksestä, jonka avulla pyritään keräämään tietoa kohteen haavoittuvaisuuksista useasta eri näkökulmasta. Tämä on usein monivaiheinen prosessi, jonka aikana kerätään mahdollisimman paljon dataa jokaisen vaiheen etenemisestä (F-Secure 2017).

2 Tietoturva ja siihen kohdistuvat uhat

Tietoturvaan kohdistuu monenlaisia uhkatekijöitä. Sekä yrityksiin että yksityishenkilöihin kohdistuu useammin phishing eli tiedonkalastusyrityksiä kuin suoraa hakkerointia, mutta molemmat ovat mahdollisia syitä sille, että tietoturva on uhattuna.

Rikolliset, jotka kalastavat tietoa, yleensä tekevät sen lähettämällä virallisen näköisen viestin, jossa pyydetään käyttäjätunnusta ja salasanaa tai muita tietoja (Haasio 2017, 75-76). Jos huijauksen kohde sattui olemaan johtoasemassa oleva henkilö isossa yrityksessä, rikollinen voi helposti päästä varastamaan kaikenlaista luottamuksellista tietoa yritykseltä, etenkin jos muita varotoimenpiteitä ei ole henkilöllä käytössä.

Phishing on erityisen yleistä sivuilla, joissa käsitellään rahaa, kuten verkkopankkisivustot, maksupalvelut kuten PayPal, ja verkkokaupat kuten Amazon ja eBay (Järvinen. 2012, 73).

Koneen kaappaus ja uhrin kiristys ovat myös yleisiä tietoturvaan murtautuneen henkilön aiheuttamia uhkia. Kuten aiemmin mainitut phishing-viestit, nämä yleensä saapuvat henkilön sähköpostiin ja näyttävät virallisilta ilmoituksilta, jotka sisältävät tiedoston tai ohjelman liitteenä. Joskus viestin mukana tulee virus, kun taas toisinaan niistä siirtyy toisenlainen haittaohjelma tietokoneelle (Haasio 2017, 53).

Jos kone menee lukkoon eikä käyttäjä pääse avaamaan ollenkaan laitteella olevia tiedostoja, kyseessä saattaa olla ransomware-ohjelma. Rikolliset kiristävät rahaa uhreiltaan näitten ohjelmien avulla, tarjoten maksua vastaan avaimia, joilla koneen saa uudestaan haltuun (Haasio 2017, 53), mutta tämäkään ei takaa sitä, että laite olisi taas käyttökuntoinen, ja sen tietoturvallisuus voi jatkossakin olla uhattuna haittaohjelmien takia.

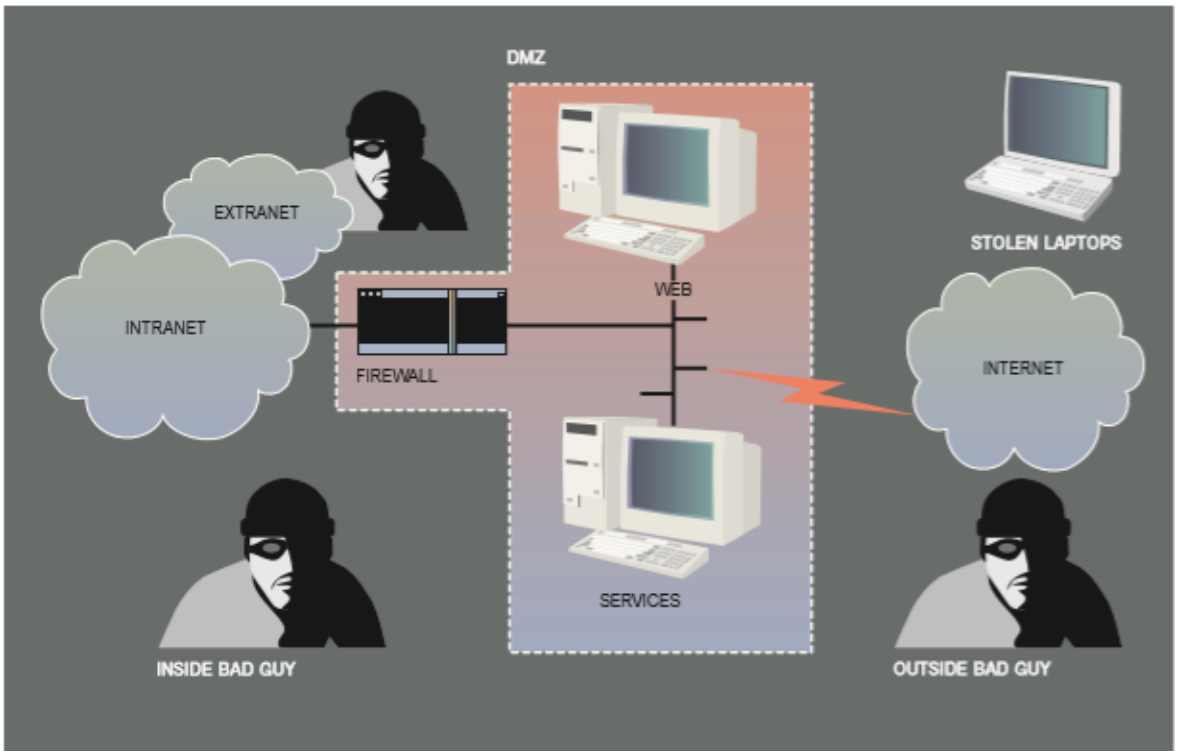
Koneen käyttöä varten olevan käyttäjätunnuksen varastamisen lisäksi toinen uhka on eri palveluita käyttävän tunnuksen kaappaus, esimerkiksi viemällä käyttäjän Office 365-tunnus, johon sisältyy Word, Outlook, Excel ja muita sovelluksia. Tämän jälkeen he lähettävät uhrin kontakteille viestejä tekeytyen uhriksi ja pyytäen heiltä tietoja, joilla he voivat kerätä rahaa ja muita resursseja (Kyberturvallisuuskeskus 2020). Kuva 1 näyttää, kuinka kalastusviestin avulla rikollinen ottaa tunnuksen itselleen ja täten huijaa käyttäjiä lähettämään hänelle rahaa valheellisen laskun avulla.

Kuva 1. Office 365-tunnuksen kaappaus kalasteluviestin avulla (Kyberturvallisuuskeskus 2020)

Toinen tapa, jolla rikollinen voi kaapata tunnukset tai laitteen, on hyödyntämällä cross-site hyökkäyksiä. Näissä sivulla olevaa tietoturva-aukkoa hyödynnetään siten, että haittaa tekevä henkilö saa kerättyä sivulla vierailevien ihmisten tiedot itselleen syötettyään haittaohjelman sivustolle (OWASP).

