Lauri Vikström

Pilvipalveluihin kohdistuvat hyökkäykset ja niiltä suojautuminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

20.4.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Lauri Vikström Pilvipalveluihin kohdistuvat hyökkäykset ja niiltä suojautuminen 37 sivua 20.4.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Ohjelmistotekniikka
Ohjaaja(t)	Lehtori Ilpo Kuivanen

Tämän insinöörityön tarkoitus oli tutkia erilaisia tapoja, joilla pilvipalvelujen kimppuun voi hyökätä sekä keinoja estää kyseiset hyökkäykset. Työ on pääosin suunnattu pilvipalvelujen ylläpitäjille, mutta myös pilvipalvelujen käyttäjät voivat hyötyä työn tiedoista.

Työssä tarkastelun alla on kolme asiaa: hyökkääjät, hyökkäykset ja heikkoudet. Hyökkääjiä tarkastelemalla yritetään löytää heidän motiivinsa ja toimintatapansa, ja hyökkäyksistä yritetään löytää niin tuntomerkit kuin torjuntakeinot. Työssä käydään myös läpi tyypilliset heikkoudet pilvipalvelujen tietoturvassa ja erilaisia keinoja poistaa kyseiset heikkoudet.

Tämän selvityksen avulla pilvipalvelut voivat entistä helpommin varautua erilaisiin hyökkäyksiin. Hyökkäykset on paljon helpompi torjua, kun niiden toiminta on tiedossa. Myös yleisten heikkouksien torjuminen vaikeuttaa hyökkääjien tehtävää huomattavasti.

Avainsanat	pilvipalvelut, tietoturva

Author	Lauri Vikström
Title	Attacks against Cloud Services and How to Protect against Them
Number of Pages	37 pages
Date	20 April 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Software
Instructor(s)	Ilpo Kuivanen, Senior Lecturer

The purpose of this final year project was to inspect various ways that cloud services can be attacked as well as ways to prevent said attacks. The study is mostly intended for providers of cloud services, but the users of cloud services may also find it useful.

Three subjects are examined in the study: attackers, attacks and weaknesses. By examining the attackers, the study tries to find out their motives and modi operandi. By examining the attacks, the study tries to find out both their signs and ways to prevent them. The study also goes through common weaknesses in cloud service security and ways to remove them.

With the help of the present work, cloud service providers have an easier time to prepare themselves for different attacks. It is much easier to prevent attacks once one understands how they work. Removing common weaknesses will also make the work of attackers much harder.

Keywords	cloud services, computer security

Sisällys

Lyhenteet

API	Application Programming Interface. Ohjelmointirajapinta, jonka avulla ohjelma voi lähettää pyyntöjä toiselle ohjelmalle.
APT	Advanced Persistent Threat. Hyökkäys, jossa hyökkääjä yrittää pysyä järjestelmässä huomaamatta pitkään.
DDoS	Distributed Denial of Service. Hyökkäys, jossa hyökkääjä käskee hallitsemiaan koneita lähettämään turhia palvelupyyntöjä kohteelle.
DoS	Denial of Service. Hyökkäys, jossa hyökkääjä lähettää koneeltaan kohteelle turhia palvelupyyntöjä.
EV-sertifikaatti	Extended Validation -sertifikaatti. Ulkoisen yrityksen tekemä todennus siitä, että sivuston omistaa se, joka väittää omistavansa sivuston. Vaihtaa palvelimen käyttämään HTTPS -protokollaa.
HTML	Hypertext Markup Language. Verkkosivujen käyttämä merkintäkieli, joka voi sisältää hyperlinkkejä.
HTTP	Hypertext Transfer Protocol. Protokolla, jolla tietokoneet siirtävät tietoa.
HTTPS	Hypertext Transfer Protocol Secure. Protokolla, jolla tietokoneet siirtävät tietoa suojatusti. Turvallisempi kuin HTTP.
IaaS	Infrastructure as a Service. Pilvipalvelun malli, jossa asiakas ostaa tarjoajalta vain muistia ja/tai suorituskykyä, ei mitään toimivaa ohjelmaa.
MD5	Message Digest 5. Algoritmi, joka luo 128-bittisen tiivisteen annetusta syötteestä. Tiivisteen perusteella syötteestä ei voi päätellä yhtään mitään. Sama syöte antaa kuitenkin aina saman tiivisteen.
PaaS	Platform as a Service. Pilvipalvelun malli, jossa asiakas ostaa tarjoajalta ympäristön, jossa hän voi luoda tai käyttää omia ohjelmiaan.

PBKDF2 Password-Based Key Derivation Function 2. Funktio, jolla voi luoda vahvoja tiivisteitä. Se toimii luomalla tiivisteen aiemmasta tiivisteestä ja toistamalla tätä monta kertaa.

SaaS Software as a Service. Pilvipalvelun malli, jossa asiakas ostaa tarjoajalta valmiin ohjelman, jota hän voi käyttää haluamallaan tavalla.

SHA-1 Secure Hash Algorithm 1. Algoritmi, joka luo 160-bittisen tiivisteen annetusta syötteestä. Tiivisteen perusteella syötteestä ei voi päätellä yhtään mitään. Sama syöte antaa kuitenkin aina saman tiivisteen.

SHA-256 Secure Hash Algorithm 256. Algoritmi, joka luo 256-bittisen tiivisteen annetusta syötteestä. Tiivisteen perusteella syötteestä ei voi päätellä yhtään mitään. Sama syöte antaa kuitenkin aina saman tiivisteen.

SPI Software, Platform, Infratructure. Lyhenne yleisimmistä pilvipalvelutyypeistä.

SSL-sertifikaatti Secure Sockets Layer -sertifikaatti. Ulkoisen yrityksen tekemä todennus sertifikaatin omistajasta. Vaihtaa palvelimen käyttämään HTTPS -protokollaa. Ei yhtä vahva todennus kuin EV-sertifikaatti. Nykyään SSL-protokollaa kutsutaan Transport Layer Security -protokollaksi. Sen lyhenne on TLS.

UTF-8 Unicode Transformation Format – 8-bit. Koodaustapa merkkien (kuten kirjainten ja numeroiden) tallentamiseksi.

XaaS X as a Service. Yläkäsite kaikille asioille, joita pilvestä voi ostaa.

1 Johdanto

Pilvipalveluja hyödyntävät yritykset kasvavat 19,6 % nopeammin kuin vastaavat yritykset, jotka eivät hyödynnä pilvipalveluja [1]. Ei siis ole mikään ihme, että moni yritys on kiinnostunut pilvestä. Tällöin asiakas maksaa vähän toiselle yritykselle, niin he hoitavat palvelusta riippuen kaiken laitteistosta aina valmiiseen ohjelmaan saakka. Näin asiakas voi keskittyä kokonaan omaan työhönsä.

Kun asiakas tallentaa tietonsa jonkun toisen palvelimelle, syntyy kuitenkin erinäisiä turvallisuusriskejä. Kuinka paljon asiakas oikeastaan tietää palvelun tapahtumista? Missä asiakkaan tiedot oikeasti ovat? Kuinka hyvin palvelun tarjoaja on varautunut niin vahinkoihin kuin tahallisiin hyökkäyksiin?

Jos joku pitää tietonsa omalla koneellaan tai palvelimellaan, tietää hän kaiken, mitä hänen tiedoilleen tapahtuu. Pilvipalveluissa sekä palvelun tarjoajan että palvelun ostajan täytyy päästä yhteisymmärrykseen turvallisuutta lisäävistä säännöistä. Kummankin osapuolen pitää noudattaa näitä sääntöjä. Yksikin heikko kohta riittää hyökkääjälle.

Tässä työssä tarkastellaan erilaisia tapoja, joilla hyökkäysten riskiä voi pienentää. Tarkastelun alla on myös keinoja, joilla voidaan myös rajoittaa onnistuneen hyökkäyksen aiheuttamaa vahinkoa. Työ tarkastelee myös yleisimpiä reittejä, joita pitkin hyökkäykset kulkevat sekä keinoja tukkia niitä.

2 Määritelmät

Aluksi on hyvä määrittää, mistä työ tarkkaan ottaen kertoo. Pilvi on nimittäin vielä kirjoitushetkellä varsin epämääräinen käsite, sillä alan terminologia ei ole vielä vakiintunut. On siis tarpeen käydä läpi työn kannalta tärkeitä käsitteitä.

2.1 Pilvipalvelut

Pilvipalveluja on kaikenlaisia, ja niiden suosion ja epätarkan määritelmän takia koko sanan merkitys on alkanut hälventyä. Kuitenkin monissa määritelmissä on jotain yhteistäkin.

Urbaani Sanakirja määrittelee pilvipalvelun seuraavasti [2]: ”Yrityksen ulkopuolinen tiedonkäsittelyn vuokrapalvelu, uusi bisnesidea, jonka merkitys kasvaa koko ajan”.

VirtualisointiWikin määritelmässä korostetaan vapaata pääsyä tietotekniikkaresursseihin. Näitä resursseja voidaan ottaa ja poistaa käytöstä tarpeen mukaan. [3.] VirtualisointiWiki mainitsee myös NIST:n määrittelemät viisi pilvipalvelun ominaispiirrettä. Nämä piirteet ovat seuraavat:

- nopea joustavuus
- resurssien yhteiskäyttö
- itsepalvelullisuus
- päätelaiteriippumattomuus
- resurssien käyttö ja valvonta.

Tietohallintopalvelu.fi puolestaan myöntää sanan olevan huonosti määritelty ja sekava [4]. Sivusto kuitenkin antaa pilvipalvelulle kolme vaatimusta:

- Palvelulta voi pyytää eri asioita, kuten tallennustilaa tai laskentatehoa, ja pilvi antaa ne nopeasti käyttöön.
- Moni sovellus (ja moni käyttäjä) voi käyttää pilveä samaan aikaan.
- Palvelun käyttö vaatii ainoastaan internetyhteyden.

Sivusto korostaa, että pilviteknologiaa ymmärtävät eivät kutsu pelkkää datan tallentamista pilvipalveluksi. Jotkin yritykset tosin kutsuvat sitäkin pilvipalveluksi.

Web-opas sen sijaan sanoo pilvipalvelun määräytyvän seuraavista ominaisuuksista [5]:

- Käyttäjä voi mennä verkkosivustolle ja hankkia resursseja itsenäisesti. Puhelinneuvottelut tai sähköpostisodat eivät ole tarpeen.
- Pilvipalveluissa ei ole räätälöityjä sopimuksia. Jos sellainen on, on kyseessä jonkinlainen ulkoistuspalvelu.
- Resursseja voi ottaa käyttöön tai poistaa käytöstä tilausta muuttamalla.
- Sama pilvipalvelu on käytössä usealle asiakkaalle samanaikaisesti. Asiakkaiden ei tarvitse huolehtia siitä, miten tämä suoritetaan.
- Ohjelmointirajapinta, jonka avulla asiakkaat voivat itsenäisesti laajentaa pilvipalvelua, jos kokevat sen tarpeelliseksi (ei kaikissa pilvipalveluissa).

Jo nämä esimerkit paljastavat, että sanalla pilvipalvelu on monia erilaisia määritelmiä. Koska tämä työ käsittelee pilven tietoturvaa, voimme käyttää varsin leveää määritelmää, ja ottaa mukaan myös sellaisia palveluita, joita vaikkapa Tietohallitopalvelu.fi ei hyväksyisi. Voisimme siis määritellä pilvipalvelun seuraavasti:

- Pilvipalvelun käyttö vaatii ainoastaan verkkoyhteyden.
- Moni käyttäjä ja/tai sovellus voi käyttää yhtä pilveä samaan aikaan.
- Pilven asiakkaat voivat käyttää pilven resursseja tarpeensa mukaan. Pilvi voi kuitenkin määrittää asiakkaille resurssikaton.
- Asiakkaat eivät tiedä pilven palvelimien tarkkaa sijaintia ja toimintaa, eikä sillä myöskään ole väliä.
- Asiakkaat eivät tiedä, kuka pääsee heidän tietoihinsa käsiksi.

Tämän määritelmän mukaan voimme siis ottaa mukaan sellaisiakin palveluita, jotka vain säilyttävät käyttäjän dataa verkossa. Tietoturvan suhteenhan ne muistuttavat paljon ”oikeita” pilvipalveluja.

2.2 Pilvipalvelujen tyypit

Pilvipalvelu on varsin korkean tason käsite, joka kattaa alleen lukuisia erilaisia palvelutyyppejä. Näistä palveluista yleisimmät ja suosituimmat ovat Software as a Service

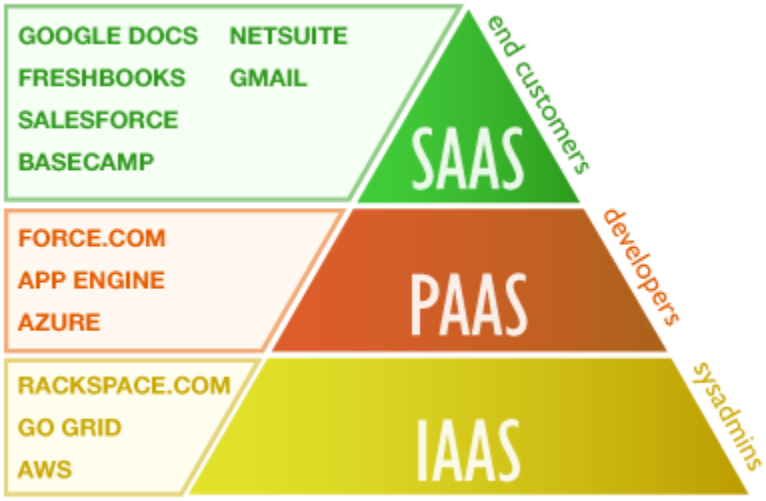
(SaaS), Platform as a Service (PaaS) ja Infrastructure as a Service (IaaS). Näistä käytetään lyhennettä SPI (Software, Platform, Infrastructure). [6; 7.]

SaaS-tyyppiset pilvipalvelut tarjoavat käyttäjälle valmiin ohjelman, jota tämä voi vapaasti käyttää. Palvelun tarjoaja huolehtii ohjelman ylläpidosta ja päivittämisestä. SaaS on todennäköisesti tutuin pilvipalvelumalli, sillä sen kohteena on loppukäyttäjä. [8; 9.]

PaaS-tyyppinen pilvipalvelu sen sijaan tarjoaa alustan, jossa palvelun asiakas voi luoda, kehittää ja käyttää haluamiaan ohjelmia. Palvelun tarjoaja tarjoaa asiakkaalleen erilaisia kehitystyökaluja, jotka hän myös pitää päivitettyinä ja toimintakuntoisina. PaaS on siis suunnattu ohjelmistojen kehittäjille. [8; 9.]

