Juho Virtanen

PALVELUNESTOHYÖKKÄYKSET PILVIPALVELUISSA

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

PALVELUNESTOHYÖKKÄYKSET PILVIPALVELUISSA

Virtanen, Juho
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
helmikuu 2017
Ohjaaja: Grönholm, Jukka
Sivumäärä: 42
Liitteitä: -

Asiasanat: tietoturva, verkkohyökkäykset, pilvipalvelut

Tässä työssä tarkasteltiin pilvipalveluihin kohdistuvia palvelunestohyökkäyksiä, niiden luonnetta ja toteutustapoja sekä esiteltiin joitakin yleisimpiä torjunta- sekä suojautumistapoja. Aihe on ja tulee olemaan ajankohtainen it-maailmassa, koska palvelunestohyökkäykset tulevat lisääntymään sekä määrältään että teholtaan tulevaisuudessa ja ovat jo nyt yksi suurimmista tietoturvauhista maailmassa.

Työssä tarkasteltiin aluksi sekä tietoturvaa että pilvipalveluja yleisesti, jonka jälkeen esiteltiin palvelunestohyökkäyksen ominaispiirteet. Tämän jälkeen havainnollistettiin esimerkkien kautta, miten pilveen kohidstuvat hyökkäykset vaikuttavat kuluttajien arkeen. Lopuksi koostettiin aiemipien lukujen pohjalta ohjeistus yritykselle sekä suunnattiin katsetta aiheen tulevaisuuteen.

Denial-of-service attacks in cloud services

Virtanen, Juho
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
February 2017
Supervisor: Grönholm, Jukka
Number of pages: 42
Appendices: -

Keywords: information security, network attack, cloud services

---

In this thesis the matter of work was to inspect denial-of-service attacks in cloud services and the used techniques and behavior of them as well as to present some of the common ways to deal with them from the point of prevention and security. The matter is and will be current in the IT world because DoS-attacks will grow in number and power in the future and these attacks are amongst the most dangerous security threats in the world.

On the first few chapters of the work the main focus was to present the common lines of information security and cloud services. After that, chapters of cloud service security and DoS-attacks followed until the work concludes with the presentation of some of the best know DoS-attacks on cloud and a small guidance to the companies as well as a quick look to the future of the DoS attacks in cloud services.

SISÄLLYS

1 JOHDANTO

Pilvipalveluihin kohdistuu tänä päivänä entistä enemmän palvelunestohyökkäyksiä ja myös suomalaisissa yrityksissä ja laitoksissa ne alkavat hiljalleen olemaan tuttuja ilmiöitä. Hyökkäyksiin suojautuminen on silti monesti puutteellista tai hyökkäyksiin ylipäätään suhtaudutaan niin, että ”ei ne meidän kohdalle satu”. Totuus kuitenkin on se, että tulevaisuudessa – myös Suomessa – pilveen kohdistuvat palvelunestohyökkäykset tulevat yleistymään ja koskettavat yhä useamman ihmisen elämää.

Palvelunestohyökkäykset ovat tietoturvan kannalta ongelmallisia, sillä ne ovat halpoja toteuttaa, ne saa suoritettua erittäin nopeasti ja hyökkäyksen voi vieläpä tehdä kuka tahansa internettiin pääsyn omaava henkilö. Hyökkäykset eivät ole uusi ongelma it-maailmassa, mutta tällä vuosikymmenellä tapahtunut kehitys on johtanut siihen, että palvelunestohyökkäyksiä pidetään tällä hetkellä jopa suurimpana uhkana tietoturvalle ja yksityisyydelle. Oman lusikkansa soppaan tuo kasvava IoT-laitteiden (Internet of Things, esineiden internet) määrä, joka edelleen tullee kasvattamaan hyökkäysten tekemää tuhoa. Tämä pakottaa sekä pilvipalveluiden tarjoajat että niiden käyttäjät etsimään jatkuvasti uusia keinoja hyökkäysten torjumiseen.