Tämä on erityisen vaarallista sivuilla, joilla käsitellään henkilötietoja tai rahaa, sillä tietojen menetys voi johtaa suuriin rahallisiin tappioihin ja muihin ongelmiin. Lieventävänä tekijänä cross-site-hyökkäykset vaativat sen, että sivulla on jo olemassa olevia tietoturvaan liittyviä haavoittuvaisuuksia, joten ne eivät ole kovin yleisiä hyvin huolletuilla nettisivuilla. Tästä huolimatta on aina hyvä tarkistaa, onko kyseisen sivuston tietoturva ajan tasalla.

Figure 5 Different ways to attack computer security



Kuva 2. Eri tapoja hyökätä tietokoneen turvaverkkoihin (C. C. Palmer 2001)

Tietokoneet eivät ole ainoa kohde, johon yleensä kohdistuu erilaisia kalasteluyrityksiä tai muunlaisia iskuja hakkereilta. Älypuhelimet, pankkiautomaatit ja muut laitteet, joista saa internetyhteyden voidaan kaapata erilaisilla haittaohjelmilla tai suoraan yhdistämällä niihin tietoturva-aukkojen kautta (F-Secure 2017). Kun yksi laite on kaapattu, hyökkääjän on

yleensä helpompi päästä muihin laitteisiin käsiksi, ja sama pätee kaikkiin hänen käsiinsä joutuneisiin käyttäjätunnuksiin.

Ulkopuolelta tulevat hyökkäykset ovat ne, joihin on yleisesti kiinnitetty paljon huomiota, mutta sen lisäksi on myös tapauksia, joissa yrityksen tai organisaation sisällä toimiva henkilö on paljastunut tietoturvamurroksen tekijäksi. Verrattuna ulkopuoliseen hyökkääjään sisältäpäin iskevä henkilö on jo entuudestaan todennäköisesti saanut tietyt käyttöoikeudet järjestelmiin, ja työntekijöittensä luottamuksen. (F-Secure 2017)

Kuva 2 osoittaa, kuinka varastettu kannettava voi olla tie usean tietokoneen kaappaukseen riippumatta siitä, onko tunkeutuja verkon sisäpuolella tai ulkopuolella. Yksi aukko tietoturvassa voi vaarantaa kokonaisen verkon, ja täten kaikki siihen liittyvät laitteet.

3 Hakkerin rooli

Valkohatut eivät yleensä tule ensimmäisenä ihmisten mieleen, kun puhutaan hakkereista, sillä moni ajattelee rikollista hakkeria ja näistä yleensä puhutaankin uutisissa ja mediassa. Tästä syystä heidän saattaa olla vaikea sanoa, kuinka hyödyllisiä valkohatut tosiaan ovat käytännössä.

Yleensä valkohattuhakkeri palkataan samanlaiseen työhön kuin tietoturvavastaava, jos hän ei ole yksin toimiva henkilö yritysmaailman ulkopuolella. Merkittävin ero tietoturvavastaavien ja valkohattuhakkerien välillä on hakkerin oma kokemus tietomurtojen suhteen, joka voi vaihdella melko vahvasti henkilön mukaan.

3.1 Haavoittuvaisuuksien havaitseminen

Suurin syy valkohatun palkkaamiselle kokemuksen ja tietämyksen lisäksi on hänen työkalunsa, joiden avulla löydetään heikkoja kohtia tietoturvassa. Nämä voivat olla harmittomia olemassa olevalle systeemille tai pahimmassa tapauksessa voivat jopa vaurioittaa järjestelmää, jonka takia valkohattu sopii erikseen työnantajan kanssa siitä, miten hän toimii.

Hakkerin työn tulokset ovat yleensä suhteutettuna testauksiin käytettyyn aikaan (Haastattelu 2020) joten pikaiset tarkistukset eivät yleensä auta yhtä paljoa kuin pitkä ja laaja-alainen analyysi koko järjestelmän rakenteesta. Riskit voivat myös vaikuttaa odotuksiin, sillä kaikki yritykset eivät välttämättä ole valmiita ottamaan riskejä, jos seuraukset voivat aiheuttaa suuria tappioita heille.

Itse testauksen lisäksi tarkkaavaisuus raportoinnissa on erittäin tärkeää valkohatulle ja hänen kanssaan toimiville henkilöille, sillä yksikin unohdettu seikka tietoturvassa voi tarkoittaa sitä, että järjestelmä pysyy testauksenkin jälkeen haavoittuvaisena.

Valkohattuhakkereilla on monta eri tapaa testata olemassa olevan tietoturvan tehokkuutta. Heidän keinonsa ovat yleensä tarkoitus mukauttaa siihen, miten hyökkääjät toimivat, sillä tieto näistä työkaluista auttaa torjumaan niitä.

SQL-injektio

Tämä metodi on riskialtis mutta tehokas tapa testata tietokannan turvallisuutta. Se on myös työkalu, jota hakkerit käyttävät tunkeutuakseen tietoturvajärjestelmiin, etenkin tietokantoihin. Huonosti suoritettu injektio voi vaurioittaa tietokantaa, pahimmassa tapauksessa muuttaen sen käyttökelvottomaksi (SQL Injection FAQ, 1999).

Kohteena on tietokannat, jotka on yleensä koodattu SQL eli Structured Query Language-kielellä. Yleisiä palvelimia tietokannoille, joissa on suljettu lähdekoodi, ovat Oracle, Microsoft SQL Server ja IBM DB2, kun taas avoimen lähdekoodin palvelimissa ovat esimerkiksi MariaDB ja MySQL.

SQL-injektiossa hyödynnetään olemassa olevaa aukkoa palvelinten tietoturvassa, jonka avulla hyökkääjä syöttää palvelimeen erilaisia komentoja, joiden avulla hän pääsee muokkaamaan tietoja, joihin hänellä ei normaalisti olisi pääsyä. Taitava hakkeri pystyy tätä kautta avaamaan tien järjestelmänvalvojan tunnuksiin. Sen mukaan, millä tavalla yrityksen tietokannat ovat koodattu, SQL-injektiota varten syötetty koodi voi vaihdella (SQL Injection Knowledge Base 2012).

Red Team

Testaus, jossa simuloidaan tietoturvaan murtautumista tiimin kanssa. Tiimi, joka pyrkii red team-tyyliseen testaukseen kerää tietoa kohteesta, jonka järjestelmään yritetään murtautua useasta eri lähteestä kuten julkiset sivustot ja tiedotteet, sosiaalinen media, ja yhteyshenkilöt, joilla on valtuuksia kertoa yrityksestä (F-Secure 2017). Tämän jälkeen he yrittävät rikollisen tunkeutujan tavoin päästä käsiksi kohteen tietojärjestelmiin askel kerrallaan matkien tekniikoita, joita oikeat hyökkääjät käyttäisivät.

Puolustuksena toimivat yrityksen tietoturvavastaavat ja kohteen olemassa oleva tietoturvaohjelmisto. Näitten tarkoituksena on torjua hyökkäys, vaikka tässä tapauksessa ei olekaan kyse oikeasta iskusta. Tietoturvaryhmän reaktio uhkaan raportoidaan muun toiminnan lisäksi osana testausta.