Vastaavasti IaaS-pilvipalvelu tarjoaa ainoastaan resursseja, kuten laskentatehoa, tallennustilaa ja verkkoyhteyksiä. Asiakas voi käyttää näitä resursseja miten haluaa. Palvelun tarjoaja huolehtii resursseja tarjoavien palvelinkoneiden toimintakunnosta. Asiakas siis ostaa laitteiston sijaan suoraan haluamiansa resursseja. [8; 9.]

Kuva 1 esittää esimerkkejä edellä mainituista pilvipalvelutyypeistä, palvelutyyppien suhteesta toisiinsa sekä palvelujen kohdeyleisöstä.



Kuva 1. SPI-palveluesimerkit ja kohderyhmät. [10.]

Nämä ovat kuitenkin vain yleisimmät pilvipalvelujen tyypit. GlobalDots kertoo myös seuraavanlaisista pilvipalveluista: Storage as a Service, Security as a Service, Data as

a Service, Test environment as a Service, Desktop as a Service ja API as a Service. [10.]

GlobalDots ei kuitenkaan kerro kaikkia pilvipalvelutyyppejä. ESDS kertoo kahdesta muusta palvelutyypistä: Hardware as a Service ja Workplace as a Service [11]. Kumpikin edellisistä artikkeleista on kuitenkin kirjoitushetkellä vanha, joten uusia palvelutyyppejä on varmasti ilmestynyt ajan myötä.

Kaikista näistä pilvipalvelutyypeistä käytetään usein lyhennettä XaaS. XaaS tarkoittaa useita asioita, kuten X as a Service, Anything as a Sevice tai Everything as a Service. Kaikki nuo tarkoittavat samaa asiaa: jotakin jota voi ostaa pilvestä sen sijaan, että se hankittaisiin tai luotaisiin paikan päällä. Kaikki pilvipalvelut ovat XaaS-palveluja. [12.]

2.3 Tietoturva ja hyökkäys

Hyökkäys tarkoittaa yleensä jotain pahaa: mieleen voi tulla kuvia pahoinpitelystä, ryöstöstä tai sodasta. Tietotekniikan yhteydessä hyökkäys ei kuitenkaan välttämättä ole paha asia: palvelun tarjoaja voi palkata jonkun hyökkäämään palvelunsa kimppuun kokeillakseen turvatoimiensa tehokkuutta.

Tästä pääsemme sanaan tietoturva ja siihen, mitä se tarkkaan ottaen on. Sitä on määritetty muun muassa seuraavasti.

Sanastokeskus TSK:n termipankki määrittelee tietoturvan näin [13]:

> järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus
>
> huomautus
>
> Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.
>
> Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit on otettu huomioon ja minimoitu.

Suomen internetoppaan mukaan tietoturva tarkoittaa toimenpiteitä, joiden ansiosta yhtiön tiedot pysyvät koskemattomina [14]. Opas määrittää tietoturvan tavoitteeksi yhtiön tai organisaation tietojen:

- eheys
- kiistämättömyys
- luottamuksellisuus
- pääsynvalvonta
- saatavuus
- tarkastettavuus.

Eheys tarkoittaa, että tieto on oikeaa. Kiistämättömyys tarkoittaa, että tietoa käsitelleet voidaan tunnistaa. Luottamuksellisuus tarkoittaa ainoastaan valittujen henkilöiden pääsyä tietoon. Pääsynvalvonta tarkoittaa tiedon käsittelyn valvomista ja rajoittamista. Saatavuus tarkoittaa helppoa ja vaivatonta pääsyä tietoon, jos siihen on oikeus. Tarkastettavuus tarkoittaa, että täytyy olla keino osoittaa tietojen pitävän paikkansa.

Toisin kuin pilvipalvelun määritelmässä, nämä samat asiat esiintyvät muissakin määritelmissä, kuten T. Karvin [15] ja Pekka Poutaisen [16] määritelmissä.

Valtiovarainministeriö sanoo hyökkäyksen tarkoittavan seuraavaa [17]: ”Yritys vahingoittaa tai rajoittaa tietojärjestelmän tai tietoverkon toimintaa, esimerkiksi tunkeutumalla suojattuun tietojärjestelmään”.

Muut lähteet eivät oikein halua määritellä hyökkäystä. Tämän työn puitteissa voimme yksinkertaisesti sanoa, että hyökkäys on tahallinen yritys rikkoa tietoturvaa.

2.4 Heikkoudet

Tietoturvasta ja hyökkäyksistä puhuttaessa on hyvä käsitellä myös heikkouksia. Heikkouden määrittäminen voi olla yllättävän vaikeaa, mutta moni määrittelee sen suunnilleen samoilla tavoilla [18;19]. Tämän työn puitteissa heikkoudet ovat asioita, joiden

avulla hyökkääjä voi kiertää pilvipalvelun käyttämiä suojausmenetelmät. Katsomme muitakin asioita kuin järjestelmän sisäisiä virheitä.

Klassinen esimerkki heikkoudesta on salasanan päätyminen vääriin käsiin. Se ei itsestään ole hyökkäys, mutta se mahdollistaa hyökkäyksen tai helpottaa sitä.

Jos tietoturvahyökkäystä verrataan fyysiseen murtovarkauteen, hyökkäys voisi olla vaikkapa lukon tiirikointi. Heikkous sen sijaan olisi avaimen päätyminen vääriin käsiin. Se ei ole murtotapa, mutta se helpottaa sisälle pääsyä merkittävästi. Kannattaa siis pitää niin avaimet kuin salasanat turvassa.

3 Hyökkäysten ennaltaehkäisy

Mikään suoja hyökkäyksiä vastaan ei ole täydellinen. Myös tietotekniikan suuret nimet, kuten Microsoft, [20] Google [21] ja Apple [22] ovat joutuneet hyökkäysten uhreiksi. Jos nämä tietojätitkään eivät voi suojata tuotteitaan ja/tai palvelujaan kaikilta hyökkääjiltä, niin miten kukaan voi olettaa muidenkaan yritysten pystyvän samaan?

Täysin murtovarmaa tietojärjestelmää ei ole olemassa unelmien ulkopuolella. Järjestelmät ovat ihmisten suunnittelemia, ja ihmiset tekevät toisinaan virheitä, tai ainakin heiltä jää huomaamatta järjestelmän toiminta erikoistapauksissa. Hyvinkin suunniteltu järjestelmä saattaa ajan kuluessa muuttua turvattomaksi, kun käyttäjien laitteiston suorituskyky ja tallennustila kasvavat ja halpenevat.

Järjestelmän ei kuitenkaan välttämättä tarvitse olla täysin murtumaton. Jatkuvan valvonnan avulla moni hyökkäys voidaan pysäyttää ennen kuin ne tekevät vahinkoa. Jos järjestelmään murtautuminen on tarpeeksi hankalaa ja tietomurron oletettu hyöty tarpeeksi pieni, saattaa hyökkääjä jättää hyökkäyksensä tekemättä tai kohdistaa sen toiseen järjestelmään.

Tästä pääsemme seuraavaan kysymykseen: miten hakkeri valitsee kohteensa? Vastaus riippuu siitä, miksi hakkeri ylipäänsä yrittää tehdä tietomurtoa. Suomen laissa tietojärjestelmän luvaton käyttö tai sen yritys on rikos. Murron motiivilla ei ole väliä; urhei-

lumurto on rangaistavaa siinä missä vahingon tekeminenkin. Vahingon tekemisestä voi tosin saada muunkin rangaistuksen. [23.]

Muissa maissa on omat lait, mutta esimerkiksi EU-direktiivi 2013/40/EU pitää tietomurtoa rikoksena [24]. Hakkeri siis haluaa jotain, jonka vuoksi kannattaa ottaa riski sakon tai vankilatuomion saamiseksi.

Se, mitä hakkeri haluaa, riippuu hänestä itsestään [25; 26]. Hakkereilla ei loppujen lopuksi ole niin montaa motiivia rikkoa lakia, joten heidät on varsin yksinkertaista lajitella sen perusteella [27]. Yksi motiivi on yleinen hakkerien keskuudessa. Vaikka heidän toimintansa on laitonta, jää siitä harvoin kiinni, jolloin hakkeria ei tietenkään rangaista [28]. Tieto siitä, että rikoksesta ei jää kiinni, madaltaa kynnystä rikoksen tekoon huomattavasti.

Tarkastellaan seuraavaksi hakkerien motiiveja sekä mahdollisia keinoja sellaisen pilvipalvelun tekemiseen, joka ei hakkereita kiinnosta. Eri lähteet ovat hieman eri mieltä motiiveista: jotkut haluavat korostaa vaikkapa itselleen työskentelevien ja hallituksen tai armeijan palvelussa olevien hakkerien eroja; toisten mielestä kumpikin työskentelee rahasta.

Seuraavaksi esitellään erilaisia hakkereita. Hakkerien jaottelu on tehty motiivin perusteella. Jokaiselle tyypille on myös annettu kuvaava nimi.

3.1 Murtovaras

Murtovarkaan motiivi on yksinkertainen: raha. Murtautumalla tietojärjestelmään hän haluaa joko suoraan rahaa, ostaa jotain itselleen toisten rahoilla tai jotain, mitä hän voi myydä.

Loppujen lopuksi tämä hakkeri ei eroa fyysisen maailman murtovarkaasta paljoakaan. Toinen murtautuu omakotitaloihin, huoltoasemiin ja pankkeihin, toinen kannettaviin, pöytäkoneisiin ja palvelimiin. Kumpikin yrittää ottaa jotain, mikä ei heille kuulu.

Tällä hakkerilla on monia etuja kollegaansa nähden: verkkoyhteyden avulla hän voi hyökätä kaikkiin verkkoon kytkettyihin koneisiin, kun taas fyysinen varas on usein rajoittunut tienooseensa. Tietomurtoa on myös paljon vaikeampi todistaa: esimerkiksi huoltoasemalla rikokselle on usein todistajia, jos murtoa yritetään aseman ollessa auki. Jos asema taas on suljettu, jää rikollisesta kuva valvontakameroihin. Lisäksi puuttuvat tavarat paljastavat ainakin rikoksen tapahtuneen. Tietomurrossa sen sijaan hakkeri voi vain kopioida datan, jolloin siitä jää tuskin mitään jälkiä. Mahdolliset lokitiedostot paljastavat hyökkääjän henkilöllisyydestä paljon vähemmän kuin valvontakameran nauha.

Koska murtovaras haluaa rahaa, on häneltä suojautuminen yksinkertaista: luo pilvipalvelu, jossa ei ole mitään tietoa, jota voi muuttaa rahaksi. Jos pilvipalvelu esimerkiksi vain tallentaa kuvia, joita kuka vain voi katsella, ei murtovaras todennäköisesti ole kiinnostunut kyseisestä pilvipalvelusta. Ainoat tiedot, josta hän voisi saada rahaa, olisivat käyttäjien tilien tiedot. Moni käyttää samoja tunnuksia useissa palveluissa, joten yhden palvelun kirjautumistunnusten avulla voi päästä useaan paikkaan.

Kannattaa kuitenkin pitää mielessä, että arvokas tieto on yllättävän laaja käsite. ”Entä sitten, jos joku saa selville synnyinkaupunkini tai äitini tyttönimen? Turhaa nippelitietoa!” saattaa moni ajatella, kunnes muistaa, että moni paikka käyttää noita varmennekysymyksinä, jos käyttäjä unohtaa salasanansa.[29] Jos hakkeri saa nuo tiedot ja esittää unohtaneensa salasanan, saa hän haltuunsa uhrin tilin. KotiPizza-tilin menetys ei ehkä kuullosta kovin pahalta, mutta kun hakkeri tilaa itselleen kymmenen tuhatta pizzaa ja KotiPizza lähettää tilin omistajalle laskun, on leikki varmasti kaukana.

Varmennekysymykset alkavat olla jo historiaa, ja ominaisuus kannattaa jättää pois uusien palvelujen suunnitelmista. Identiteettivarkaus on sen sijaan on uhka nykyäänkin. Mitä enemmän hyökkääjä tietää kohteesta, sitä helpommin hän voi kerätä kohteesta lisää tietoa.

Nykyään kannattaa myös muistaa big data. Big data tarkoittaa valtavaa määrää dataa, josta ei ole suoraa hyötyä. Siitä voi kuitenkin kaivaa merkitystä, vaikkapa trendejä. Se on jo miljardiluokan bisnes. [30.] Esimerkiksi kaupan kuitit ovat osa big dataa.

Arvoton data on siis nykyään varsin harvinaista, joten murtovarkaisiin kannattaa aina varautua.

3.2 Kunnian etsijä

Kunnian etsijä, nimensä mukaisesti, haluaa mainetta ja kunniaa. Tietyissä piireissä paljon tietotekniikasta ymmärtävä saa osakseen paljon arvostusta [31]. Mikäpä olisikaan parempi tapa näyttää taitonsa kuin ottamalla haltuunsa jonkun toisen järjestelmä, jota suojaavat ammattilaisryhmien suunnittelemat palomuurit ja virussuojat?

Näissä hakkereissa on paljon vaihteluja. Jotkut etsivät turvallisuusaukkoja tietojärjestelmissä vain kertoakseen järjestelmän omistajalle aukosta [27]. Tämäkin on rikos, ellei kyseistä hakkeria ole palkattu etsimään aukkoja.

Jotkut kunnian etsijät vain haluavat todistaa voivansa päästä sisälle. Päästyään sisälle he ovat jo hoitaneet hommansa ja lopettavat.[25.] Jotkut haluavat jättää todisteen käynnistään. Toisinaan todiste on pelkkä pikku jekku. Toisinaan he tuhoavat niin paljon dataa kuin ehtivät. Se on virtuaalista vandalismia [26].

Vaikka kunnian etsijät eivät suoraan vahingoita palveluita tai laitteita, joihin he murtautuvat, ovat he silti ongelma. Kiusaus vuotaa murtautumismenetelmä verkkoon voi olla vastustamaton. Sitten onkin vain ajan kysymys, milloin menetelmä rantautuu jollekulle, joka aikoo vahingoittaa palvelua tai laitetta.

Kunnian etsijän torjumisessa on sellainen ongelma, että hyvät tietosuojat vain innostavat heitä. Mitä paremman suojan murtaa, sitä parempi hakkeri on ja sitä enemmän kunnioitusta saa. Vastaavasti huonosti suojatut sivustot voivat päätyä aloittelevien hakkerien käyttöön ponnahduslaudoiksi. [27.]