Palvelunestohyökkäykset aiheuttavat suuressa määrin taloudellista vahinkoa ja suurilla yrityksillä hyökkäyksistä aiheutuneet kustannukset ovat miljoonaluokkaa. Vaikka palvelunestohyökkäykset loukkaavat yksilön suojaa, yritykselle tärkein asia on juuri taloudellisen puolen kunnossapito. Hyökkäykset voivat olla kovin ennalta arvaamattomia ja uhriksi voi joutua kuka tahansa, mikä pitää it-alaa hyväksikäyttäviä palveluja varpaillaan nyt ja tulevaisuudessa.

2 TIETOTURVA YLEISESTI

2.1 Tietoturva käsitteenä

Termille ”tietoturva” on useita tarkkoja määrittelyjä, joista esimerkiksi Legal Information Instituten määritelmä kuuluu seuraavasti: ” Termillä ´tietoturva´ tarkoitetaan informaation ja informaatiota sisältävien laitteiden suojaamista valtuuttamattomalta käytöltä, paljastamiselta, häiriöltä, muokkaamiselta tai tuhoamiselta, jotta voidaan tarjota informaation yhtenäisyyttä, luottamuksellisuutta sekä saatavuutta. (Legal Information Institute.)

Yhtenäisyydellä tarkoitetaan tässä tapauksessa suojautumista väärältä informaatiolta tai informaation tuhoutumiselta. Yhtenäisyys sisältää myös informaation kiistämättömyyden varmistamisen sekä todentamisen. Luottamuksellisuudella varmistetaan se, että informaatioon ei pääse käsiksi kuka tahansa, vaan pääsy siihen on rajoitettu vain siihen valtuutetuille tahoille. Tämä sisältää myös henkilökohtaisen yksityisyyden sekä omistajakohtaisen informaation suojaamisen. Viimeisenä määrittelyssä mainittu saatavuus tarkoittaa vain sitä, että informaatioon käsiksi pääsy tulee olla mahdollista ajasta riippumatta sekä luotettavaa. (Legal Information Instititute.)

2.2 Työaseman tietoturva

Työaseman tietoturva on perusta kaikelle muulle tietoturvalle, sillä työasemien kautta toteutetaan hyvin usein muiden it-laitteiden, kuten palvelinten ja verkon hallintaa. Työaseman tietoturvan takaamiseksi on olemassa useita eri järjestöjen, virastojen tai laitosten tekemiä määrittelyjä parhaan turvallisuuden takaamiseksi työasemalla. Seuraavassa esitetään joitakin yleisimmistä käytännöistä.

Käyttäjästä riippuvaisia asioita on työaseman tietoturvaan liittyen useita. Esimerkiksi yksinkertaiset asiat, kuten salasanoistaan huolehtiminen ja koneelta uloskirjautuminen ovat tällaisia asioita. Kaiken luottamuksellisen datan tallentaminen tulisi ensisijaisesti

tehdä verkkolevyille ja epämääräisistä lähteistä ladatut sovellukset tulisi sekä jättää asentamatta että ylipäätään jättää lataamatta. (SANS Policy Team.)

Työaseman turvaamiseen liittyvät asiat, jotka liittyvät enemmän it-hallinnon puoleen, ovat esimerkiksi käyttöoikeuksien jakaminen niin, että data ei päädy vääriin käsiin. Myös koneet, jotka sisältävät arkaluontoista dataa ja eivät ole käytössä, tulisi sulkea lukkojen taakse, esimerkiksi lukolliseen kaappiin. Myös yksi tärkeimmistä asioista, mikä tulee ottaa huomioon, on verkkoturvallisuuden varmistaminen työaseman puolella. Verkkoliikennettä tulisi monitoroida myös päätelaitteilla. (SANS Policy Team.)