Vaikka hyökkäyksen aikomus on olla suurimmalta osin replikoida oikeaa hyökkäystä, joissain kohdissa pyritään tahallaan viestimään kohteelle, että tietoturvajärjestelmään yritetään murtautua. Tämä kuuluu osaan raportointia, joka tehdään hyökkäyksestä kokonaisuudessaan, sillä yrityksen reaktio mahdolliseen hyökkäykseen on osa tietoturvaa muiden toimenpiteitten ja turvaohjelmien ohella. Sen jälkeen, kun testaus on ohi, tiedot kerätään talteen ja raportoidaan asiakkaalle (F-Secure 2017).

Havoittuvaisuusskannaus

Joskus tietoturvan testaus ei vaadi muuta kuin yksinkertaisen katsauksen. Tämä menetelmä viittaa tunnettujen haavoittuvaisuuksien etsimiseen skannausohjelmien avulla sekä tarkistamalla, mikäli eri ohjelmistoissa on tunnettuja haavoittuvaisuuksia, joita rikolliset pystyvät hyödyntämään (Belangia 2015, 4).

3.2 Mahdollisten murtoyritysten torjuminen

Mikäli haavoittuvaisuuksia on havaittu yrityksen tietoturvassa, valkohattu voi, mikäli hänelle on annettu valtuudet, toimia niiden paikkaamisessa. Murtoja on erittäin vaikea torjua siinä vaiheessa, kun järjestelmään on päästy sisään, joten suurin osa keinoista ovat ennaltaehkäiseviä.

Tietoturvan päivitykset, lisäohjelmiston asennukset sekä aktiivinen verkkojen tarkkailu kuitenkin auttavat hyökkäysten estämisessä. Tärkeitten tiedostojen varmuuskopiointi on myös suositeltavaa, jotta dataa ei menetä, vaikka järjestelmä kaatuisi täysin hyökkäyksen tai vahingon sattuessa (Kyberturvallisuuskeskus 2020).

3.3 Ohjeistus tietoturvan parantamiseksi

Hakkeri on usein asemassa auttamaan järjestelmän suunnittelijoita antamalla palautetta ja muuta tietoa, joilla voidaan parantaa olemassa olevaa järjestelmää. Haavoittuvaisuuksien raportointi kuitenkin kuuluu valkohatun työkuvaan (Haastattelu 2020).

Tietoturvaohjelmien päivittäminen ei ole ainoa tapa, jolla tietoturvan laatua voidaan parantaa. Se ei myöskään ole takuuvarma suoja hyökkäyksiltä, sillä ohjelmien toiminta muuttuu vaikeammaksi, mitä monimutkaisempi ohjelma on kyseessä (F-Secure 2017). Virustorjuntaohjelmissa on omat haavoittuvaisuutensa, joita hyödyntämällä hakkeri voi ohittaa turvajärjestelyt tai jopa huijata ohjelmaa luulemaan, että kaikki on kunnossa.

4 Yritysten odotukset

Yrityksillä on syytä harkita tarkkaan kaikki investointinsa, ja hakkerin palkkaaminen ei ole poikkeus tässä tapauksessa. Tietoturvan osalta moni yritys panostaa kuitenkin tietyn määrän rahaa tietojensa suojaukseen, mutta resurssien määrä sekä yrityksen ottamat riskit vaihtelevat vahvasti riippuen alasta, paikasta ja muista tekijöistä.

4.1 Resurssit

Yrityksen budjetti on yleensä melko merkittävä tekijä siinä, kuinka paljon rahaa ja muita resursseja investoidaan tietoturvaan. Isommilla yrityksillä on varaa maksaa enemmän ja usein tarvitsevatkin tietoturvaohjelmistoa usealle koneelle.

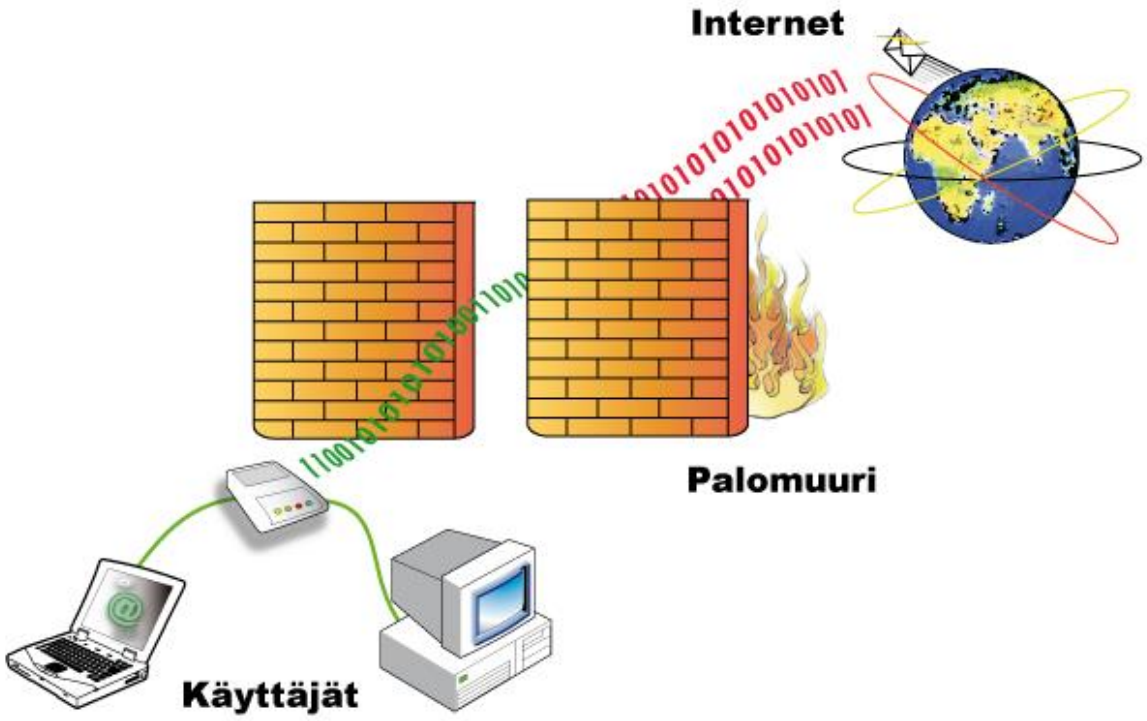
Tämän lisäksi moni yritys ja tietoturvallisuuden henkilö on tässä vaiheessa tietoinen siitä,

kuinka arvokas tehokkaasti toimiva tietoturvajärjestelmä on, ja pitääkin valkohattujen toimintaa tästä syystä tärkeänä (Haasio 2013, 102).