Tässä tapauksessa paras vaihtoehto on tulella tulta vastaan taistelu. Voi palkata jonkun noista apua tarjoavista hakkereista. He ovat jo valmiiksi kiinnostuneita asiasta, joten he todennäköisesti pitävät itsensä ajan tasalla. He myös osaavat ajatella kuten hyökkääjät, sillä he ovat olleet hyökkäysten takana.

3.3 Mielenosoittaja

Mielenosoittaja on täysin toista maata kuin kaksi edellistä tyyppiä. Murtovaras haluaa itselleen rahaa tai jotain rahan arvoista, kunnian etsijä mainetta. Kumpikin vahingoittaa toisia vain, koska se on heistä paras menetelmä saada se, mitä he oikeasti haluavat.

Tämä ei päde mielenosoittajaan. Hänelle toisen vahingoittaminen ei ole välttämätön paha päämäärän saavuttamiseksi, vaan itse päämäärä. Hän voi siis käyttää sellaisia hyökkäyksiä, joita muut hakkerit välttävät.

Mielenosoittajan motiivi on kosto tai viha. Hän kokee, että palvelu tai yritys on jollain tavalla loukannut häntä tai toiminut jollain muulla lailla moraalittomasti. Mielenosoittaja päättää sitten ottaa oikeuden omiin käsiinsä ja jakaa rangaistuksen henkilökohtaisesti.

Mielenosoittajien teot pääsevät toisinaan otsikkoihin. Esimerkiksi Phantom Squad väitti kaataneensa PlayStation Networkin vuoden 2016 alussa [32]. Taustalla ei ollut rahallista tai poliittista syytä. Ainoa jäljellä oleva syy lienee siis kosto jostain, mitä Sony oli tehnyt.

Hyökkäykselle löytyy monia mahdollisia syitä. Sony on esimerkiksi joutunut maksamaan sakkoja kartelliin osallistumisesta [33]. Koska kohde oli nimenomaan PlayStation Network, hyökkääjät saattoivat myös olla Microsoft- tai Nintendo-faneja, jotka halusivat tukea alustaansa hyökkäämällä sen kilpailijan kimppuun. Sony on myös suuri, vanha ja varakas yritys. Jotkut ihmiset suhtautuvat sellaisiin yrityksiin hyvinkin negatiivisesti. Joku Sonyn työntekijä, nykyinen tai entinen, on myös voinut kokea yrityksen kohdelleen häntä kaltoin, ja hän on valmis rikkomaan lakia kostaakseen. Myös yrityksen asiakkaat saattavat kokea saaneensa todella huonoa palvelua ja/tai tuotteita Sonylta.

Tällaisen hyökkäyksen torjuminen kuulostaa yksinkertaiselta: älä suututa ketään tai toimi niin moraalittomasti, että ihmiset vaivautuvat tekemään jotain näin radikaalia. Ongelmaksi muodostuu se, että ihmisten käsitys oikeasta ja väärästä vaihtelee rajusti.

Väärä tieto on myös ongelma: esimerkkinä Stardock-yrityksen skandaali [34; 35]. Eräs yrityksen työtekijä syytti toimitusjohtajaa ahdistelusta. Syytteet olivat perusteettomia, mutta toimitusjohtaja sai silti roppakaupalla tappouhkauksia.

Tällä kertaa kukaan ei ehkä yrittänyt murtautua yrityksen tiedostoihin rangaistusmielessä, mutta ei ole vaikea kuvitella, että jossain vaiheessa jonkun mielenosoitusmurron syy paljastuu tekaistuksi. Ihmisten turhaa ärsyttämistä kannattaa aina välttää, mutta kunniakkainkaan käytös ei anna täydellistä suojaa mielenosoittajailta.

3.4 Muita hakkereita

On olemassa myös muitakin hakkereita. Jotkut hakkerit työskentelevät valtiolle tai armeijalle [27]. He muistuttavat paljon murtovarkaita, mutta heitä on vieläkin vaikeampi viedä oikeuden eteen kuin muita hakkereita. Heidän suhteensa murtovarashakkeriin on sama kuin kaapparin suhde vapaasti ryöstelevään merirosvoon. Vieraat valtiot ovat onneksi harvoin kiinnostuneita varastaman perhevalokuvia, mutta jos pilvipalvelu tarjoaa palvelunsa jollekin valtiolle tai asevoimille, kannattaa varautua vakaviin hyökkäyksiin.

Teollisuusvakoilu on markkinoiden vanha perinne. Arvokkaiden tietojen siirtyessä verkkoon vakoilu livahti sinne myös. Häikäilemättömät yritykset eivät kaihda tällaisen vakoojan käyttöä. [36.] He ovat kutakuinkin murtovarkaan ja valtiolle työskentelevän hakkerin välimaastossa. Osa heistä yrittää jopa fyysisesti soluttautua kohteena olevaan yritykseen. Pilvipalvelun on siis syytä varoa myös läheltä tulevia uhkia.

Verkossa liikkuu myös kyberterroristeja [36]. He ovat läheistä sukua mielenosoittajille. He yrittävät ajaa jonkin uskonnon tai poliittisen ideologian etuja luomalla sekasortoa ja pelkoa. Ero mielenosoittajaan on se, että siinä missä mielenosoittajan päämäärä on yrityksen tai sen johdon rankaiseminen, kyberterroristille se on vain keino saavuttaa hänen oikea tavoitteensa. Heidän lopulliset päämääränsä ovat paljon rajummat, kuten pelonlietsonta ja murha.

3.5 Hakkerit kokonaisuutena

Ihmisillä on monia syitä tehdä tietoturvahyökkäyksiä [26]. Taulukossa 1 on vielä lyhyesti aiemmin käsitellyt hakkerityypit.

Taulukko 1. Hakkerien tyypit, motiivit ja torjuntakeinot.

Hakkerin tyyppi	**Motiivi**	**Torjuntakeino**
Murtovaras	Raha ja rahanarvoiset tiedot	Arvokkaan sisällön säilönnän välttäminen
Kunnian etsijä	Maine, kunnia, arvostus	Maine heikosta tai keskinkertaisesta tietoturvasta
Mielenosoittaja	Kosto, viha	Skandaalien ja epäsuosittujen päätösten välttäminen
Valtion hakkeri	Työ, raha, patriotismi	Valtion tai armeijan työtarjouksista kieltäytyminen
Teollisuusvakooja	Työ, raha	Arvokkaan sisällön säilönnän välttäminen
Kyberterroristi	Uskonto, ideologia, pelonlietsonta	Arvokkaan sisällön säilönnän välttäminen

Kuten taulukosta näkyy, joidenkin hakkerien torjunta on huomattavasti vaikeampaa kuin toisten. Kuitenkaan mikään esitetty keino ei ole pomminvarma. Erityisesti ”arvokas tieto” on todella laaja käsite.

Rikolliset kuitenkin tuppaavat valitsemaan helppoja kohteita [37]. Fyysisessä maailmassa jopa pelkkä auton hälytin saattaa pelottaa rikollisen pois. Tietotekniikassa vastaavia hälyttimiä ei ole, mutta internetin ansiosta kaikki maailman verkkoon kytketyt tietokoneet ovat yhtä lähellä hyökkääjää.

Tästä siis seuraa, että jos jokin pilvipalvelu on liian vaivalloinen murtaa, saattaa roisto valitakin helpomman kohteen, tai jopa jättää koko leikin sikseen. Pilvipalvelun suojausmenetelmien ei siis välttämättä tarvitse olla murtumattomia (se ei ole edes mahdollista) – riittää, että ne ovat tarpeeksi hyviä, ja että palvelun sisältämä data on tarpeeksi arvotonta.

Hyökkäysten ennaltaehkäisyllä on mahdollista vähentää palveluun kohdistuvia hyökkäyksiä, mutta se ei yksin riitä millekään palvelulle. Pieneen maalitauluun tulee varmasti vähemmän osumia kuin suureen, mutta silloin tällöin sekin ottaa osumaa.

4 Hyökkäyksiä ja torjuntakeinoja

Millä tavalla hyökkääjä sitten pääsee käsiksi valvottuihin tietoihin? Tietokoneet ja ohjelmat ovat ihmisten suunnittelemia, joten niissä on aina virheitä. Näiden virheiden avulla hyökkääjä pääsee vaikkapa ohittamaan kirjautumisen.

Osa näistä aukoista on suhteellisen yksinkertaista paikata. Nämä aukot käsitellään seuraavassa luvussa. Tässä luvussa käsitellään hyökkäyksiä, joita voi suorittaa myös hyvin suojattuihin järjestelmiin.

4.1 Fyysinen murto

Miltä tietoturvahyökkäyksen teko näyttää? Monella on varmaankin jokin tämän kaltainen mielikuva: pimeä huone, jota valaisee vain yksinäinen näyttö, mies näytön äärellä. Näytön valo heittää pitkiä, karmivia varjoja miehen kasvoille, ja näytöllä oleva teksti näkyy peilikuvana miehen silmälaseista. Miehen sormet nakuttavat näppäimistöä kuumeisesti. Eipä aikaakaan, kun jokin kaukainen tietokone on täysin miehen vallassa.

Edellinen kuvaus lienee turhan romantisoitu, mutta siinä piilee silti totuuden siemen. Tällaisen hakkerin hyökkäyksiin varautuessa on kuitenkin helppo unohtaa eräs toinenkin mahdollisuus: jotkut hyökkääjät voivat olla murtovarkaita myös sanan tavanomaisessa merkityksessä ja murtautua fyysisesti tietokoneiden ja palvelinten luo. [38; 39.]

Fyysinen murto voi kuulostaa kaukaa haetulta, mutta jos pilvessä on paljon dataa eikä kukaan vartioi palvelinhuonetta, saattaa pilvipalvelun ryöstäminen olla sekä helpompaa että tuottoisampaa kuin vaikkapa myymälävarkaus. Tällöin fyysisen murron kohteeksi joutuminen on vain ajan kysymys.

Toisaalta tällaisia murtoja on tehty jo vuosituhansia, joten nykyään löytyy jo kaikenlaisia konsteja estää fyysinen varkaus. TechRepublic.com antaa kymmenen ohjetta fyysisen turvallisuuden lisäämiseksi. [40.] Tiivistettynä ne ovat:

- Järjestä valvonta yrityksen tiloihin.
- Laita kaikkein haavoittuvimmat laitteet lukittuun huoneeseen.
- Käytä palvelintelineitä.
- Suojaa pöytäkoneet.
- Säilytä kannettavia laitteita ja varmuuskopioita lukkojen takana.
- Poista käytöstä kaikki tavat liittää ulkoisia muistiasemia.
- Suojaa myös tulostimet.

Maailmassa on monia turvallisuusyrityksiä, jotka tarjoavat monia työkaluja murtoja vastaan hälyttimistä vartijoihin. Heihin kannattaa ottaa yhteyttä, jotta näistä fyysisistä murroista päästäisiin kokonaan eroon.

4.2 Sisäinen uhka

Hakkerit pystyvät hyökkäämään mistä vain ja minne vain. Tästä syystä yritykset varautuvat kaukaa tuleviin hyökkäyksiin. Kuitenkin vuonna 2014 yli puolet hyökkäyksistä teki joku, jolla oli lupa käyttää pilvipalvelua [41].

Sisäinen uhka koostuu monista asioista [42]. Tämän vuoksi sisäisen uhkan kitkeminen vaatii monenlaisia tekoja ja toimintatapoja. Teollisuusvakooja mainittiinkin jo aiemmin. Kannattaa siis jo työntekijää palkatessa varmistua, ettei hän etsi työpaikkaa pahat mielessä.

Toisinaan on myös mahdollista, että joku työntekijä suuttuu niin paljon, että hän haluaa kostaa. Näin voi käydä eteenkin, jos yritys alkaa sanoa työntekijöitä irti. Tämän estämiseksi on syytä tehdä kaksi asiaa. Ensiksi kannattaa ottaa varmuuskopioita kaikista tarpeellisista tiedoista, joihin työtekijällä on oikeudet. Toiseksi kannattaa pienentää mahdollisesti tuohtuvan työntekijän oikeuksia ennen tämän suututtamista.

Tuossa tapauksessa kannattaa pitää varansa, sillä jotkut valmistelevat hyökkäyksen ennen lähtöään ja laukaisevat sen vasta irtisanomisen jälkeen [43]. Heidän viimeisimpiä tekojaan pitää siis vahtia erityisen tarkasti.

Jotkut hyökkäykset eivät kuitenkaan toimi ohjelmallisesti. Kostoa janoava entinen työntekijä voi myös yksinkertaisesti muistaa, mitä tietoa palvelussa on liikkunut. Hän voi helposti vuotaa muistamansa jollekin toimittajalle, jolloin se varmasti päätyy uutisiin. Pahimmassa tapauksessa kostaja voi tehdä vahinkoa myös yksinkertaisesti valehtelemalla.

Aina uhka ei ole tarkoituksellinen. Joku pahaa-aavistamaton työntekijä voi vain käyttää samaa salasanaa useassa paikassa, jolloin yhden salasanan vuotaminen avaa hyökkääjälle monta tietä. Joku toinen voi asentaa haittaohjelmia tietämättään. Tässä tapauksessa työntekijät kannattaa vain kouluttaa paremmin.

Toisin kuin tavallisessa yrityksessä pilvipalveluissa sisäinen uhka voi tulla kahdesta suunnasta: palvelun tarjoajalta ja sen käyttäjältä. Kummankin on siis pelattava yhteen tietoturvan säilyttämiseksi. Palvelun tarjoaja ei voi mitenkään tietää, että oikeilla tunnuksilla kirjautuva henkilö aikoo tehdä vahinkoa, ja vastaavasti palvelun käyttäjä ei saa minkäänlaista tietoa siitä, mitä pilvipalvelun työntekijät tekevät. [43.]

Sisäistä uhkaa torjuttaessa kannattaa hyödyntää vähimpien oikeuksien periaatetta [44]. Toisin sanoen, joka käyttäjällä on mahdollisimman vähän oikeuksia tehdä muutoksia. Näin jokaisen tekemän vahingon määräkin on mahdollisimman pieni. Jos jokin työntekijä tarvitsee silloin tällöin valtavia oikeuksia, on syytä harkita niiden antamista tilapäisesti eikä jatkuvasti.

Sisäiselle uhkalle on vielä yksi tekijä: laiskuus. Kaikki eivät vain jaksa käyttää kunnollisia salasanoja tai vaihtaa niitä tarpeeksi usein. Joskus ne varmuuskopiot jäävät tekemättä. Ainoa lääke tähän on joko pakottaa työntekijä tekemään asiat (esimerkiksi lukitsemalla tietokone kunnes hän vaihtaa salasanan) tai tekemällä asioista mahdollisimman vaivatonta (varmuuskopion voi tehdä kuvaketta näpäyttämällä).