2.3 Palvelimen tietoturva

Palvelimen tietoturvan pitää olla vielä työaseman tietoturvaa kovemmalla tasolla. Sen läpi kulkee verkkoliikennettä hyvin usein enemmän kuin työaseman kautta ja se sisältää useimmat yrityksen tai yksilön käyttämät palvelut. Vaikka palvelin saattaa fyysisesti olla samanlainen kuin osa työasemista, on näiden kahden tietoturvassa yleensä huomattavia eroja ohjelmiston suhteen.

Palvelimeen on hyvä soveltaa tehokkaampaa salausta, palomuuria, liikenteen monitorointia ja palvelimen eristämistä. Tehokkaammalla salauksella tarkoitetaan hyväksi havaittua SSH-avainten käyttöä. Tavallisen salasanan murtaminen käy paljon helpommin, kuin SSH-avaimen, sillä avain sisältää paljon enemmän bittejä ja on näin vaikea murtaa ulkopuolelta. Avain toimii siten, että niistä tehdään yhteensopiva pari, private sekä public. Private-avain on jokaisen käyttäjän henk. koht. avain, kun taas public-avain annetaan palvelimille. Yhteyttä avatessa palvelin toteaa, ovatko avaimet yhteensopivia ja näin joko estää tai sallii liikenteen. Tehokkaampaan salaukseen kuuluu myös ns. PKI/SSL- salattu liikenne. Domain controller –palvelimelle usein luotu sertifikaatti salaa liikenteen firman sisäverkossa, esimerkiksi SharePointia varten. (Ellingwood, 2015.)

Palomuurin rooli on tietenkin estää haitallisen liikenteen pääsy koneelle, mutta palvelimen tapauksessa on erityisen tärkeää, että vain oikeat portit ovat auki liikenteelle, jotkin firman sisäverkkoon, jotkin ulkoverkkoon. It-henkilöstön tulee ottaa huomioon

minkä tyyppistä liikennettä ja protokollia firman verkossa kulkee ja sen mukaan määrittää palomuuriensa asetukset. Vaikka yrityksen sovellukset ja laitteisto sinänsä olisivatkin suojattuja, on palomuuri - joko fyysisenä tai sovelluspohjaisena – aina ekstralisä turvallisuuteen. Palvelimia voi edelleen suojata eristämällä ne muusta verkkoympäristöstä, esimerkiksi omaan verkkoonsa tai laittamalla tiettyjä sovelluksia vain tietynlaisille palvelimille. Nämä asiat ovat hyvin paljon riippuvaisia siitä, millaisia yrityksen infrastruktuuri ja käytetyt sovellukset ovat. Eristämisellä pyritään siihen, että jos verkko joutuu hyökkäyksen kohteeksi, ovat vahingot pienempiä, kun palvelimet on pilkottu omiksi kokonaisuuksikseen. (Ellingwood, 2015.)

2.4 Verkon tietoturva

Työaseman ja palvelimen tietoturvan jälkeen luonnollisena jatkumona tulee verkon tietoturva. Yritysten verkoista on hiljalleen tullut varsin suuria kokonaisuuksia ja verkon ymmärtäminen on tärkeä osa yrityksen toimintaa. Yritysten käyttämissä koneissa on mahdollisesti useampia käyttöjärjestelmiä ja varmasti vielä useampia sovelluksia, komponentteja ja protokollia. Nämä kaikki laitteet ovat kytkettynä yleensä ulospäin menevää verkkoon, joten tietoturvan on oltava kunnossa. (Tutorials Point.)

Internet-verkko rakentuu TCP/IP-protokollan ympärille. Protokolla määrittää säännöt verkon liikenteelle ja sisältää mm. datan kohdeosoitteen, tulo-osoitteen, datan sekä varmistaa, että data kulkee oikein paikasta A paikkaan B. Protokolla on kaksiosainen ja TCP-osa (Transmission Control Protocol) kommunikoi sovellusten kuljetuskerroksen kanssa, kun taas IP (Internet Protocol) kommunikoi verkkokerroksen kanssa. (Tutorials Point.)