Datan rahallinen arvo on suurin syy sille, miksi isoja yrityksiä tai varakkaita henkilöitä yritetään hakkeroida. Heiltä kerätty tieto on aina tavalla tai toisella arvokasta, joko kiristysmateriaalina tai myytynä eteenpäin. Suuret yritykset ovat erityisen houkuttelevia kohteita, ja heitä vastaa kohdistuneita hyökkäyksiä on alettu kutsumaan nimellä Big Game Hunting. Nämä hyökkäykset ovat kuitenkin kohdistuneet sekä julkisen sektorin organisaatioihin että yksityisiin yrityksiin. (Kyberturvallisuuskeskus 2019).

Useampi rikollinen organisaatio hyötyy erittäin paljon tiedosta, jota yksittäiset hakkerit ja tideonkaappaajat onnistuvat keräämään ja myymään eteenpäin heidän puolestansa. Järjestäytyneet rikolliset ovat hyödyntäneet kaapattuja laitteita monilla eri tavoilla, aiheuttaen suuret taloudelliset tappiot yrityksille ympäri maailmaa (F-Secure 2017).

Kaikki tietokoneet nykyisin toiminnassa hyödyntävät palomuureja torjuakseen erilaisia hyökkäyksiä. Palomuurin rooli on jaotella viestit saapuvien ip-pakettien sisällön ja erinäisten ohjaussääntöjen mukaisesti sallittuun ja estettyyn liikenteeseen (Järvinen 2012, 189). Kuva 3 näyttää, miten palomuuri toimii käytännössä, sallien vain tietynlaisen kommunikaation liikkumisen siitä läpi käyttäjälle ja hänen käyttämille laitteille.



Kuva 3. Yksinkertaistettu kuva palomuurin toiminnasta (MiaK~fiwiki 2005)

Moni yritys, erityisesti IT-alalla, on myös panostanut työntekijöitten koulutukseen, jotta he tunnistaisivat tietoturvaan liittyvät uhat itse ja pystyvät toimimaan tilanteissa, joissa joku yrittää aktiivisesti murtautua sisään.

Vahvat salasanat, laitteiden asentaminen paikkoihin, joista ulkopuoliset eivät pääse helposti laitteisiin käsiksi sekä muut yleiset turvallisuuteen liittyvät järjestelyt kuten säännölliset päivitykset, ja varmuuskopiointi auttavat pitämään sekä yrityksen että yksityishenkilön datan suojattuna.

4.2 Mahdollisuudet ja riskit

Pahantahtoisen hakkerin aiheuttamat taloudelliset tappiot voivat nousta äärimmäisen korkeiksi. Esimerkkinä tästä on elektroniikkafirma Sony, joka vuonna 2011 kärsi 171 miljoonan dollarin menetyksistä hakkerien takia. Kyseinen hakkeriryhmä, joka tunnettiin käyttäjänimellä LulzSec, onnistui väliaikaisesti sulkemaan yrityksen sivustot täysin. Samana vuonna oli puhuttu jopa 12,5 miljardin dollarin tappioista eri yrityksille, jotka ovat aiheutuneet hakkerien toiminnasta. (Haasio 2017, 70.)

Riskit riippuvat suurimmalta osin siitä, mitä metodeja hyödynnetään tietoturvan testauksessa valkohatun osalta. Yksinkertainen skannaus tai murtotestaus virtuaalisessa ympäristössä on suhteellisen vaaraton tapa testata tietoturvan tehokkuutta, kun taas järeät keinot, kun SQL injektio voivat pahimmassa tapauksessa tuhota tietokannan, jota yritettiin valkohatun työkaluilla suojella (Haastattelu 2020.) Mikäli tätä riskiä ei ole otettu huomioon, yksi tai molemmat osapuolet voivat joutua lain osalta selvittelyyn vahingonkorvauksista.

5 Haastattelu

Tutkimusta varten pyrin haastattelemaan henkilöitä, joilla on aiempaa kokemusta toiminnasta yritysten palkkaamina valkohattuhakkereina, tai paljon tietoa yritysten tietoturvajärjestelmistä yleisellä tasolla.

Haastattelun valinta menetelmänä perustui siihen, että sen avulla saisi ajankohtaista tietoa alan ammattilaisilta, jotka ovat pyrkineet pysymään tietoturvan kehityksen tahdissa tehdessään heidän työtään. Aktiivisen vuorovaikutuksen lisäksi metodina se on melko joustava, ja sen voi perustella monesta eri näkökulmasta. (Hirsjärvi 2009, 205.)

5.1 Haastateltavat ja haastattelutilanne

Henkilöitä, joita halusin haastatella, oli viisi kappaletta. Tästä huolimatta vain yksi vastasi kyselyyn, jonka olin lähettänyt. Nämä henkilöt ovat kiireisiä, heidän toimipaikkansa ovat ympäri Suomea ja tutkimuksen aikana olosuhteitten takia tapaamiset kasvotusten olivat tavallista vaikeampia järjestää.

Esitin seuraavat kysymykset haastateltaville henkilöille.

1) Kuka olet ja kauanko olet ollut töissä valkohattuna?
2) Millä tavoin yrityksen tietoturvaa voi turvallisesti testata?
3) Onko jotain metodeja, joissa on riskiä yritykselle?
4) Mitkä ovat olleet yritysten odotukset töitten osalta?
5) Ovatko yritysten odotukset toteutuneet töissä?
6) Onko töissä mitään erityisiä haasteita yrityksen odotusten ohella?

Koska haastatteluja ei pystynyt järjestämään kasvotusten, kysymykset lähetettiin erillisenä tiedostona sähköpostitse, ja täten tutkimuksen metodi vaihtui haastattelusta enemmän kyselyn suuntaan. Tulosten tulkinnasta on tämän takia tullut hiukan hankalampaa, ja tutkimusmetodissa on muitakin haittapuolia. (Hirsjärvi 2009, 195.)

Ensimmäisen kysymyksen tarkoituksena oli kartoittaa henkilön asiantuntijuus, kun taas myöhempien kysymysten myötä pyrin selvittämään valkohatun toimintaa käytännön tasolla sekä heidän suhdettansa yrityksiin työnantajina. Tätä kautta saisi kuvan siitä, mitä hyötyä yritykset ovat saaneet valkohattujen toiminnasta. Samalla saisin paremman ymmärryksen siitä, millaista työnteko valkohattuna on.

5.2 Haastattelututkimuksen tulokset

Kyselyyn vastannut henkilö on Vaasasta kotoisin oleva valkohattuhakkeri nimeltään Jarkko Vesiluoma. Hän on toiminut tehtävissään viiden vuoden ajan, ja aktiivisesti perehtyy tietoturvaan liittyviin asioihin sekä töissä että vapaa-ajallaan (Haastattelu 2020).

5.2.1 Yleiset käytännöt

Valkohattuhakkerit pyrkivät varmistamaan, että kaikki mitä he tekevät yritysten systeemien kanssa on dokumentoitua, ja kirjalliset sopimukset siitä, mitä hän saa tiedolla tehdä on

molemmilla osapuolilla tallella siltä varalta, että tapahtuu jotain odottamatonta (Haastattelu 2020).