4.3 DoS ja DDoS

DoS (Denial of Service) ja DDoS (Distributed Denial of Service) saattavat olla jo tuttuja termejä. Moni protestoija on hyökännyt kohteensa kimppuun juuri näillä tavoilla. Isoimmat hyökkäykset pääsevät monesti jopa otsikkoihin. Tarkastellaan seuraavaksi näiden hyökkäysten toimintaa ja torjuntakeinoja sekä syitä niiden suosioon.

DoS-hyökkäyksessä hyökkääjä lähettää omalta koneeltaan mahdollisimman paljon pyyntöjä, joita hän ei edes yritä käyttää. Jokainen palvelin voi vastata vain rajattuun määrään kutsuja. Jos kutsujen määrä ylittää tämän rajan, alkaa palvelimen toiminta hidastua. Pahimmassa tapauksessa palvelin saattaa jopa kaatua. [45.]

DDoS-hyökkäyksen toimintaperiaate on sama, mutta sen sijaan, että hyökkääjä lähettäisi pyynnöt omalta koneeltaan, hän ottaakin toisten ihmisten omistamia tietokoneita hallintaansa, ja lähettää pyyntöjä niillä. Yleensä tällaisia alistettuja tietokoneita kutsutaan zombitietokoneiksi [45] ja niiden muodostamaa verkkoa botnetiksi [46].

DDoS-hyökkäyksellä on paljon etuja: yhdenkään yksittäisen tietokoneen ei tarvitse olla tehokas. Mitä enemmän tietokoneita hyökkääjä käyttää, sitä tehokkaampi ja vaarallisempi hyökkäys on. Toinen etu on se, että joka tietokoneella on oma IP-osoite. Yhden osoitteen pyyntöjen huomiotta jättäminen paljon helpompaa kuin tuhannen, etenkin kun seassa on paljon oikeaa liikennettä.

DoS-hyökkäys sen sijaan on paljon nopeampi ja helpompi tehdä. Ei ole tarpeen ottaa haltuun lukuisia muiden ihmisten koneita – riittää, että lataa verkosta ilmaisen ohjelman, antaa kohteen osoitteen ohjelmalle ja hyökkäys voi alkaa. Hyökkääjä voi myös maksua vastaan saada hyökkäykseensä mukaan lisää koneita. [46.]

Nykyään on syytä pitää mielessä, että muutkin kuin tietokoneet voivat osallistua hyökkäyksiin. Kaikillahan on virusturva tietokoneessaan, mutta kuinka moni on suojannut matkapuhelimensa ja tablettinsa?

Kohteen kannalta nämä hyökkäykset ovat siinä mielessä lieviä, että ne ainoastaan hidastavat oikeiden asiakkaiden toimintaa. Pahimmassakin tapauksessa ne vain sam-

muttavat palvelun joksikin aikaa. Kaikki palvelussa oleva tieto on ja pysyy tallessa ja koskemattomana, joten tietomurrosta tai vuodosta ei tarvitse huolehtia.

DoS- ja DDoS-hyökkäyksellä ei siis voi varastaa tietoa, mutta palvelun sulkemisellekin on monta syytä, kuten aktivismi, kosto, kilpailijan haittaaminen ja kiristys [46]. Näillä hyökkäyksillä ei kuitenkaan saa arvostusta hakkeripiireissä, sillä jotkut eivät edes pidä näitä hyökkäyksiä hakkerointina [47]. Mainetta näillä kyllä saa, sillä isommat hyökkäykset pääsevät usein otsikoihin, ja nykyään niitä on aina vain helpompi tehdä [48].

Kummankin hyökkäyksen torjuntaperiaate on yksinkertainen: koska hyökkäykset toimivat lähettämällä turhia pyyntöjä, saadaan ne torjuttua hylkäämällä nuo pyynnöt [45]. DoS-hyökkäyksen kanssa tämä on yksinkertaista, mutta DDoS -hyökkäykselle tämä on paljon vaikeampaa. Yksittäisten IP-osoitteiden poistamiseen riittää pelkkä palomuuri.

Palomuuri on kuitenkin varsin pitkällä järjestelmän sisällä, ja hyökkäys voi tukkia järjestelmän jo ennen sitä, jolloin palomuurista ei ole hyötyä. Tällöin torjunta pitää tehdä aikaisemmin. Torjunnan voi hoitaa joko asettamalla reititin lähettämään turhat pyynnöt jonnekin, mistä niistä ei ole haittaa, [45] tai tekemällä sopimus verkkoyhteyden tarjoajan kanssa liikenteen siistimisestä [49].

Viimeinen vaihtoehto on hankkia niin kova palvelinjärjestelmä, että se pystyy vastaamaan myös tekaistuihin pyyntöihin. Tässä on myös se etu, että järjestelmä ei takkuile myöskään tavallisessa kysyntäpiikissä. [49.] Toisaalta järjestelmä, joka pystyy käsittelemään monta kertaa tavallista käyttöä suurempaa määrää pyyntöjä, on kalliimpi kuin järjestelmä, joka pystyy käsittelemään vain tavallista käyttöä vastaavan määrän pyyntöjä. Tämän vaihtoehdon hinta-hyötysuhde ei siis ole kovinkaan hyvä, jos sitä joutuu käyttämään kauan.

DoS- ja DDoS-hyökkäysten täysi torjuminen on todella vaikeaa, ellei lähes mahdotonta. Tämä johtuu vaikeudesta erotella oikeita palvelupyyntöjä vääristä [49]. Hyökkäyksillä on tiettyjä piirteitä, joiden avulla niitä voi havaita. Tässäkin tapauksessa asiantuntijan kannatta tarkistaa liikenne, ettei oikean asiakkaan palvelunpyyntöjä hylätä.

DDoS-hyökkäystä vastaan on myös oma torjuntakeino: hakkerien laitteenvaltausyritysten estäminen Jos kukaan ei anna muuttaa laitettaan zombiksi, ei DDoS-

hyökkäystäkään voi tehdä. Jokaisen on tehtävä oma osansa näiden hyökkäysten estämiseksi. Nykyään laite tarkoittaa pöytäkoneiden ja kannettavien lisäksi myös puhelimia, tabletteja ja jopa älykelloja. Eteenkin jälkimmäisten tietoturva unohtuu usein niiden käyttäjiltä. Edes laitteiden suunnittelijat eivät aina suhtaudu niiden tietoturvaan tarpeeksi vakavasti.

4.4 Verkkourkinta

Verkkourkinta (engl. phising) on huijausyritys [50]. Tyypillinen urkintayritys tehdään lähettämällä kohteelle sähköpostiviesti, jonka esitetään olevan joltain tunnetulta yritykseltä. Viestissä käyttäjää pyydetään seuraamaan viestissä olevaa linkkiä ja kirjautumaan sisään. Kohdetta uhataan jollain rangaistuksella, jos hän ei tottele.

Näistä huijausyrityksistä on useita versioita. Joissain tapauksissa linkki ohjaa valesivustolle, joka esittää olevansa huijausviestissä mainitun yrityksen virallinen sivusto. Kirjautumalla tähän väärään sivustoon kohde antaa kirjautumistietonsa hyökkääjälle.

Linkki voi myös käynnistää jonkin haittaohjelman latauksen. Latauksen jälkeen ohjelma asentaa itsensä käyttäjän koneeseen. Jos kohde lukee viestin HTML-muodossa, voi hyökkääjä käyttää sähköpostiohjelmaa hyväkseen hyökkäyksessä. Viestissä voi esimerkiksi olla kuvia, joiden linkit vievät jonnekin aivan muualle, kuin mitä viesti väittää. [51].

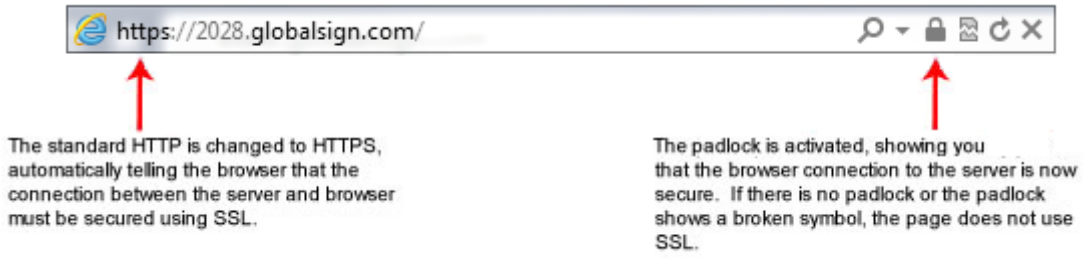
Jotkut hyökkääjät yrittävät hyökätä puhelimitse. Tällöin hyökkääjä esittää korjaavansa kohteen tietokoneen ongelmia tai myyvänsä ohjelmia. Saatuaan kohteen luottamuksen hyökkääjä joko pyytää tämän kirjautumistietoja tai käskee hänen mennä jollekin verkkosuville ja ladata jonkin ohjelman, jonka pitäisi ratkaista ongelma. Todellisuudessa kyseessä on tietenkin haittaohjelma. [52.]

Verkkourkinta ei siis suoraan hyökkää pilvipalvelun kimppuun. Sen sijaan se ottaa kohteekseen joko pilvipalvelun asiakkaan tai, joissain tapauksissa, työntekijän. Fyysisessä maailmassa tätä voisi verrata varkaaseen, joka varastaa kadulla liikkuvalta kohteelta avaimet, joiden avulla hän pääsee vaivatta kohteen taloon.

On erittäin vaikea erottaa hyökkäystä palvelun tavallisesta käytöstä, jos hyökkääjä kirjautuu sisään oikeilla tunnuksilla. Taustalla pyörivä haittaohjelma voi myös aiheuttaa suurta tuhoa.

Paras konsti verkkourkintaa vastaan on tieto niiden toiminnasta. Mitä paremmin palvelun käyttäjät ja ylläpitäjät tietävät huijausyritysten toiminnan, sitä harvemmin he niihin lankeavat.

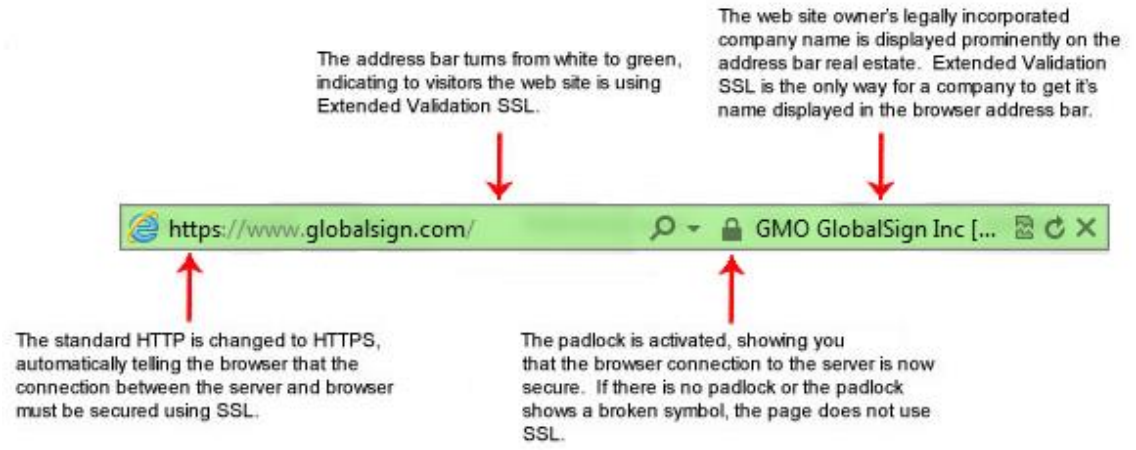
Pilvipalvelun kannattaa myös hankkia SSL-sertifikaatti. Se vaihtaa HTTP-protokollan HTTPS-protokollaksi. Monissa verkkoselaimissa näkyy tällöin suljetun lukon kuva. [53.] Tästä näkyy esimerkki kuvassa 2.



Kuva 2. SSL-sertifikaatin tuntomerkit Internet Explorer -selaimessa [53].

Palvelin on syytä asettaa niin, että se pakottaa HTTP-protokollalla yhteyttä hakevan käyttämään HTTPS-protokollaa. Muuten yhteys toimii yhä HTTP-protokollalla, jolloin sertifikaatista ei ole mitään hyötyä.

Vielä parempi on EV-sertifikaatti. Se laittaa verkkosivun osoitepalkkiin sivuston omistaman yrityksen nimen vihreällä. Huijarit eivät yleensä pysty näitä väärentämään, jolloin huijaussivuston havaitseminen on paljon helpompaa. [53] Esimerkkinä tästä on kuva 3.



Kuva 3. EV-sertifikaatin toiminta Internet Explorer-selaimessa. [53]

Lopuksi pilvipalvelun kannattaa tehdä asiakkaille selväksi sen toiminta. Jos esimerkiksi palvelu ei koskaan pyydä käyttäjätietoja sähköpostissa, tietää käyttäjä kaikkien salasanaa pyytävien sähköpostiviestien olevan huijausyrityksiä. Vastaavilla yhteisillä sopimuksilla huijausyritykset voidaan pysäyttää.

4.5 Haittaohjelmat

Pilvi tuo haittaohjelmille ja niiden luojille lukuisia uusia mahdollisuuksia. Kaikki käyttäjät yrittävät varoa haittaohjelmia, kun he latailevat tiedostoja vierailta sivuilta. Yrityksen omassa pilvessä liikuttaessa ollaan paljon varomattomampia. Miksi huolehtia haittaohjelmista tällaisella yksityisalueella? Eihän kukaan yrityksen työntekijöistä laittaisi tahallaan haittaohjelmia pilveen?

Tässä työssä on jo käsitelty sisäisiä uhkia. On myös mahdollista, että jonkun kirjautumistiedot päätyvät jonkun ulkopuolisen käsiin. Näiden lisäksi joku voi huolimattomuuttaan saada koneelleen haittaohjelman. Kaikissa tapauksissa lopputulos on sama: haittaohjelma siirtyy pilveen ja sitä kautta kaikkien pilveä käyttävien koneille – usein erittäin nopeasti. [54.]

Haittaohjelmat voivat tehdä paljonkin vahinkoa tällä tavalla. Ne voivat varastaa pilven käyttäjien kirjautumistiedot, jolloin hyökkäyksen tekijälle avautuu lukuisia uusia teitä

tehdä hyökkäyksiä. Ne voivat myös yksinkertaisesti kopioida kaikki tietokoneilla olevat tiedot.

Tällainen hyökkäys voi tapahtua asteittain. Ensimmäisellä hyökkäyksellä vain mennään järjestelmään sisälle. Seuraavat hyökkäykset aiheuttavat vahinkoa. Näiden hyökkäysten torjuminen ei auta, jos hyökkääjällä on koko ajan helppo keino päästä takaisin järjestelmän sisälle. On siis tärkeää havaita jo ensimmäinen hyökkäys. [54.]