TCP/IP-protokolla sisältää joitakin tunnettuja heikkouksia, joita ovat mm. ip-protokollan sisällä olevan http-protokollan rakenne, sen autentikointiominaisuudet sekä ip-protokollan avoimuus. Http-protokolla on sovelluskerroksen protokolla, jonka avulla toteutetaan web-sivuja. Heikkoutena sillä on se, että protokolla sisältää yksinkertaisesti pelkkää tekstiä, jota tunkeutujan on helppo muokata. Autentikointiongelmat puolestaan tarkoittavat, että kolmas osapuoli saattaa kaapata yhteyden, kun sitä käynnistetään kahden tahon välillä. Ip-protokollan avoimuus puolestaan on riskialtis ominaisuus,

sillä protokollan otsikkoa muuttamalla hyökkääjä voi tehdä hyökkäyksen kohdeverkkoon varsin helposti. (Tutorials Point.)

Verkon tietoturvan lisäämiseksi eräs suosittu menettely on ottaa käyttöön VPN (Virtual Private Network). VPN:ää käytetään etäkoneiden yhdistämiseen yrityksen verkkoon ja ne esitetään kuin ne olisivat yrityksen sisäisen verkon koneita. Tätä kautta esimerkiksi etäpalvelimiin saadaan aikaseksi turvallinen yhteys ja verkko saadaan määriteltyä kuin se olisi paikallinen verkko. Jos VPN:n käyttö vain on mahdollista, kannattaa sitä ehdottomasti käyttää firman sisäiseen kommunikointiin. Sen käyttöönotto saattaa koko yrityksen laajuudelta viedä aikaa, mutta se maksaa tietoturvassa moninkertaisesti takaisin. (Ellingwood, 2015.)

3 PILVIPALVELUT

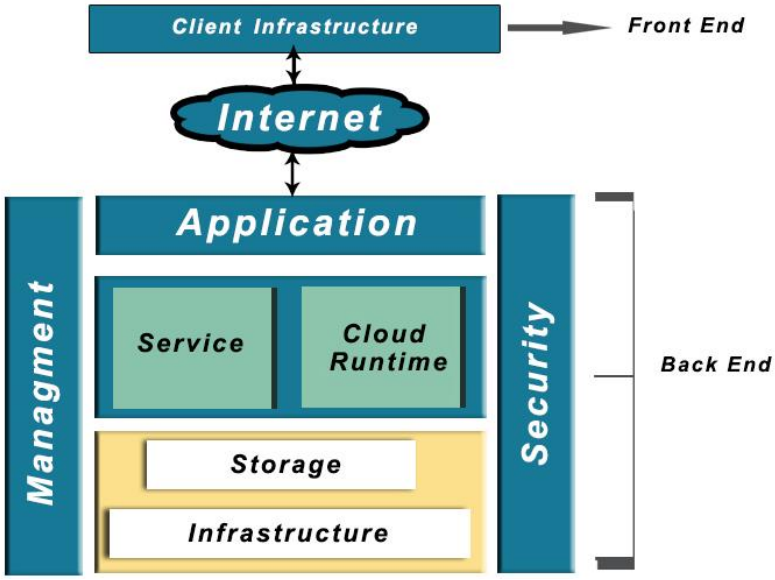
3.1 Arkkitehtuuri

Pilvilaskennan arkkitehtuurista puhuttaessa on helpointa lähteä liikkeelle jakamalla se kahteen osaan: front end sekä back end. Front end on käyttäjälle näkyvissä oleva osa arkkitehtuurista ja se sisältää käyttäjän päätelaitteen (ja mahdollisesti päätelaitteen käyttämän verkon) sekä sovelluksen, jolla itse pilvipalveluun päästään käsiksi. (Strickland.)