Jotta heidän työkalunsa antavat toivotut tulokset, valkohatut pyrkivät hyödyntämään työkaluja, joita rikolliset hakkerit käyttävät. Näin heidän toimintansa pysyy ajantasaisena, ja analyysi tuottaa parempia tuloksia, kun kaikki osalliset tietävät, millaisia iskuja odottaa. Tämä ei kuitenkaan takaa suojaa, sillä hyökkääjällä on melkein aina etulyöntiasema hakkerointitilanteissa (F-Secure 2017).

5.2.2 Tietoturvan testaus

Tietoturvan testaamista varten on useampi eri vaihtoehto, mutta yleensä testausta voi tehdä haavoittuvaisuusskannauksen tai tunkeutumistestauksen avulla. Myös Red Team tyylinen simuloitu tunkeutuminen on katsottu tehokkaaksi tavaksi mitoittaa sitä, kuinka hyvin nykyiset tietoturvajärjestelyt yritysten sisällä toimivat, mikäli tiimi on hyvin järjestäytynyt (Johnson 2011).

Ohjelmat ja simulaatiot eivät ole ainoat työkalut saatavilla, sillä myös asiakkaana toimiva yritys voi altistaa tietoturvansa uhkatekijöille ihan arkisella toiminnalla. Ohjeistus, joka on yleistynyt yritysten keskuudessa tietoturvan suojaamiseksi, on silti hyvä toisinaan käydä läpi, ja valkohattu voi joutua ottamaan tämän huomioon tietoturvan testauksessa, etenkin jos hän meinaa tehdä Red Team-tyylistä testausta.

5.2.3 Palvelujen tarjonta

Valkohattuna palveluita on erilaisia, ainakin yhtä monta kuin hyökkääjillä on vaihtoehtoja, joilla iskeä kohteisiinsa, mutta suurin osa eri työkaluista keskittyy haavoittuvaisuuksien etsimiseen (Haastattelu 2020). Tämän jälkeen tehdään raportit näistä haavoittuvaisuuksista ja pyritään paikkaamaan ne, jolloin tietoturvan laatu paranee. Tiimin koko ja kokemuksen taso voivat vaikuttaa palvelujen laatuun sekä siihen, minkälaista testausta hakkeri pystyy tarjoamaan yritykselle.

Yleisimmät palvelut, joita valkohattu voi tarjota, on penetraatiotestaus, haavoittuvaisuusskannaus ja red team-testaus (Haastattelu 2020). Metodit ovat tarpeeksi monimuotoiset, että tietoturvan vahvuuksista ja heikkouksista voi saada kattavan yleiskuvan, joka helpottaa puutteiden paikkaamisessa.

5.2.4 Kokemukset alalla

Jarkko on toiminut valkohattuhakkerina viisi vuotta, ja ilmoitti, että yritysten odotukset ovat yleistasolla toteutuneet oman työntekonsa osalta. Tästä huolimatta on välillä ollut epäselvyyksiä siitä, mitä hän käytännössä tekee työkseen. Eri analyysimetodit voivat ulkopuolisen silmissä näyttää erittäin samanlaisilta, mutta poiketa luonnossaan ja antamissa tuloksissaan melko paljon. (Haastattelu 2020.)

6 Kirjallisuus

Hakkereista on tässä vaiheessa melko paljon dokumentaatiota saatavilla. Ilmiönä hakkerointi tietoturvamurtona on ollut tiedossa jo 1980-luvulta (Haasio 2017, 70), mutta internetin käytön yleistymisen myötä on kiinnitetty erityistä huomiota siihen, että hakkerit ja krakkerit ovat todellinen uhka sekä yksityishenkilöille että yrityksille, mikäli heillä on laittomuudet mielessä.

Toisaalta valkohattujen tieto ja taidot ovat olleet auttamassa ihmisiä ja yrityksiä jo pitkään, sillä hakkerit ovat melko tietoisia siitä, miten tietoturvajärjestelmät toimivat ja mistä löytää haavoittuvaisuuksia. Heidän työnsä tuloksia on yleisesti katsottu hyvällä (Haasio 2013, 102), kun taas moni hakkeri yritystoiminnan ulkopuolella on saattanut olla tekemässä asioita, joiden hyötyjä ja haittoja on vaikea suoraan arvioida.

Tästä huolimatta on otettava huomioon, että tietomurrot katsotaan rikokseksi tietojen kaappauksen ja muitten verkkohyökkäyksien lisäksi Suomessa ja muualla maailmalla (Poliisi), jonka takia valkohatuille onkin tärkeää tehdä erillinen sopimus yrityksen tai henkilön kanssa aina kun hänen täytyy murtautua tietojärjestelmään.

6.1 Erilaisia Hakkereita

Jotkut valkohattuhakkerit ovat aikoinaan olleet mustahattuja. Eräs tunnettu esimerkki entisestä tietoturvatunkeilijasta on amerikkalainen Kevin Mitnick (Haasio 2017, 70), joka on kirjoittanut teoksen hänen ajoistaan rikollisena sekä muutaman kirjan aiheeseen liittyen, toimien nykyään tietoturva-asiantuntijana istuttuaan useaan kertaan vankilassa erilaisten tietomurtorikosten takia (From Being Hunted By The FBI To Working Alongside Them-Kevin Mitnick, 2016).

6.2 Hakkerit Suomessa

Hakkerien lukumäärä Suomessa on todennäköisesti suhteellisen pieni verrattuna muuhun maailmaan, mutta väkilukuun katsoen niitä löytyy useita. Tunnettu tietotekniikan asiantuntija ja hakkeri sen vanhassa kontekstissa, Linus Torvalds on Suomessa syntynyt IT-alan ekspertti ja on eräs Linux-käyttöjärjestelmän kehittäjistä (Haasio 2017, 68), toimien järjestelmän projektikordinaattorina nykyään.

Muita suomalaisia hakkereita, jotka ovat saaneet jonkun verran kuuluisuutta tunkeutumalla erilaisiin tietojärjestelmiin ovat saksalaissuomalainen Kim Dotcom ja brittiläissuomalainen Lauri Love (Haasio 2017, 70-71).

Valkohattuhakkeri nimeltään Toni Ruhanen oli raportoinut tietoturvaongelmia, joita hän oli löytänyt vuonna 2019 joistakin julkisista palveluista. Hänen raporttinsa jäivät alun perin huomioimatta yritysten osalta, mutta haavoittuvaisuudet ovat yritysten osalta otettu käsittelyyn hänen ansiostaan (Kyberturvallisuuskeskus 2019).