Tämä voikin olla yllättävän vaikeaa. Pilven sisällä on nimittäin liikennettä ohjelmien ja koneiden välillä, ilman, että järjestelmää käyttävät ihmiset tekevät mitään. [55.] Jos hyökkääjä muokkaa tätä liikennettä, on hyökkäystä erittäin vaikea erottaa tavallisesta liikenteestä.

Haittaohjelmien torjunta pilvipalvelun tarjoajan näkökulmasta on mutkikasta. Moni pilvipalvelu ei tarkastele käyttäjien toimintaa ihan vain liikenteen määrän vuoksi. [56.] Toisaalta käyttäjätkään eivät varmaan halua ulkopuolisten nuuskivan tekojaan.

Haittaohjelmien torjunta jäänee siis enimmäkseen pilvipalvelujen asiakkaiden vastuulle. Tämä ei kuitenkaan tarkoita, että pilvipalvelun kannattaa olla täysin toimeton. Jotkut hyökkääjät yrittävät vallata hylättyjä tilejä. [56.] Nämä tilit voisi vain poistaa. Jos tämä kuulostaa liian ankaralta, voisi pitkään toimettomana olevan tilin käyttö herättää joitain hälytyksiä.

Jos käyttäjät siihen suostuvat, jotkut pilvipalvelut voisivat myös tarkastella palvelun tietoliikennettä yleisesti ja antaa ilmoituksen, jos jotain merkillistä tapahtuu. Ei välttämättä edes jatkuvasti – asiakas voisi pyytää palvelun tarjoajaa tarkastelemaan liikennettä vaikkapa kuukauden verran. Jos liikenne ei vastaa käyttöä, jotain on varmasti pielessä.

Useimmissa tapauksissa haittaohjelmien oletetaan käyvän pilvipalvelun käyttäjän kimppuun. Haittaohjelmat voivat myös saastuttaa palvelun tarjoajan. Jos tavallisen käyttäjän tilin joutuminen hyökkääjän käsiin on vakavaa, niin palvelua ylläpitävän, täydet oikeudet saaneen tilin menetys on valtava katastrofi. Samalla tavalla yhden tiedoston saastuminen haittaa yhtä yritystä, pilven pääohjelman tartunta vahingoittaa kaikkia

pilven käyttäjiä. Pilvipalvelun ylläpitäjän täytyy varoa haittaohjelmia vielä käyttäjiäkin tarkemmin, sillä heihin kohdistuneet hyökkäykset ovat paljon vakavampia.

4.6 Advanced Persistent Threat

Advanced Persistent Threat (APT) on hyökkäys, jossa hyökkääjä pysyy tietoverkossa piilossa pitkään [57]. Sen tarkoitus on yleensä tietojen varastaminen, ei vahingon aiheuttaminen. APT:n tarkat määritelmät vaihtelevat, mutta yleisesti ottaen se eroaa tavallisista hyökkäyksistä seuraavilla tavoilla: [58; 59.]

- Sen toteutus on paljon monimutkaisempi kuin tavallisella hyökkäyksellä.
- Hyökkääjä ei vain varasta tietoja ja karkaa. Hän kerää dataa pitkään ja lähtiessäänkin jättää itselleen jonkin tien sisään uutta hyökkäystä varten.
- Hyökkäyksellä on jokin tietty päämäärä tai kohde. Jos hyökkäyksen tarkoitus on vain tehdä hyökkääjälle rahaa nopeasti, keinolla millä hyvänsä ja kenen tahansa kustannuksella, se ei ole APT.
- Ihminen – tai joukko ihmisiä – ohjaa hyökkäystä. Kohteen ei siis täydy torjua itseään suorittava ohjelma, vaan taitava ja älykäs rikollinen.
- Hyökkäys yrittää vallata kohteen koko verkon, ei vain yksittäistä aluetta, jolla on arvokasta tietoa.
- Hyökkäyksen takana on paljon resursseja. Tällaista hyökkäystä ei yksinäinen hakkeri yleensä pysty tekemään: sen takana on aina jokin järjestö, jolla on kyky sijoittaa resursseja pitkäkestoiseen hyökkäykseen.

APT on monivaiheinen hyökkäys. Vaiheiden tarkoista määristä ja sisällöstä ollaan monta mieltä, [58; 60] kuten myös hyökkäyksen varsinaisista alku- ja loppumisvaiheista, [61; 62] mutta hyökkäyksen pääpiirteistä ja yleisestä toiminnasta ollaan yhtä mieltä.

Hyökkäys alkaa tiedustelulla. Hyökkääjä etsii sopivan kohteen. Aluksi hän varmistaa, että kohteella on jotain tällaisen hyökkäyksen arvoista. Tämän jälkeen hyökkääjä kerää listan kohteen työntekijöistä, mukaan lukien entisistä. Etenkin sellaisista, jotka kantavat kaunaa kohteelle.

Tiedustelu jatkuu tutkimalla kohteen palomuureja ja muita turvakeinoja. Hyökkääjä haluaa löytää niin monta aukkoa kuin mahdollista. Kun tämäkin tiedustelu on tehty, hyökkääjä aloittaa varsinaisen hyökkäyksen.

Tämä hyökkäys on usein pieni, vain yksi pieni haittaohjelma yhdessä koneessa riittää. Hyökkääjä saattaa myös käynnistää vaikkapa DDoS-hyökkäyksen kohteen harhauttamiseksi.

Kohteeseen saadulla haittaohjelmalla on vain yksi tehtävä: auttaa hyökkääjää soluttautumaan syvemmälle järjestelmään. Hyökkääjä monesti asentaa muita vastaavia haittaohjelmia toisiin kohteen laitteisiin. Näin yhden ohjelman löytyminen ja poistaminen ei haittaa hyökkääjää kovinkaan paljon.

Hyökkääjä tutkii kohteen järjestelmää hitaasti ja varovasti. Hän myös tekee koko ajan parhaansa pitääkseen haittaohjelmansa piilossa. Kun hyökkäys on levinnyt tarpeeksi laajalle alueelle, alkaa varsinainen varkaus.

Haittaohjelmat keräävät kaikenlaista dataa, eteenkin kirjautumistunnuksia. Ohjelmat lähettävät datan johonkin turvalliseen paikkaan kohteen oman järjestelmän sisällä. Kun tarpeeksi dataa on kerätty, hyökkääjä yrittää siirtää sen kohteen laitteista omaansa. Tässäkin vaiheessa hyökkääjä voi käyttää DDoS-hyökkäystä harhautuksena.

Hyökkäyksen viimeistelyksi hyökkääjä poistaa asentamansa haittaohjelmat kohteen koneista. Hyökkääjä myös poistaa kaikki todisteet hyökkäyksestä. Usein hyökkääjä jättää kohteeseen jonkin takaoven, jonka avulla hän voi helposti tehdä uuden hyökkäyksen.

APT-hyökkäysten torjuminen on, hyökkäyksen tapaan, monimutkaista. APT:n tärkeä ominaisuus on sen piiloutuminen [59]. Kohteet eivät voi torjua hyökkäystä, jos he eivät tiedä sen olemassa olosta. Miten hyökkäys sitten havaitaan? InfoWorld kertoo kuusi merkkiä käynnissä olevasta hyökkäyksestä: [63]

- Verkostossa tapahtuu tavallista enemmän kirjautumisia öisin.
- Haittaohjelmia löytyy monilta laitteilta.
- Suuret tietomäärät liikkuvat oudolla tavalla.

- Tietokoneista löytyy outoja, monen gigan tietopaketteja
- Laitteista löytyy pass-the-hash – työkaluja.
- Yrityksen johto kohtaa yhden tai useamman verkkourkintayrityksiä.

Viimeinen kohta ei kerro varmuudella, että hyökkäys on käynnissä, mutta mihin tahansa urkintayritykseen on syytä suhtautua vakaavasti. Jos johdon kirjautumistiedot päätyvät vääriin käsiin, voi hyökkääjä tehdä paljon vahinkoa välittömästi.

APT-hyökkäyksellä on eräs toinenkin heikkous: se vaatii komentoja hyökkääjältä toimiakseen. Yhteys hyökkääjään on myös tarpeen, jotta haittaohjelmien keräämä data saadaan ulos kohteen järjestelmästä. [59.] Tästä seuraa kaksi asiaa: ensinnäkin, jos haittaohjelmien yhteys hyökkääjään katkeaa, eivät ohjelmat tee paljoakaan. Toiseksi, jos hyökkäys saadaan pysäytettyä ennen tietojen lähettämistä hyökkääjälle, ei mitään vahinkoa tapahtunut.

APT koostuu usein varsin yksinkertaisista haittaohjelmista. Tällaisen ohjelman torjumiseen tavalliset keinot haittaohjelmien torjumiseen ovat riittäviä. Tällä tavalla hyökkäystä voidaan ainakin hidastaa. [59.]

Sivusto incapsula.com ehdottaa myös seuraavia keinoja APT-hyökkäysten torjumiseksi: [58]

- Valvo verkkoliikennettä.
- Luo valkoiset listat sekä ohjelmille että verkkotunnuksille.
- Anna työntekijöille vain niin paljon käyttöoikeuksia kuin heidän työnsä vaatii.
- Pidä ohjelmat ja järjestelmät päivitettyinä.
- Salaa etäyhteydet.
- Suodata sähköpostit.
- Pidä kirjaa kaikkiin turvallisuuteen liittyvistä tapahtumista.

Jotkut yritykset myös myyvät palveluita näiden hyökkäysten havaitsemiseksi ja torjumiseksi [58; 61]. Ennen tuollaisen palvelun tilaamista kannattaa kuitenkin muistaa, että APT-hyökkäykset kohdistuvat tiettyihin palveluihin useammin kuin toisiin [64]. Jos siis

ei kuulu riskiryhmiin, ei välttämättä kannata hankkia mitään kallista palvelua, ellei se torju muitakin hyökkäyksiä.

5 Heikkoudet ja niiden poistaminen

Aina hyökkääjän ei ole tarpeen keksiä mitään ovelaa temppua päästäkseen varastamaan tai tekemään vahinkoa. Toisinaan hänen kohteensa suojaukset ovat niin heikot, että sisään pääsemiseen riittää vain yksinkertainen kokeilu. Jos haluaa murtautua taloon, ei lukkoa tarvitse tiirikoida tai avainta varastaa, jos asukas on jättänyt oven lukitsematta.

Vielä nykyäänkin niin palvelut kuin käyttäjät tekevät kaikenlaisia virheitä, joiden ansiosta hyökkääjän työ on liiankin helppoa. Useimmat näistä johtuvat laiskuudesta, ajattelemattomuudesta tai tietämättömyydestä.

Pilvipalvelun käyttäjä voi parantaa monien palvelujen turvallisuutta salaamalla tietonsa ennen niiden tallentamista pilveen. Tällä tavalla datasta ei ole hyökkääjälle mitään hyötyä, vaikka hän saisikin varastettua sen. Hyökkääjä todennäköisesti yrittää murtaa salatun datan, mutta tämä ainakin hidastaa häntä.

5.1 Heikko autentikointi

Keeper Security tutki 10 miljoonaa vuonna 2016 vuotanutta salasanaa. 25 suosituinta salasanaa kattaa yli puolet näistä vuotaneista salasanoista. 17 % tileistä käyttää salasanaa ”123456”. Suosituimmissa salasanoissa ei ollut tapahtunut suura muutoksia. [65.] Tutkimuksen kymmenen yleisintä salasanaa ovat seuraavat:

- 123456
- 123456789
- qwerty
- 12345678
- 111111

- 1234567890
- 1234567
- password
- 123123
- 987654321.

Suomalaisten suosituimmat salasanat ovat hieman erilaisia. Tämä lista oli luotu vuonna 2011. Jos kuitenkaan maailmalla suosituimmat salasanat eivät ole muuttuneet, ovat suomalaisten salasanasuosikitkin todennäköisesti pysyneet ennallaan. [66.] Viisi suomalaisten suosituinta salasanaa ovat seuraavat:

- salasana
- aurinko
- 123456
- perkele
- johanna.

Yleisimpiä salasanoja ei edes tarvitse murtaa – ne ovat niin tavallisia, että hyökkääjä voi vain kokeilla eri salasanoja palvelun sisäänkirjautumissivulla. Varsinaiset salasananmurto-ohjelmat murtavat myös nämä yleiset salasanat jo muutamassa sekunnissa.

Yleensä salasanan murtaminen tapahtuu sanakirjan avulla. Sanakirja voi tässä tapauksessa tarkoittaa oikean sanakirjan lisäksi listaa yleisimmistä salasanoista. Kehittyneemmät sanakirjat osaavat myös muunnella sanoja: password, Password, password1 jne. Juuri tämän vuoksi edellä mainittuja salasanoja kannattaa välttää: jos salasana tai pieni muunnelma siitä löytyy noin lyhyestä listasta, voi hyökkääjä murtaa sen lähes välittömästi. [67.]

Jos hyökkääjä ei löydä salasanaa sanakirjan avulla, hän yrittää murtaa sen raa’alla laskentateholla, eli kokeilemalla kaikkia mahdollisia kirjain-, numero- ja merkkiyhdistelmiä. Tämä vie kuukausia, jopa vuosia.

Heikoista salasanoista on helppo syyttää loppukäyttäjää [67]. Toisaalta voisi kysyä, miksi verkkosivut ja palvelimet sallivat näin heikkojen salasanojen käytön. Vahvojen salasanojen tärkeys on varmasti asia, jonka sivun tai palvelun ylläpitäjät tietävät.

Mikä tahansa kirjautumista vaativa palvelu voi siis käyttää salasanojen murtautumismenetelmiä hyväkseen ja pakottaa käyttäjiä miettimään salasanaansa edes hieman enemmän. Palvelu voisi vaikka aloittaa yhdistämällä sekä tavallisen sanakirjan että suosittujen salasanojen listan salasanan muutosprosessiin. Jo tämä vaikeuttaisi salasanojen murtamista huomattavasti.

Moni sivusto määrittää salasanan pituudeksi kuusi merkkiä, mutta sen nostaminen kahdeksaan tai kymmeneen auttaisi huomattavasti [67]. Nykyään tosin kymmenenkin merkkiä on aika vähän, joten vieläkin pidempi salasana olisi suositeltava. Lisäksi kannattaa vaatia ainakin yhtä pientä kirjainta, isoa kirjainta, numeroa ja muuta merkkiä. Eritoten muut merkit ovat tärkeitä, sillä ne vaikeuttavat sateenkaaritauluja käyttäviä murtoyrityksiä. Mitä enemmän merkkejä salasanassa voi olla, sitä pidempään salasanan murtaminen vaatii.