Back end puolestaan sisältää kaiken muun pilveen kuuluvan arkkitehtuurin, eli reitittimet, muut mahdolliset päätelaitteet sekä tallennustilat, joihin data tallennetaan. Back endin voi siis teoriassa kuulua kaikki internettiin liitetyt laitteet, mutta käytännössä se on rajattu eri tietosuojamenetelmin lukuisiin eri osiin. Lisäksi lähes jokaisella pilveen toteutetulla sovelluksella on oma palvelin/palvelinklusteri. (Strickland.)

Arkkitehtuuria valvoo järjestelmänvalvoja ja koko pilven hallinta on usein keskitetty yhdelle fyysiselle palvelimelle, joka on virtualisoitu. Se toimii sille asetetun protokol-

lajoukon mukaan ja käyttää hallintaan middlewareksi kutsuttua ohjelmistoa. Middleware sallii verkkoon yhdistettyjen koneiden kommunikoinnin toistensa kanssa. (Strickland.)



Kuva 1. Pilvilaskennassa toteutettua arkkitehtuuria (Kelvin 2014.)

Myös virtualisoinnilla on suuri rooli tämän päivän pilvipalveluissa. 70-luvulla alkanut koneiden virtualisointi antaa mahdollisuuden skaalata talletettua dataa, koska virtualisointi usein yhdenmukaistaa datan. Virtualisointi myös yksinkertaistaa datan toimitusta tarjoamalla alustan monimutkaisillekin it-ratkaisuille useiden käytössä olevien käyttöjärjestelmien ansiosta. (Bloor, Halper, Hurwitz & Kaufman 2016.)

Virtualisointia voi soveltaa verkkoihin, laitteiden fyysisiin komponentteihin, käyttöjärjestelmiin ja sovelluksiin. Virtualisoinnilla on kolme pääpiirrettä, jotka tekevät siitä laadukkaan alustan pilvipalveluiden tarjoamiselle: kovalevyjen partitointi, virtuaalikoneiden eristäminen sekä sovellusten kapselointi. (Bloor, ym. 2016.)

Kovalevyjä partitoimalla on mahdollista asentaa samalle fyysiselle järjestelmälle useita eri käyttöjärjestelmiä ja tätä kautta monipuolistaa järjestelmään talletetun datan käyttöä ja jakelua. Virtuaalikoneiden eristämisellä puolestaan haetaan parempaa tietoturvaa. Jos yksi kone kaatuu ja data menetetään, ei kaatuminen lähde ketjureaktiona eteenpäin vaan muut virtuaalikoneet jatkavat toimintaansa normaalisti. Sovellusten kapseloinnin ansiosta jokainen virtuaalikone voidaan esittää ulkoverkolle yksittäisenä

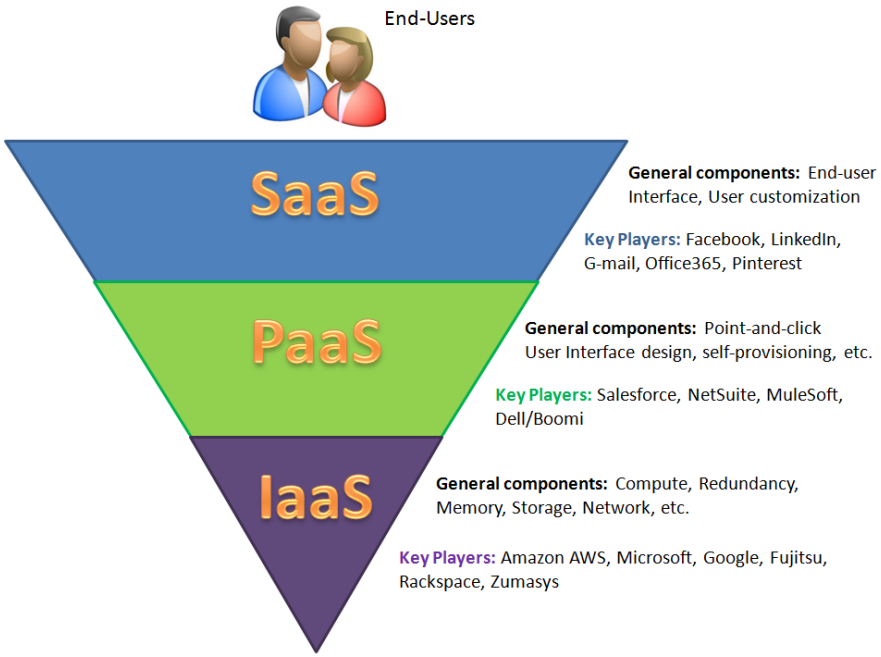
tiedostona mikä tekee sovellusten etsimisen ja tunnistamisen helpommaksi. (Bloor, ym. 2016.)