6.3 Etiikka

Hakkerien osalta on ollut paljon keskustelua heidän etiikastansa. Moni mustahattu ei ole etiikasta kiinnostunut, sillä melko suuri osa heidän toiminnastaan menee laittomuuksien puolelle, sekä loukkaa ihmisten yksityisyyttä puhumattakaan taloudellisista tappioista, joita he voivat aiheuttaa heidän toiminnallaan. Jotkut hakkerit taas toimivat enemmän kunnianhimon tai silkan huvin vuoksi, piittaamatta taloudellisista hyödyistä (Haasio 2013, 101).

Rikollinen toiminta on ymmärrettävästi eettisesti kyseenalaista, ja internetin alkuaikoina moni yritys ja valtio olivat huolestuneita kuultuaan tapauksista, jolloin sivuston tai palvelun tietoturvaan oli murtauduttu. Vahingot, joita kokematon tai pahantahtoinen hakkeri pystyi aiheuttamaan, olivat suuret, ja ovat nykyäänkin vakavasti otettavissa oleva uhka.

6.4 Yritystoiminta

Usein hakkereista puhuttaessa sekä fiktiossa että oikeassa elämässä ajatellaan yksittäisiä toimijoita, koneella istuvia neroja, jotka sattuvat murtautumaan toisten ihmisten omistamiin tietoverkkoihin kotoa käsin. Nykyään moni hakkeri toimii ryhmässä, olkoon se sitten ryhmä aktivisteja kuten vuonna 2004 perustettu ryhmä Anonymous (Haasio 2017, 71.) tai hakkereitten luoma tietoturvayritys.

Solita on vuonna 1996 perustettu suomalainen yritys, joka toimii IT-palveluitten kehittäjänä, ja on tehnyt töitä Fortumille, Finavialle, Fazerille ja monille muille. Yksi heidän palveluistansa on WhiteHat-kokonaisuus, joka tunnettaan englanniksi nimellä Solita WhiteHat. Sen ideana on tarkan analyysin myötä löytää haavoittuvaisuuksia ja raportoida ne asiakasyritykselle (Solita 2019).

North European Oil Trade (NEOT) oli ollut Solitan asiakkaana, joka hyödynsi heidän tarjoamaa WhiteHat-palvelua. Solitan tarjoaman SaaS eli Software as a Service-palvelun kautta yrityksen haavoittuvaisuuksia saatiin analysoitua ja raportoitua nopeasti, jolloin yritys pääsi toimimaan niiden paikkaamisessa ilman suuria investointeja tietoturvajärjestelmiin tai erillisiin skannaussysteemeihin (NEOT to minimize information security risks with Solita WhiteHat service – Solita). Tästä päätellen heidän tietoturvansa taso parani huomattavasti, vähentäen hakkereitten mahdollisuuksia tunkeutua heidän järjestelmiinsä.

F-Secure on tietoturvaratkaisuja kehittävä suomalainen yritys, jonka ohjelmisto on pääosin luotu Windows-tietokoneita varten mutta ovat astumassa myös tablettien ja puhelimien piiriin. Kuluttajatuotteiden osalta F-Secure tarjoaa normaalia virustorjuntaa, VPN-palveluja sekä yritystarkoitukseen luotuja versioita virustorjuntaohjelmistostaan. Tietoturvaohjelmiston lisäksi F-Secure on tehnyt Red Team testausta (F-Secure 2017).

Yritykset ovat myös pyrkineet rohkaisemaan hakkereita avustamaan heitä toisin tavoin tietoturvauhkien paikkaamisessa. Google ja Facebook ovat maksaneet palkkioita haavoittuvaisuuksia löytäneille hakkereille (Haasio 2013, 101), ja tätä ilmiötä on alettu kutsumaan nimellä bounty hunting (Bug Bounty Program – Complete List | HackerOne) eli palkkionmetsästys. Sen aikomuksena on rohkaista hakkereita aktiivisesti etsimään tietoturvassa olevia aukkoja ja raportoimaan ne yritykselle sen sijaan, että varastaisi tietoa järjestelmästä. Suurin osa bounty hunting-toimintaan osallistuneista henkilöistä on toiminut yritysten hyväksi, mutta on myös ollut tapauksia, joissa on aiheutettu tahallaan uhka, josta on jälkikäteen pyydetty palkkiota vilpillisesti (Haasio 2013, 101).

Hakkereitten raportointiin ei kuitenkaan aina luoteta. Joskus yritykset eivät syystä tai toisesta huomioi heille lähetettyjä raportteja, tai epäilee ilmoittajan motiiveja. Pahimmassa tapauksessa ilmoitusta tekevää henkilöä voidaan uhata oikeustoimilla, vaikka hänen aikomuksensa olisi avustaa kyseistä yritystä. Kyberturvallisuuskeskus on ohjeistanut sekä valkohattuja että yrityksiä kommunikoimaan tehokkaammin tietoturvariskien torjumiseksi, joka on johtanut ainakin muutamassa tapauksessa todellisiin toimiin tietoturvahaavoittuvaisuuksien korjauksessa. (Kyberturvallisuuskeskus 2019.)

Linux-käyttäjien osalta merkittävänä työkaluna on olemassa Debianiin perustuva jakelupaketti nimeltään Kali Linux, jonka toiminta perustuu tietoteknisten rikosten tutkimiseen ja tunkeutumistestaukseen. Aiemmat versiot ohjelmistosta tunnettiin nimellä BackTrack, ja siinä olevat ohjelmat ovat lisätty mukaan nykyiseen Kali Linux pakettiin. (Kali Linux Documentation.)

7 Lopputulokset ja Pohdinta

Tulosten osalta vertailua on tehty kyselyvastausten ja aiheen kirjallisuuden välillä sekä aiheeseen perehtymisestä yleisellä tasolla. Kyselyn vastauksilla olisi suurempi painoarvo, mikäli vastaajia olisi ollut useampi.

Artikkelit ja materiaalit vaihtelevat melko uusista suhteellisen vanhoihin, mutta tietoturvan yleisessä toiminnassa ei ole vähään aikaan ollut suuria muutoksia, joita pitäisi ottaa huomioon luotettavuuden osalta.

Suurin osa näkee valkohatut ja heidän toimintansa hyvänä asiana yritysten kannalta, antaen tietoturvaan liittyviin asioihin näkökulmia ja työkaluja, joita normaalilla tietoturvavastaavalla ei välttämättä olisi. Tähän johtopäätökseen pääsee lähteitten vaihtelevasta laadusta huolimatta.

7.1 Hakkerien näkökulma tietoturvaan liittyen

Suurin osa tunnetuista hakkereista ovat ihmisiä, jotka ovat erityisen kiinnostuneita IT-alaan liittyvistä asioista, tietotekniikasta ja tietokoneista yleisesti. Moni heistä näkee tietoturvan vahvuuksien ja heikkouksien selvittämisen henkilökohtaisena haasteena ja tapana testata omita taitojaan, kun taas toiset hakkeroivat yrityksiä tai henkilöitä, joista he eivät syystä tai toisesta pidä (Haasio 2013, 101).