Nykyään on myös tarjolla kaksivaiheinen autentikointi: kirjautumistunnusten antamisen jälkeen palvelu lähettää käyttäjälle vielä teksti- tai sähköpostiviestin, jonka avulla käyttäjä viimeistelee sisään kirjautumisen. Vaikka hyökkääjä saisikin salasanan selville, ei siitä ole hänelle mitään hyötyä, jos hän ei pääse myös käsiksi kyseiseen viestiin.[67; 68.]

Jotkin palvelut, kuten Valve Corporationin Steam, ovat ottaneet käyttöön erään toisen suojaustavan: käyttäjänimen piilottamisen. Steam-palvelun tileillä on sekä tilin nimi että yhteisönimi. Näistä ensimmäistä käytetään ainoastaan sisään kirjautumisessa, eikä se näy muille. Jälkimmäinen näkyy muille käyttäjille. Näillä nimillä ei tarvitse olla mitään yhteistä toistensa kanssa, joten jos hyökkääjä haluaa selvittää ”Matti”-nimisen käyttäjän salasanan, on hänen ensin selvitettävä tämän tilin nimi. [69.]

Salasanojen suojaus

Jokainen sisään kirjautumista vaativa palvelu säilyttää käyttäjien käyttäjänimiä ja salasanoja jonkinlaisessa tietokannassa. Kun joku yrittää kirjautua sisään, palvelu vertaa

käyttäjän antamia tunnuksia tietokannassa oleviin tunnuksiin. Jos tunnukset löytyvät tietokannasta, pääsee käyttäjä sisään. Jos niitä ei löydy, sisään kirjautuminen epäonnistuu. [70.]

Yksinkertaisin tapa säilyttää näitä tietoja on tavallinen teksti. Toisin sanoen, jos käyttäjän salasana on ”password”, lukee myös tietokannassa ”password”. [70; 71.]

Hyökkääjän on kuitenkin yllättävän helppoa saada tämä tietokanta käsiinsä, sillä siihen riittää pelkkä lukuoikeus. Jos tietokanta päätyy hyökkääjän käsiin, pystyy hän yksinkertaisesti lukemaan jokaisen palvelun käyttäjän kirjautumistunnukset. Näin hän pystyy valtaamaan jokaisen tilin.

Tämä käyttäjien tietoja säilyttävä tietokanta pitää siis jollain tavalla muuttaa sellaiseksi, että hyökkääjä ei pysty sitä lukemaan. Yksi ratkaisu tähän on salaus (engl. encryption). Salaustekniikkoja on monenlaisia, mutta niiden toimintaperiaate on sama: salattava merkkijono muunnetaan jonkin avaimen (engl. key) avulla lukukelvottomaksi. Avaimen avulla salattu teksti voidaan myös muuttaa luettavaksi. Tässä yhteydessä avain tarkoittaa mitä tahansa tietoa, jonka avulla salaus suoritetaan. Avain voi siis merkkijonon lisäksi olla ohje. [72.]

Salaus on kuitenkin huono tapa suojata salasanoja, sillä jos avain päätyy hyökkääjän käsiin, voi hän purkaa koko salasanalistan todella nopeasti. Vaikka avainta säilytettäisiin kokonaan toisella palvelimella kuin salasanoja, on hyökkääjän aivan yhtä helppoa saada se käsiinsä kuin salasanalistankin. [71.]

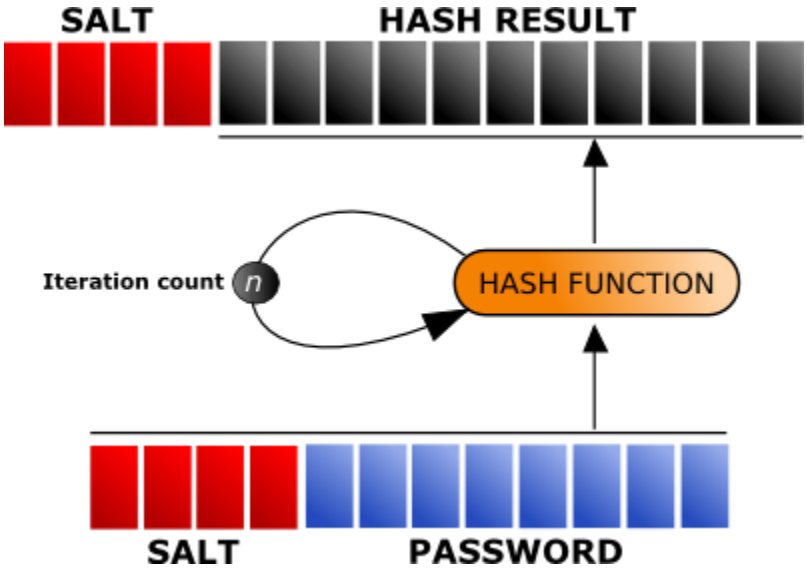
Salasanoja ei siis kannata salata; niistä kannattaa tehdä tiiviste (engl. hash). Tiivistettä ei saa sekoittaa pakkaukseen (engl. data compression). Tiiviste muodostuu sekoittamalla syötettä tiivistealgoritmin määräämällä tavalla, jolloin siitä tulee lukukelvoton tiiviste. Toisin kuin salattua tekstiä, tiivistettä ei voi purkaa millään tavalla. Tiivisteen avulla ei voi päätellä mitään alkuperäisestä tekstistä. Käyttäjän syöttämää salasanaa verrataan tähän tietokannassa olevaan tiivisteeseen yksinkertaisesti luomalla tiiviste käyttäjän syötteestä ja vertaamalla tätä tiivistettä tietokantaan. Sama syöte antaa aina saman tiivisteen. [70; 71.]

Myös tiivisteissä on ongelma: koska sama teksti tuottaa aina saman tiivisteen, voi hyökkääjä luoda itsellensä listan tiivisteistä (tai ladata valmiin listan verkosta) ja katsoa, löytyykö salasanalistasta samoja tiivisteitä. Tällaista tiivistetaulua kutsutaan sateenkaaritauluksi (engl. rainbow table). Jos tiiviste löytyy, tietää hyökkääjä salasanan olevan se merkkijono, joka loi kyseisen tiivisteen. [73.]

Ratkaisu tähän on suola (engl. salt). Suola tarkoittaa merkkijonoa, joka liitetään yleensä salasanan alkuun. Tiiviste luodaan salasanan ja suolan yhdistelmästä. Suola kannattaa luoda satunnaisesti. Eri käyttäjillä pitää olla eri suola. Näin kaikkien käyttäjien salasana tiiviste on erilainen, vaikka käyttäjillä olisi sama salasana. Tiivisteitä ei myöskään löydy mistään sateenkaaritauluista, sillä suolattu salasana on yksinkertaisesti liian pitkä.[70; 71.]

Eri lähteet suosittelevat eri pituuksia suolalle. Naked Security ehdottaa 16 merkkiä suolan vähimmäispituudeksi, mutta sivusto sanoo myös, että suolaa voi säilyttää salasanatietokannassa sellaisenaan [71]. Jasypt taas sanoo kahdeksan merkin riittävän, mutta sivusto kehottaa myös pitämään suolan salassa [74]. Salasanakannan vuotaminen on kuitenkin niin vakava asia, että pitkä suola salasanakannassa on parempi vaihtoehto kuin lyhyt suola jossain piilossa.

Ikävä kyllä tietokoneet ovat nykyään niin nopeita, että jopa suolattu salasana voidaan murtaa, vaikka siinä kestääkin kauan [70]. Tähän on onneksi yksinkertainen ratkaisu: syötä tiiviste uudestaan tiivistealgoritmiin. Toista tätä vaikkapa 1 000 tai 10 000 kertaa, niin hyökkääjän on erittäin vaikea murtaa salasanaa. Tämä hidastaa sisään kirjautumista hieman, ehkä sekunnin verran, mutta jos hyökkääjä joutuu kuluttamaan sekunnin jokaiseen murtoyritykseen, hidastuu hyökkäys niin paljon, ettei se ole enää kannattavaa. [74.] Kuvassa 4 näkyy tiivistelmä tästä toiminnosta.



Kuva 4. Salasanan ensin suolataan, sitten suolatusta salasanasta tehdään tiiviste. Tiivisteestä tehdään uusi tiiviste n kertaa, ja viimeinen tiiviste tallennetaan tietokantaan suolan kanssa. [74.]

Tällaiseen toistuvaan tiivisteen luontiin on olemassa omia algoritmeja. Naked Security suosittelee PBKDF2-algoritmia, Lifehacker taas bcrypt-algoritmia [70; 71]. Jälkimmäinen suosittelee yleensäkin hitaampia algoritmeja kuin yleisiä MD5-, SHA-1 tai SHA-256-algoritmeja. Nopea algoritmi on monissa tilanteissa parempi, mutta tiivistämisessä hitaampi algoritmi on turvallisempi, sillä mitä hitaammin algoritmi toimii, sitä hitaammin hyökkääjä voi käydä mahdollisia salasanoja läpi [70]. Nykyään eteenkin MD5- ja SHA-1-algoritmeja pidetään turvattomina [75].

Jasypt tarjoaa myös muita huomioita salasanan tallentamisesta. Kaikki syötteet kannattaa kääntää samaan muotoon, sillä muuten erikoisemmat merkit salasanassa saattavat kääntyä bittimuotoon eri tavalla, jos käyttäjä kirjautuu sisään eri laitteelta. Tiivistealgoritmin antama tiiviste voi myös sisältää outoja merkkejä, joten sekin pitää muuntaa jonkinlaiseksi merkkijonoksi. Sivusto suosittelee ensimmäiseen UTF-8-koodausta, jälkimmäiseen BASE64-koodausta. [74.]

Lyhyesti, salasana kannattaa tallentaa ja tarkistaa seuraavalla tavalla:

- Muunna sisään kirjautumista yrittävän antama salasana johonkin vakiomuotoon, kuten UTF-8.
- Lisää salasanaan käyttäjäkohtainen suola.

- Luo suolatusta salasanasta tiiviste jollain hitaalla tiivistealgoritmilla.
- Luo tiivisteestä uusi tiiviste. Toista tätä monta kertaa, tai mieluummin käytä jotain algoritmia tähän.
- Koodaa tiiviste joksikin luettavaksi merkkijonoksi, esimerkiksi BASE64-algoritmilla.
- Tallenna koodattu tiiviste, tai vertaa näin saatua tiivistettä tallennettuun tiivisteeseen.

5.2 Pilvipalvelujen väärinkäyttö

Kuten johdannossa jo todettiin, pilvipalvelut ovat niin hyödyllisiä, että moni yritys on kiinnostunut niistä hyvästä syystä. Pilvipalvelut ovat itse asiassa niin hyviä, että jopa hyökkääjät käyttävät niitä pahoihin tarkoituksiinsa. Pilvipalvelu voi olla hyökkääjälle kohteen lisäksi työkalu.

Aiemmassa alaluvussa kerrottiin, että jotkut hyökkääjät yrittävät murtaa salasanoja pelkällä laskentateholla. Sitä saa pilvestä. Jos hyökkääjä kerää paljon dataa laittomasti, hän voi tallentaa sen ainakin tilapäisesti pilveen. Pilvi on myös oiva paikka säilöä kunnollisten ohjelmien lisäksi haittaohjelmia. On varmasti erittäin noloa, jos pilvipalveluun kohdistunut hyökkäys tehtiin saman pilvipalvelun avulla.

Moni pilvipalvelu tarjoaa käyttäjille ilmaisia kokeiluja [76]. Nämä vaativat usein pelkän sähköpostiosoitteen, joita hyökkääjän on helppo hankkia roppakaupalla. Jotkut palvelut vaativat tekstiviestin tai luottokortin myös kokeiluun, mutta näidenkin massakäyttö on varsin yksinkertaista määrätietoiselle hyökkääjälle. Hyökkääjät ovat tottuneita käyttämään uusinata teknologiaa pahoihin tekoihinsa. [77.]

Ilmaiset kokeilut ovat yhä suosittuja, sillä ne tuovat lisää käyttäjiä, joista osa siirtyy jossain vaiheessa käyttämään maksullista versiota. Ne tuskin tulevat koskaan täysin poistumaan. Moni hyökkääjä on varmasti valmis maksamaan reilun summan rahaa hyvästä pilvipalvelusta, joten kokeiluversioiden poistaminen ei varmasti estä kaikkea pilvipalveluiden väärinkäyttöä.

Pilvipalveluiden väärinkäyttöä voi olla vaikea havaita, sillä tyypillisesti pilvessä liikkuu niin paljon dataa, että väärinkäyttö yksinkertaisesti hukkuu tavallisen liikenteen sekaan

[76]. Tietysti palvelun tarjoaja voi vain skannata, mitä dataa palvelussa tarkkaan ottaen liikkuu, mutta palvelun käyttäjät eivät välttämättä arvosta tällaisia pistokokeita. Jokainen käyttäjä väittää käyttävänsä pilvipalvelua vain laillisiin töihin, oli se totta tai ei.

Vaihtoehtoisesti pilvipalvelu voisi vaatia enemmän tietoa palvelun rekisteröinnin yhteydessä. Ei enää nimettömiä tilejä, joka käyttäjän on pystyttävä todistamaan henkilöllisyytensä. [78.] Hankala rekisteröinti ilman muuta rajoittaa palvelua käyttävien määrää, mutta hyvät turvatoimet voivat lisätä niitä.

Pilvipalvelujen väärinkäytön estäminen on siis yllättävän vaikeaa. Pilvipalvelun tarjoajan pitää siis tehdä asiakkailleen selväksi, miksi he tekevät palvelunsa käytöstä näin hankalaa. Hyvien ideoiden väärinkäyttö on hyökkääjille jo tuttua toimintaa.

5.3 Turvaton API

Moni pilvi tarjoaa nykyään käyttäjilleen ohjelmointirajapinnan (Application Programming Interface), jonka avulla käyttäjä voi hyödyntää pilven palveluita ohjelmallisesti [79]. Käyttäjä voi esimerkiksi hallita useaa pilveä samanaikaisesti pilvien API:en avulla.

Tässä ei periaatteessa ole mitään ongelmaa, mutta jotkut API:n suunnittelijat eivät tule ajatelleeksi, miten API tarjoaa uusia työkaluja myös hyökkääjälle. Tästä esimerkkinä on sisäänkirjautuminen: jotta pilven palveluja voi käyttää, pitää käyttäjän jollain tavalla kertoa pilvelle, kuka hän on. Tämä tapahtuu kirjautumistunnusten avulla.