Useat yritykset käyttävät pilvensä hallintaan hypervisoreiksi-nimitettyä ohjelmistokokonaisuutta. Hypervisor esittää pilvessä talletettuna olevan datan ongelmitta monille ulkoverkon käyttöjärjestelmille, jotka dataa tulevat lukemaan. Hypervisorit pystyvät lataamaan useita käyttöjärjestelmiä mikä jälleen kerran laskee yritysten käyttökustannuksia. (Bloor, ym. 2016.)

3.2 Tekniikka

3.2.1 Yleistä

Pilvilaskennan pohjalta on syntynyt kolme yleisesti tunnustettua palvelumallia, joiden avulla pilvilaskenta valjastetaan päätelaitteiden käyttäjille. Malleja kutsutaan yleisnimityksellä pilvipalveluiksi ja nämä kolme mallia ovat IaaS (Infrastructure as a Service), PaaS (Platform as a Service) sekä SaaS (Software as a Service). Palvelumallit täydentävät toisiaan, kuten alla olevassa kuvassa on esitetty (Kuva 2).



Kuva 2. Pyramidikuvio pilvipalvelumalleista esimerkkien kanssa. (Paasisafad.com 2013.)

3.2.2 SaaS

Software as a Service -mallilla tarkoitetaan pilvipalvelua, jolla asiakas pääsee haluttuun palveluun (software) käsiksi verkon – tyypillisesti internet – kautta. Hyviä esimerkkejä SaaS-palveluista ovat mm. Facebook, Twitter ja Googlen hakukone. (Interroute 2015.)

The National Institute of Standards and Technologyn (NIST) yleisesti tunnustettu kuvaus SaaS-mallista on seuraavanlainen: Kuluttajalle tarjottu palvelu, jolla kuluttaja käyttää kehittäjän pilvessä toimivia sovelluksia. Sovellukset ovat saatavilla useiden eri päätelaitteiden kautta, joko 'thin clientin' - kuten web-selaimen – tai ohjelman käyttöliittymän kautta. Kuluttaja ei hallitse sovelluksen takana olevaa pilvi-infrastruktuuria mukaan lukien verkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa tai edes yksilöllisiä sovelluksen ominaisuuksia, poikkeuksena mahdolliset sovelluksen käyttäjäkohtaiset määrittelyasetukset. (Mell & Grance 2012, 16.)

SaaS-palveluiden tyypillinen ominaisuus on myös palveluiden vuokraus sekä palvelussa käytetyn datan tallentaminen pilveen. SaaS-palveluita harvoin ostetaan kertamaksulla kokonaisina paketteina niiden toimittajilta. Yleisempi tapa on vuokrata palvelu esimerkiksi kuukausittaista käyttömaksua vastaan. (Interroute 2015.)

3.2.3 PaaS

Platform as a Service on yhden tason SaaS-mallia alempana. Nimensä mukaisesti PaaS tarjoaa alustapohjaisia palveluita. Se kehitettiin lähinnä sovelluskehittäjiä silmällä pitäen, sillä PaaS-tason alustapalveluiden avulla kehitetään, suoritetaan ja hallitaan sovelluksia pilvessä.