Tietoturvajärjestelmien jatkuva päivitys pakottaa hakkerit, olkoon heidän aikomuksensa sitten laillisia tai laittomia, kehittämään uusia tapoja päästä tietoturvajärjestelmien ohi tai etsimään uusia haavoittuvaisuuksia, joita he voivat hyödyntää. Yritykset ja rikolliset molemmat hyötyvät hakkerien taidoista.

7.2 Yritysten näkökulma tietoturvaan liittyen

Yritysten näkökulmasta tietoturvan toimivuus on elintärkeää liiketoiminnalle, sillä moni yritys pitää tallella tietoja, joiden avulla he pystyvät kilpailemaan markkinoilla. Ilman toiminnallista tietoturvaa tärkeää tietoa voi helposti vuotaa kilpailijoille tai sosiaaliseen mediaan, aiheuttaen vahinkoa brändille, puhumattakaan rahasta, jota hakkeri saattaa itselleen vaatia tai jopa suoraan varastaa yritykseltä.

Tästä syystä moni firma investoi paljon rahaa tietojärjestelmää rakentaessa myös tietoturvaan. Valkohattuhakkeri on alan ammattilainen, joka tietää miten toimia hakkerien varalta,

jonka takia moni yritys näkee henkilön palkkaamisen hyvänä investointina. Moni myös täydentää tietoturvaansa koulutuksella ja tietoturvaohjelmistolla kuten virustorjunnalla, johon yleensä myös sisältyy erilaisia skannausohjelmia.

7.3 Tutkimustulokset

Tulokset täsmäävät odotuksia ainakin alustavalla tasolla. Yritykset ovat löytäneet valkohattujen arvon, etenkin sen jälkeen, kun useat isot yritykset ovat kärsineet suuria tappioita hakkereitten ja muunlaisten tietoturvaongelmien jäljiltä. Heidän määränsä yritystoiminnassa on nähtävästi myös noussut, vaikka tietenkin yksin toimivia valkohattuhakkereitakin on todennäköisesti melko paljon.

Suomesta ei löydy julkisia tilastoja tietoturvatestauksesta (Tiainen 2018, 28), joka on vaikuttanut tutkimuksen laajuuteen sekä siihen, että tilastollisen tiedon määrä tutkimuksessa on melko vähäistä.

Lähteitten laatu ja ajankohtaisuus on melko vaihteleva tutkimuksessa, mutta yleisesti palaute valkohattuihin liittyen on ollut melko positiivista. Omasta mielestä on ihan loogista pyrkiä ajattelemaan hyökkääjän tavalla, jotta helpommin tietäisi miten torjua heitä. Mikään puolustus ei ole täydellinen, mutta jos tietää mitkä ovat yleisimmät haavoittuvaisuudet ja miten niitä hyödynnetään, on mahdollista keksiä vastatoimenpiteitä helpommin.

Kyselyn ja tutkimuksen jäljiltä yleiskuva valkohattuhakkerin toiminnasta ei näyttäisi poikkeavan vahvasti normaalista tietoturvaekspertin työstä. Suurin ero on siinä, kuinka paljon valkohattu tietää hakkeroinnista kokemuksen kautta, ja mahdollisesti henkilön omasta historiasta hakkerina. On kuitenkin vaikea sanoa, kuinka moni valkohattu oli ennen mustahattu, vaikka muutama esimerkki olikin löytynyt tutkimuksen aikana erinäisten artikkelien kautta.

7.4 Mahdolliset jatkotutkimukset

Jatkotutkimusta voisi tehdä siitä, kuinka yleisiä valkohattuhakkerit ovat Suomessa, jos ei muualla maailmalla, tai miten heidän metodinsa eroavat muista tietoturvaan perehtyneistä asiantuntijoista kuten yritysten tietoturvavastaavista käytännön tasolla. Lisäksi tutkimuksen kohteena voisi olla erot eri maitten hakkerien toiminnassa lain molemmin puolin.

Näiden lisäksi tarkempaa tutkimusta voisi tehdä metodien kehittymisestä mustahattujen ja valkohattujen sekä muiden hakkerien keskuudessa vuosien myötä. Teknologian kehittyminen on aina ollut keskeinen tekijä hakkerien keskuudessa, ja yleistason sijaan tutkimusta

voi myös tehdä yksittäisistä tietoturvaan liittyvistä työkaluista kuten simuloiduista hyökkäyksistä yrityksen tietoturvaan.

7.5 Oma oppiminen

Tutkimustyyppisen opinnäytetyön laatimisen osalta opin sen, että kaikkeen ei pysty varautumaan, ei väliä kuinka hyvin on pyrkinyt projektia suunnittelemaan. Suurin osa yhteyshenkilöstä ei vastannut heille lähetettyyn kyselyyn, jonka vuoksi tutkimus joutui kääntämään suuntaa haastattelupohjaisesta työstä kirjallisuuskatsaukseksi.

Tämä suunnitelmien muutos kuitenkin sopi henkilökohtaisesti hyvin minulle, sillä olen tottunut tekemään laajamittaista kirjallisuuteen perustuvaa raportointia opiskeluni aikana, ja koen olevani sen osalta hyvin varautunut, vaikka tämä johtikin siihen, että työ on ollut aikataulusta jäljessä ja osittain puutteellinen materiaalin osalta.

Aihe kuitenkin kiinnostaa minua henkilökohtaisesti, jonka takia motivaatio ei hiipunut työtä tehdessä, vaikka välillä kyseenalaistin sitä, saanko tarpeeksi hyvän työn tehtyä aikataulun mukaisesti. Materiaalin riittävyys sekä kyky kirjoittaa hyväksyttävää tekstiä oli yleisimmät huolenaiheet etenkin puolivälin ohituksen jälkeen.

Lähteitten osalta haasteena oli löytää yrityksen puolelta tilastoja ja tietoja, sillä moni ymmärrettävästi ei halua puhua siitä, että heidän tietoturvansa on ollut uhattuna tai jopa täysin ohitettu. Julkisuudessa tietomurrot ovat melko suuri asia, ja yleensä aiheuttavatkin suurta vahinkoa yritysten imagolle ja brändille.

Tilastojen puutteesta huolimatta hakkerien työkaluista ja niiden vaikutuksesta yritysten liiketoimintaan löytyi kyllä tarpeeksi tietoa. Sen muotoilu tutkimusta varten oli taito, jota piti vielä jonkun verran kirjoittamisen aikana kehittää pidemmälle. Aihe oli kiintoisa, sen tutkimisen aikana opin uusia asioita, ja on mahdollista, että tutkin aihetta jatkossakin.

8 Lähteet

Belangia, D. 2015. Securing Single Points of Compromise (SPoC). Luettavissa: https://www.sans.org/reading-room/whitepapers/bestprac/securing-single-points-compromise-spoc-36062. Luettu: 13.05.2020.

Cross Site Scripting (XSS) Software Attack | OWASP Foundation. Luettavissa: https://owasp.org/www-community/attacks/xss/. Luettu: 03.05.2020.