Kirjautumistunnukset voivat siis usein liikkua API:en välityksellä. Jos API ei kuitenkaan salaa siinä kulkevaa tietoa, voi hyökkääjä vain varastaa API:n lähettämän datapaketin ja kopioida siinä lukevat kirjautumistunnukset. [79.] Nyt hyökkääjä pääsee helposti aiheuttamaan paljon vahinkoa käyttäjän nimissä, vaikka käyttäjä ei mitään väärää tehnytkään.

Jos käyttäjä suunnittelee pilvipalveluun API:n, täytyy pitää mielessä datan liikunta. Kaikki data on syytä salata, jotta hyökkääjä ei voi varastaa tai muutella sitä. Tähän sopii salausavain. Jokainen pilveä käyttävä organisaatio tarvitsee oman avaimen.

API:n käytön autentikointi on myös syytä tehdä hyvin. Tähän sopii esimerkiksi TLS-autentikointi (Transport Layer Security) tai SAML-autentikointi (Security Assertion Markup Language). [80] Kannattaa myös tarkkailla API:ssä liikkuvaa dataa. Jos liikenteessä tapahtuu yllättäviä piikkejä tai API:tä käytetään outoon aikaan, syynä voi hyvinkin olla hyökkäys tai yritys tutkia kohdetta ennen hyökkäystä.

API:t voivat myös estää tai sallia tiettyjä IP-osoitteita [80]. Pilvipalvelu voisi siis oletuksena estää API:n käytön kaikilta. Käyttäjä voi sitten tarpeen mukaan pyytää käyttölupaa API:hin, jolloin pilvipalvelu sallii asiakkaan määräämien IP-osoitteiden käyttää palvelun API:a. Vastaavasti pilvipalvelu voi myös estää ongelmia aiheuttaneita IP-osoitteita käyttämästä API:tä.

Nykyään käyttäjiä suositellaan välttämään sellaisia API:tä, joiden dokumentointi ei ole sekä julkista että kattavaa. Pilvipalvelun pitää siis sekä luoda että julkaista API:nsä dokumentointi. Niin kehittäjät kuin käyttäjät pystyvät näin helposti tarkistamaan API:n toimivuuden ja turvallisuuden. Jos API ei kestä tällaista tarkastelua, ei se ole kovinkaan hyvä API. [81.]

API:tä tehdessä kannattaa muistaa, että API itsessään ei ole ainoa heikkous. Myös huono käyttöönotto voi avata uusia teitä hyökkääjälle. [81.] Pilvipalvelun pitää siis kertoa API:n toiminnan lisäksi sen oikeaoppinen käyttö. Parasta olisi tietysti tehdä API:stä helppokäyttöinen, jotta virheitä ja vahinkoja ei pääse tapahtumaan.

Stormpath suosittelee myös API-avaimen käyttöä [82]. API-avain on salainen merkkijono, jolla käyttäjä voi todistaa henkilöllisyytensä API:lle [83]. Koska API-avain on tallennettuna tiedostoon, API voi lukea sen sieltä, jolloin käyttäjän ei tarvitse edes tietää sitä. Avaimen vaihto on myös paljon helpompaa kuin salasana vaihto. Lisäksi, jos avain päätyy hyökkääjälle, ei käyttäjän tarvitse tehdä tililleen mitään, riittää, että pilvipalvelu poistaa kyseisen avaimen käytöstä. [82.]

5.4 Jaettu teknologia

Pilvien toimintaperiaate on, että palvelun tarjoaja antaa asiakkaidensa käyttää omia resurssejaan, kuten tallennustilaa ja suorituskykyä. Fyysistä laitteistoa, kuten välimuis-

tia, [84] on kuitenkin harvoin suunniteltu tällä tavalla jaettavaksi. Hypervisor ratkaisee monia tähän liittyviä ongelmia, mutta nekään eivät ole täydellisiä: joskus ne antavat käyttäjälle tarpeettoman paljon oikeuksia [85].

Tavallisen käyttäjän kanssa tämä ei ole ongelma. Käyttäjä vain saa luvan tehdä asioita, joita hän ei edes halua tehdä. Jos käyttäjällä on kuitenkin pahat mielessä, voi hän näillä tarpeettomilla oikeuksilla vaikuttaa muihin pilven osiin – myös niihin, joihin hänellä ei pitäisi olla lupaa vaikuttaa!

Hyökkääjällä on monia keinoja päästä käsiksi toisille käyttäjille tarkoitettuihin resursseihin. Huonosti säädetty hypervisor voi sallia käyttäjän suorittaa koodia hypervisorin oikeuksilla, jolloin koodi voi vaikuttaa sekä kaikkiin pilven käyttäjiin että pilveen itseensä. [86.]

Vastaavasti, jotkin rootkitit antavat hyökkääjän muokata hypervisorin järjestelmäkutsuja, jolloin hyökkääjä voi siis korvata hypervisorin käskyt omillaan. Joskus hyökkääjä voi myös paeta virtuaalikoneesta kokonaan. Tällöin hän saa rajoittamattomat oikeudet kaikkiin jaossa oleviin resursseihin.

Tähän ongelmaan on onneksi useampia ratkaisuja. Hypervisor voidaan asettaa havaitsemaan suuri resurssien kulutus [86]. Tämä suojaa myös joiltain DoS-hyökkäyksiltä. Pilvipalvelun tarjoajan kannattaa myös jakaa resurssinsa selkeisiin osiin [84]. Jos esimerkiksi joka käyttäjällä on oma prosessori ja välimuisti, on heidän paljon vaikeampi tarkastella toistensa tietoja kuin jos he jakaisivat ne.

Monien muiden ongelmien tavoin näihinkin ongelmiin auttaa valvonta. Jos pilveen tai hypervisoriin tulee odottamattomia muutoksia, on syytä epäillä hyökkäystä. Hypervisor kannattaa myös asettaa antamaan asiakkaille niin vähän resursseja kuin asiakkaan tehtävän suorittaminen vaatii. [85.] Mitä vähemmän oikeuksia käyttäjällä on, sitä vaikeampaa vahingon tekeminen on.

Pilvipalvelun tarjoajan kannattaa myös aika ajoin tarkastella omaa palveluaan haavoittuvuuksien varalta – nämä tarkastukset yleensä mainitaan palvelutasosopimuksessa [84; 85]. Jos palvelun tarjoajien tai käyttäjien on tarpeen tehdä suurempia muutoksia palveluun, olisi syytä vaatia vahvempaa autentikointia kuin tavallisessa käytössä. Näitä

muutoksia tuskin tarvitsee tehdä kovin usein, joten tavallisten tilien ei tarvitse pystyä tekemään niitä.

Vaikka jaettu teknologia on enimmäkseen IaaS-palvelujen ongelma, [84] on muunkin tyyppisten pilvipalvelujen otettava huomioon jaetun teknologian ongelmat. Kaikki pilven käyttäjät käyttävät samoja laitteita ja ohjelmia. Jos yksikin osa on haavoittuvainen, voi hyökkääjä vaikuttaa kaikkiin pilven käyttäjiin. Kaikkien pilvipalvelujen täytyy siis pitää mielessä pilven resurssien jako. InfoWorld suosittelee tähän mm. verkon jakamista osiin, verkon tarkkailua ja mahdollisimman pienten oikeuksien antamista käyttäjille. [87.]

6 Yhteenveto

Tässä työssä tarkasteltiin erilaisia keinoja suojata pilvipalveluja kaikenlaisilta hyökkäyksiltä. Työssä käytiin läpi niin tyypillisimpiä pilvipalveluiden heikkouksia, erilaisia hyökkäyksiä ja niiden torjuntamenetelmiä sekä itse hyökkääjiä. Hyökkääjien suhteen phdittiin heidän motiivejaan sekä keinoja luoda sellainen pilvipalvelu, johon mahdollisimman harva haluaa hyökätä. Tämän lisäksi mietittiin keinoja tehdä pilvipalvelusta sellainen, jonka suojauksia on mahdollisimman vaikea murtaa.

Ikävä kyllä palvelu, johon kukaan ei halua hyökätä paljastui samanlaiseksi unelmaksi kuin palvelu, jonka puolustuksia ei voi murtaa. Hyökkääjillä on monia syitä rikkoa lakia, kenties tärkeimpänä se, että sekä kiinni jääminen että rangaistuksi tuleminen ovat valitettavan harvinaisia tapauksia. Samaten keinot yhden hyökkääjän torjumiseksi saattavat vain innostaa toisia: rahan perässä juokseva hyökkääjä voi vaihtaa hyvin suojatun kohteen helpompaan, kun taas mainetta hamuava vain innostuu moisesta. Jopa pelkkien rahaa haluavien hyökkääjien torjuminen on vaikeaa, sillä nykyään arvokkaan tiedon määritelmä on niin laaja.

Hyökkääjien tarkastelu ei kuitenkaan ollut täysin hyödytöntä. Mistään pilvipalvelusta ei ehkä saa sellaista, johon kukaan ei halua hyökätä, mutta tietyillä toimilla hyökkäyksien määrää voi kuitenkin vähentää. Koska arvokas data on nykyään hyvin laaja käsite, ei yhdenkään palvelun kannata väittää huonojen turvatoimien johtuvan siitä, että palvelussa ei ole mitään arvokasta.

Hyökkäysten tarkasteleminen sen sijaan oli huomattavasti palkitsevampaa. Moni saattaa ajatella, että tietomurto tapahtuu ainoastaan verkon välityksellä, mutta yllättävän usein hyökkäyksessä on takana jokin fyysinen osa, kuten pahaa tarkoittava työntekijä. Tietoturvasta on huolehdittava kaikkialla, ei vain verkossa.

Hyökkäyksiä tarkastelemalla sain myös selville, että ne jättävät monesti joitain merkkejä ennen vahingon tapahtumista. Tässä paljastuu pilven valvonnan tärkeys: jos pilvessä tapahtuu kummallisia asioita, on syynä mahdollisesti hyökkäys.

Pilvipalvelujen tyypillisten heikkouksien tarkasteleminen oli myös hyödyllistä. Hyökkääjän ei tarvitse tehdä mitään monimutkaisia temppuja päästäkseen sisään, jos pilvi on huonosti suojattu. Kun heikkoudet ovat tiedossa, on paljon helpompaa paikata ne. Heikkouksien poistaminen on usein varsin yksinkertaista.

On myös syytä korostaa, että tietoturvan ylläpitäminen kuuluu yhtä lailla niin pilvipalvelun tarjoajalle kuin sen käyttäjälle. Vaikka pilvellä olisi miten hyvät turvatoimet, jos käyttäjä antaa kirjautumistunnuksensa hyökkääjälle, ovat kaikki nuo toimet täysin hyödyttömiä. Vastaavasti asiakas voi valvoa omaa osaansa pilvestä hyvinkin tarkasti, mutta jos palvelun tarjoajan turvatoimet ovat huonot, pääsee hyökkääjä kiertämään asiakkaan valvonnan.

Työ saavutti jossain määrin tavoitteensa: yleisimmät hyökkäykset ja heikkoudet käytiin läpi. Työ tarkasteli myös tapoja pitää pilvessä olevat tiedot turvassa, niin sen tarjoajan kuin sen asiakkaiden näkökulmasta. Hyökkääjät eivät kuitenkaan ole lopettaneet työtään, ja teknologian jatkuvasti kehittyessä he keksivät varmasti uusia keinoja kiertää parhaatkin turvatoimet. Pilvipalvelujen asiakkaiden ja tarjoajien on siis syytä pysyä jatkuvasti valppaina uusien hyökkäysten ja uusien hyökkäystapojen varalta.

Lähteet

1 The transformative impact of cloud adoption. Verkkodokumentti. Saatavissa: https://www.skyhighnetworks.com/cloud-computing-trends-2016/ Luettu viimeksi 2.3.2017.

2 UrbaaniSanakijra.com: pilvipalvelu. Verkkodokumentti. Saatavissa: https://www.urbaanisanakirja.com/word/pilvipalvelu/ Luettu viimeksi 2.3.2017.

3 Pilvipalveluiden määritelmä. Verkkodokumentti. Saatavissa: http://fi.laovirtualisointi.wikia.com/wiki/Pilvipalveluiden_määritelmä Luettu viimeksi 2.3.2017.

4 Mikä on pilvipalvelun määritelmä? Verkkodokumentti. Saatavissa: http://www.tietohallintopalvelu.fi/2015/11/25/mika-on-pilvipalvelun-maaritelma/ Luettu viimeksi 2.3.2017.

5 Viisi isoa kysymystä pilvipalveluista. Verkkodokumentti. Saatavissa: http://www.webopas.net/pilvipalvelu.html Luettu viimeksi 2.3.2017.

6 Software, Platform, Infrastructure Model (SPI Model) Verkkodokumentti. Saatavissa: https://www.techopedia.com/definition/14019/software-platform-infrastructure-model-spi-model Luettu viimeksi 14.3.2017.

7 What is SPI (SaaS, PaaS, IaaS)? Verkkodokumentti. Saatavissa: http://searchcloudcomputing.techtarget.com/definition/SPI-model Luettu viimeksi 14.3.2017.

8 Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS. Verkkodokumentti. Saatavissa: https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/ Luettu viimeksi 14.3.2017.

9 Types of Cloud Computing. Verkkodokumentti. Saatavissa: https://aws.amazon.com/types-of-cloud-computing/ Luettu viimeksi 14.3.2017.

10 Cloud Computing – Types of Cloud. Verkkodokumentti. Saatavissa: http://www.globaldots.com/cloud-computing-types-of-cloud/ Luettu viimeksi 14.3.2017.

11 Types Of Services Offered By Cloud Systems. Verkkodokumentti. Saatavissa: https://www.esds.co.in/blog/types-of-services-offered-by-cloud-systems/ Luettu viimeksi 14.3.2017.

12 XaaS (anything as a service). Verkkodokumentti. Saatavissa: http://searchcloudcomputing.techtarget.com/definition/XaaS-anything-as-a-service Luettu viimeksi 14.3.2017.

13 TEPA – Sanastokeskus TSK:n termipankki : tietoturva. Verkkodokumentti. Saatavissa: http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=161&qfind=tietoturva Luettu viimeksi 2.3.2017.

14 Tietoturva. Verkkodokumentti. Saatavissa: http://www.internetopas.com/yleistietoa/tietoturva/ Luettu viimeksi 2.3.2017.

15 Tietoturvan perusteet. Verkkodokumentti. Saatavissa: https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf Luettu viimeksi 2.3.2017.

16 Työpaikan tietoturvakoulutuksen suunnittelu, järjestäminen ja koulutusmateriaalin luonti. Verkkodokumentti. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/8099/Poutanen.Pekka.pdf?sequence=2 Luettu viimeksi 2.3.2017.