Engebretson, Patrick 2013. The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Syngress. E-Kirja.

F-Secure 2017. The Value of Red Teaming. YouTube-video, katsottavissa: https://www.youtube.com/watch?v=3SRTLZ9HMpQ. Katsottu 04.04.2020.

Järvinen, P. 2012. Arjen Tietoturva, Vinkit & Ratkaisut. Docendo. Espoo.

Haasio, A. 2013. Netin pimeä puoli. Saarijärven Offset Oy. Saarijärvi.

Haasio, A. 2017. Verkkorikokset. BTJ Finland Oy. Vantaa.

HackerOne. Bug Bounty Program – Complete List | HackerOne. Luettavissa: https://hackerone.com/bug-bounty-programs. Luettu: 28.04.2020.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja Kirjoita. 15. uudistettu painos. Tammi. Helsinki.

Johnson, D. 2011. The Assembly and provisioning of a red team. Luettavissa: https://scholarworks.rit.edu/other/758. Luettu: 28.04.2020.

Khin, D. 2016. From Being Hunted By the FBI To Working Alongside Them- Kevin Mitnick. Luettavissa: https://www.appknox.com/blog/from-being-hunted-by-the-fbi-to-working-alongside-them-kevin-mitnick. Luettu: 04.04.2020.

Kyberturvallisuuskeskus 2019. Edistyneet kiristyshyökkäykset yleistyvät – Varo joutumasta saaliiksi! Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/edistyneet-kiristyshyokkaykset-yleistyvat-varo-joutumasta-saaliiksi. Luettu: 15.05.2020.

Kyberturvallisuuskeskus 2019. "Palveluistanne löytyi tietoturva-aukko". Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palveluistanne-loytyi-tietoturva-aukko. Luettu: 17.05.2020.

Kyberturvallisuuskeskus 2019. Toni Ruhanen ja muut valkohatut kuuluvat hyvisjengiin. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toni-ruhanen-ja-muut-valkohatut-kuuluvat-hyvisjengiin. Luettu: 15.05.2020.

Kyberturvallisuuskeskus 2019. Vinkkejä valkohatuille parempaan ja helpompaan yhteistyöhön. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkeja-valkohatuille-parempaan-ja-helpompaan-yhteistyohon. Luettu: 17.05.2020.

Kyberturvallisuuskeskus 2020. Näin suojaudut tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta. Luettu: 15.05.2020.

Kyberturvallisuuskeskus 2020. Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja. Luettu: 17.05.2020.

NEOT to minimize information security risks with Solita WhiteHat service – Solita. Luettavissa: https://www.solita.fi/en/customers/neot-to-minimize-information-security-risks-with-solita-whitehat-service/. Luettu: 26.04.2020.

Palmer, C. 2001. Ethical Hacking. Luettavissa: http://pdf.textfiles.com/security/palmer.pdf. Luettu: 01.04.2020.

Palomuuri – Wikipedia 2003. Luettavissa: https://fi.wikipedia.org/wiki/Palomuuri. Luettu: 14.04.2020.

Poliisi. Kyberrikollisuus. Luettavissa: https://www.poliisi.fi/rikokset/kyberrikollisuus. Luettu: 15.05.2020

Sanastokeskus TSK ry. 2018. Kyberturvallisuuden sanasto. Luettavissa: http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf. Luettu: 23.03.2020.

Solita Oy 2019. Solita WhiteHat cyber security service. YouTube-video, katsottavissa: www.youtube.com/watch?v=IwX8goO1Sy8. Katsottu 14.04.2020.

SQL Injection FAQ – SQLSecurity Home 1999. Luettavissa: http://www.sqlsecurity.com/faqs-1/sql-injection-faq. Luettu: 13.04.2020.

The SQL Injection Knowledge Base 2012. Luettavissa: https://www.websec.ca/kb/sql_injection. Luettu: 13.04.2020.

Tiainen, K. 2018. Kokonaisvaltaisen tietoturvatestauksen hyödyt yrityksille. Opinnäytetyö. Haaga-Helian Ammattikorkeakoulu. Helsinki. Luettavissa: https://hhthesis.haaga-helia.fi/thesis.php?id=3969 Luettu: 03.05.2020.

What is Kali Linux? | Kali Linux Documentation. Luettavissa: http://kali.org/docs//introduction/what-is-kali-linux/. Luettu: 08.04.2020.

WhiteHat cyber security service – Solita. Luettavissa: https://www.solita.fi/en/whitehat-cyber-security-service/. Luettu: 26.04.2020.

Liitteet

Liite 1. Haastattelukysymykset ja vastaukset

1) Kuka olet ja kauanko olet ollut töissä valkohattuna?

Olen Jarkko Vesiluoma, Vaasasta. Olen toiminut valkohattuhakkerina noin viisi vuotta, jona aikana olen raportoinut lukuisia haavoittuvuuksia eri yrityksille ympäri Suomea ja maailmaa. Teen valkohattuhakkerina tietoturvaan liittyviä asioita vapaa-ajallani.

2) Millä tavoin yrityksen tietoturvaa voi turvallisesti testata? Yrityksen tietoturvaa voi testata ainoastaan (kirjallisen) luvan kanssa, tämä takaa sen, että siitä ei joudu ongelmiin lain tai yrityksen kanssa. Toinen tärkeä asia on ymmärtää testattavien työkalujen ja kohteen toiminta sekä mitä testaukset voivat aiheuttaa ja tällä tavoin varoa aiheuttamasta vahinkoa kohteelle. On myös suositeltavaa testata kohdejärjestelmistä tehtyjä klooneja vasten, näin varmistaen, että tuotannolle ei aiheudu ongelmia.

3) Onko jotain metodeja, joissa on riskiä yritykselle? Kyllä, esimerkiksi SQL injektiot, jotka voivat pahimmillaan aiheuttaa tietokannan tuhoutumisen tai järjestelmän toimimattomuuden.

4) Mitkä ovat olleet yritysten odotukset töitten osalta? Yrityksien odotukset testauksien osalta ovat haavoittuvuuksien löytämisessä ja näiden korjausehdotusten saamisessa. Yritykset tietenkin odottavat, että testauksissa kaikki haavoittuvuudet löytyvät, mutta se on suhteellista testauksissa käytettyyn aikaan.

5) Ovatko yritysten odotukset toteutuneet töissä? Kyllä.

6) Onko töissä mitään erityisiä haasteita yrityksen odotusten ohella? Kyllä, joskus yrityksen on hankala pukea sanoiksi halujaan/tarpeitaan. Koska tilaajana ei välttämättä ole tekninen henkilö, hän voi esimerkiksi sekoittaa haavoittuvuusskannauksen ja penetraatiotestauksen tai niin sanotun red teamauksen keskenään ja näin ollen tilata haavoittuvuusskannauksen, jonka kuvittelee olevan penetraatiotestaus.