17 VAHTI 8/2008 Valtionhallinnon tietoturvasanasto: Määritelmät H. Verkkodokumentti. Saatavissa: https://www.vahtiohje.fi/web/guest/maaritelmat-h Luettu viimeksi 2.3.2017.

18 Definition of a Security Vulnerability. Verkkodokumentti. Saatavissa: https://msdn.microsoft.com/en-us/library/cc751383.aspx Luettu viimeksi 2.3.2017.

19 Vulnerability. Verkkodokumentti. Saatavissa: https://www.techopedia.com/definition/13484/vulnerability Luettu viimeksi 2.3.2017.

20 Microsoft blames Russia for cyber-attacks exploiting Windows security flaw. Verkkodokumentti. Saatavissa: https://eandt.theiet.org/content/articles/2016/11/microsoft-blame-russian-government-for-cyber-attacks-exploiting-windows-security-flaw/ Luettu viimeksi 2.3.2017.

21 More Than 1 Million Google Accounts Breached by Gooligan. Verkkodokumentti. Saatavissa: http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/ Luettu viimeksi 2.3.2017.

22 You need to update your iPhone RIGHT NOW or run the risk of a devastating hack attack. Verkkodokumentti. Saatavissa: https://www.thesun.co.uk/news/1677166/you-need-to-update-your-iphone-right-now-because-something-terrifying-has-happened/ Luettu viimeksi 2.3.2017.

23 Tietomurto. Verkkodokumentti. Saatavissa: http://www.heikniemi.fi/kirj/jur/rikos/tietomurto.html Luettu viimeksi 2.3.2017.

24 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Saatavissa: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF Luettu viimeksi 31.3.2017.

25 Why Do People Hack? Verkkodokumentti. Saatavissa: https://www.techwalla.com/articles/why-do-people-hack Luettu viimeksi 2.3.2017.

26 6 Reasons Why Hackers Want to Hack Your Website. Verkkodokumentti. Saatavissa: https://www.cloudbric.com/blog/2015/10/6-reasons-why-hackers-want-to-hack-your-website/ Luettu viimeksi 2.3.2017.

27 Why Do People Hack? Verkkodokumentti. Saatavissa: http://informationassurance.regis.edu/ia-programs/resources/ia-update/why-do-people-hack Luettu viimeksi 2.3.2017.

28 Good Question: How Often Do Hackers Get Caught? Verkkodokumentti. Saatavissa: http://minnesota.cbslocal.com/2014/12/18/good-question-how-often-do-hackers-get-caught/ Luettu viimeksi 15.3.2017.

29 Why do people hack Social Media accounts? Verkkodokumentti. Saatavissa: http://www.pandasecurity.com/mediacenter/social-media/people-hack-social-media-accounts/ Luettu viimeksi 2.3.2017.

30 Big Data muuttaa maailmaa. Verkkodokumentti. Saatavissa: http://www.talouselama.fi/kumppaniblogit/tieto/big-data-muuttaa-maailmaa-3440603 Luettu viimeksi 2.3.2017.

31 Why do people hack computers? Verkkodokumentti. Saatavissa: http://www.computerhope.com/issues/ch001530.htm Luettu viimeksi 2.3.2017.

32 Sony PSN downed; hacking group claims DDOS attack. Verkkodokumentti. Saatavissa: https://www.scmagazine.com/sony-psn-downed-hacking-group-claims-ddos-attack/article/527821/ Luettu viimeksi 2.3.2017.

33 EU slaps €166 million fine on Sony, Sanyo, Panasonic battery units over price cartel. Verkkodokumentti. Saatavissa: http://www.japantimes.co.jp/news/2016/12/13/business/corporate-business/eu-slaps-e166-million-fine-sony-sanyo-panasonic-battery-units-price-cartel/ Luettu viimeksi 31.3.2017.

34 How Sloppy, Biased Video Games Reporting Almost Destroyed a CEO. Verkkodokumentti. Saatavissa: http://www.breitbart.com/london/2014/09/23/how-sloppy-biased-video-games-reporting-almost-destroyed-a-ceo/ Luettu viimeksi 2.3.2017.

35 Stardock Lawsuits Dropped, Ex-Employee Apologizes. Verkkodokumentti. Saatavissa: http://kotaku.com/stardock-lawsuits-dropped-ex-employee-apologizes-1377925759 Luettu viimeksi 2.3.2017.

36 7 Types of Hacker Motivations. Verkkodokumentti. Saatavissa: https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/ Luettu viimeksi 2.3.2017.

37 Crime Prevention: Do Not Be An Easy Target For Crime. Verkkodokumentti. Saatavissa: https://www.moneyinstructor.com/doc/crimetarget.asp Luettu viimeksi 2.3.2017.

38 Physical attacks. Verkkodokumentti. Saatavissa: http://www.hackingtheuniverse.com/infosec/attack-methodology/penetration/physical-attacks Luettu viimeksi 2.3.2017.

39 Physical security: The cornerstone of building a safer cloud. Verkkodokumentti. Saatavissa: http://blog.trendmicro.com/physical-security-cornerstone-building-safer-cloud/ Luettu viimeksi 2.3.2017.

40 10 physical security measures every organization should take. Verkkodokumentti. Saatavissa: http://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take/ Luettu viimeksi 2.3.2017.

41 The Insider Threat: A Cloud Platform Perspective. Verkkodokumentti. Saatavissa: https://securityintelligence.com/the-insider-threat-a-cloud-platform-perspective/ Luettu viimeksi 2.3.2017.

42 Insider Threats: A Guide to your Cloud Apps Security. Verkkodokumentti. Saatavissa: https://www.syscloud.com/insider-threats-a-guide-to-your-cloud-apps-security/ Luettu viimeksi 2.3.2017.

43 Mitigating Insider Threat From the Cloud. Verkkodokumentti. Saatavissa: http://www.bankinfosecurity.com/interviews/mitigating-insider-threat-from-cloud-i-1917 Luettu viimeksi 2.3.2017.

44 Definition: principle of least privilege (POLP). Verkkodokumentti. Saatavissa: http://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP Luettu viimeksi 2.3.2017.

45 DOS Attacks and Free DOS Attacking Tools. Verkkodokumentti. Saatavissa: http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref Luettu viimeksi 2.3.2017.

46 Denial of Service Attacks. Verkkodokumentti. Saatavissa: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html Luettu viimeksi 2.3.2017.

47 Hacking vs. DDoS – A Showdown. Verkkodokumentti. Saatavissa: https://www.staminus.net/hacking-vs-ddos-a-showdown/ Luettu viimeksi 2.3.2017.

48 Today's Brutal DDoS Attack Is the Beginning of a Bleak Future. Verkkodokumentti. Saatavissa: http://gizmodo.com/todays-brutal-ddos-attack-is-the-beginning-of-a-bleak-f-1788071976 Luettu viimeksi 2.3.2017.

49 The Three Elements of Defense Against Denial-of-Service Attacks. Verkkodokumentti. Saatavissa: http://www.biztechmagazine.com/article/2013/02/three-elements-defense-against-denial-service-attacks Luettu viimeksi 2.3.2017.

50 Phishing. Verkkodokumentti. Saatavissa: https://us.norton.com/security_response/phishing.jsp Luettu viimeksi 2.3.2017.

51 What are phishing scams and how can I avoid them? Verkkodokumentti. Saatavissa: https://kb.iu.edu/d/arsf Luettu viimeksi 2.3.2017.

52 How to recognize phishing email messages, links, or phone calls. Verkkodokumentti. Saatavissa: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx Luettu viimeksi 2.3.2017.

53 What is SSL? Verkkodokumentti. Saatavissa: https://www.globalsign.com/en/ssl-information-center/what-is-ssl/ Luettu viimeksi 2.3.2017.

54 3 Reasons Why Detecting Cloud Malware Is Essential for Cloud Security Solutions. Verkkodokumentti. Saatavissa: https://www.ciphercloud.com/blog/3-reasons-why-detecting-cloud-malware-is-essential-for-cloud-security-solutions/ Luettu viimeksi 2.3.2017.

55 The Cloud Malware Threat. Verkkodokumentti. Saatavissa: http://www.networkcomputing.com/network-security/cloud-malware-threat/1806517482 Luettu viimeksi 2.3.2017.

56 Cloud malware: A growing problem for public CSPs. Verkkodokumentti. Saatavissa: http://searchcloudsecurity.techtarget.com/tip/Cloud-malware-A-growing-problem-for-public-CSPs Luettu viimeksi 2.3.2017.

57 Definition: advanced persistent threat (APT). Verkkodokumentti. Saatavissa: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT Luettu viimeksi 2.3.2017.

58 Advanced Persistent Threat (APT). Verkkodokumentti. Saatavissa: https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html Luettu viimeksi 2.3.2017.

59 What's an Advanced Persistent Threat (APT)? A Brief Definition. Verkkodokumentti. Saatavissa: https://www.damballa.com/paper/advanced-persistent-threats-a-brief-description/ Luettu viimeksi 2.3.2017.

60 Advanced Persistent Threats: How They Work. Verkkodokumentti. Saatavissa: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1 Luettu viimeksi 2.3.2017.

61 Anatomy of Advanced Persistent Threats. Verkkodokumentti. Saatavissa: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html Luettu viimeksi 2.3.2017.

62 Explained: Advanced Persistent Threat (APT). Verkkodokumentti. Saatavissa: https://blog.malwarebytes.com/cybercrime/malware/2016/07/explained-advanced-persistent-threat-apt/ Luettu viimeksi 2.3.2017.

63 5 signs you've been hit with an advanced persistent threat. Verkkodokumentti. Saatavissa: http://www.infoworld.com/article/2615666/security/5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html Luettu viimeksi 2.3.2017.

64 Advanced Persistent Threats: Learn the ABCs of APTs - Part A. Verkkodokumentti. Saatavissa: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a Luettu viimeksi 2.3.2017.

65 What the Most Common Passwords of 2016 List Reveals [Research Study]. Verkkodokumentti. Saatavissa: https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/ Luettu viimeksi 2.3.2017.

66 Suomalaisten sata yleisintä salasanaa. Verkkodokumentti. Saatavissa: http://aiheet.domnik.net/ai-2011/11/100-yleisinta-salasanaa Luettu viimeksi 2.3.2017.

67 MTE Explains: How Password Cracking Works And What You Can Do to Protect Yourself. Verkkodokumentti. Saatavissa: https://www.maketecheasier.com/how-password-cracking-works/ Luettu viimeksi 2.3.2017.

68 Two-factor authentication: What you need to know (FAQ). Verkkodokumentti. Saatavissa: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ Luettu viimeksi 2.3.2017.

69 SteamID, Steam Account Names, Merging Accounts and Deleting Accounts. Verkkodokumentti. Saatavissa: https://support.steampowered.com/kb_article.php?ref=1558-qyax-1965 Luettu viimeksi 2.3.2017.

70 How Your Passwords Are Stored on the Internet (and When Your Password Strength Doesn't Matter) http://lifehacker.com/5919918/how-your-passwords-are-stored-on-the-internet-and-when-your-password-strength-doesnt-matter Luettu viimeksi 15.3.2017.

71 Serious Security: How to store your users' passwords safely https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/ Luettu viimeksi 15.3.2017.

72 Why passwords should be hashed http://security.blogoverflow.com/2011/11/why-passwords-should-be-hashed/ Luettu viimeksi 15.3.2017.

73 Rainbow Hash Cracking https://blog.codinghorror.com/rainbow-hash-cracking/ Luettu viimeksi 15.3.2017.

74 How to encrypt user passwords http://www.jasypt.org/howtoencryptuserpasswords.html Luettu viimeksi 15.3.2017.

75 Why You Shouldn't be using SHA1 or MD5 to Store Passwords https://www.bentasker.co.uk/blog/security/201-why-you-should-be-asking-how-your-passwords-are-stored Luettu viimeksi 15.3.2017.

76 Abusing Cloud Services For Cybercrime. Verkkodokumentti. Saatavissa: http://www.darkreading.com/attacks-breaches/abusing-cloud-services-for-cybercrime/d/d-id/1141323? Luettu viimeksi 2.3.2017.

77 How are cloud threats abusing public cloud services? Verkkodokumentti. Saatavissa: http://searchcloudsecurity.techtarget.com/answer/How-are-cloud-attacks-abusing-public-cloud-services Luettu viimeksi 2.3.2017.

78 Abuse And Nefarious Use Of Cloud Computing Information Technology Essay. Verkkodokumentti. Saatavissa: https://www.uniassignment.com/essay-samples/information-technology/abuse-and-nefarious-use-of-cloud-computing-information-technology-essay.php Luettu viimeksi 2.3.2017

79 Cloud API security risks: How to assess cloud service provider APIs. Verkkodokumentti. Saatavissa: http://searchcloudsecurity.techtarget.com/tip/Cloud-API-security-risks-How-to-assess-cloud-service-provider-APIs Luettu viimeksi 2.3.2017.

80 Exposed APIs Are A Threat To Cloud Computing. Verkkodokumentti. Saatavissa: http://www.massivealliance.com/2014/03/07/exposed-apis-threat-cloud-computing/ Luettu viimeksi 2.3.2017.

81 API security: How to ensure secure API use in the enterprise. Verkkodokumentti. Saatavissa: http://searchsecurity.techtarget.com/tip/API-security-How-to-ensure-secure-API-use-in-the-enterprise Luettu viimeksi 16.3.2017.

82 Top Six Reasons to Use API Keys (and How!). Verkkodokumentti. Saatavissa: https://stormpath.com/blog/top-six-reasons-use-api-keys-and-how Luettu viimeksi 16.3.2017.

83 What is an API key? Verkkodokumentti. Saatavissa: http://stackoverflow.com/questions/1453073/what-is-an-api-key Luettu viimeksi 16.3.2017.

84 7 Security Threats in the Cloud. Verkkodokumentti. Saatavissa: https://campustechnology.com/Articles/2010/12/01/7-Security-Threats-in-the-Cloud.aspx?Page=1 Luettu viimeksi 2.3.2017.

85 Top 8 Cloud Computing Threats and its Security Solutions. Verkkodokumentti. Saatavissa: https://www.clickssl.net/blog/top-8-cloud-computing-threats-and-its-security-solutions Luettu viimeksi 2.3.2017.

86 Avoid vulnerabilities and threats in the cloud. Verkkodokumentti. Saatavissa: https://www.ibm.com/developerworks/cloud/library/cl-cloudthreats/cl-cloudthreats-pdf.pdf Luettu viimeksi 2.3.2017.

87 The dirty dozen: 12 cloud security threats. Verkkodokumentti. Saatavissa: http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html Luettu viimeksi 2.3.2017.