NIST:n tekemä kuvaus PaaS:sta antaa hyvän kokonaiskuvan: Kuluttajalle tarjottu palvelu, jolla pilvi-infrastruktuurissa otetaan käyttöön kuluttajien tekemiä tai hankkimia sovelluksia, jotka on luotu käyttämällä kehittäjän tukemia ohjelmointikieliä, kirjastoja, palveluita ja työkaluja. Kuluttaja ei hallitse alapuolella olevaa pilvi-infrastruktuuria

mukaan lukien verkkoa, palvelimia, käyttöjärjestelmiä tai tallennustilaa, mutta kontrolloi käyttöön otettuja sovelluksia ja mahdollisesti sovelluksen hallintaympäristön määrittelyasetuksia. (Mell & Grance 2012, 16.)

Toinen kuvaus PaaS:sta antaa ohjelmistoja tarjoavan yrityksen näkemyksen: ”Kehittäjät eivät halua miettiä palvelimien, tallennustilan tai varmuuskopioinnin toimittamisesta, jotka liittyvät sovelluksen kehittämiseen ja suorittamiseen. He haluavat kirjoittaa koodia, testata sovellusta, suorittaa sovellusta ja korjata sen bugeja jatkuvasti. Kaikki back endiin liittyvä työ palvelimien asentamisessa pitäisi sujua huomaamatta taka-alalla ja tässä PaaS auttaa.”(Butler 2013.)

PaaS:sta tarjoavat tahot pitävät huolen siitä, että alemman tason infrastruktuuri on kunnossa ja pystyy tarjoamaan resurssit sovelluskehittäjille. Näihin resursseihin lukeutuvat käyttöjärjestelmät, tietokannat, middleware-ohjelmistot ja ohjelmistotyökalut. (Butler, 2013.)

3.2.4 IaaS

Infrastructure as a Service on alimman tason pilvipalvelumalli ja se sisältää verkon, käyttöjärjestelmät, tallennustilan sekä palvelimet eli palvelumallien fyysiset laitteet. Infrastruktuuripalvelut tarjoavat perustan ylemmän tason palvelumalleille PaaS:lle ja SaaS:lle.(Loeffler 2011.)

NIST on määritellyt myös IaaS-mallin; Kuluttajalle tarjottu palvelu, jolla on tarkoitus tarjota prosessointi, tallennustila, verkot ja muut keskeiset laskentaresurssit, joiden avulla kuluttaja pystyy ottamaan käyttöön ja suorittamaan vapaavalintaisia ohjelmistoja mukaan lukien käyttöjärjestelmiä ja sovelluksia. Kuluttaja ei hallitse alapuolella olevaa osaa pilvestä, mutta kontrolloi käyttöjärjestelmiä, tallennustilaa, käyttöön otettuja sovelluksia sekä mahdollisesti valittuja osia verkosta (esim. palomuureja). (Mell & Grance 2012, 16.)

IaaS-mallin on toimittava joustavasti kellon ympäri, sillä ilman perustaansa PaaS ja SaaS eivät voi toimia. IaaS-tason laitteet ja verkot on varustettu usein useilla palomuureilla ja tietoturva on yksi tason tärkeimmistä prioriteeteista. Yleensä koneet ovat virtualisoituja. (Loeffler 2011.)

3.3 Käyttömallit

3.3.1 Yleistä

Pilvilaskennassa on palvelumallien lisäksi myös pilven käyttömallit, jotka määritellään käyttöoikeuksien sekä pilven muokattavauuden mukaan. Kaksi yleisintä mallia ovat private cloud (yksityinen pilvi) ja public cloud (julkinen pilvi). Näiden lisäksi on olemassa myös hybrid cloud (hybridipilvi) sekä community cloud (yhteisöpilvi). (Loeffler, 2011)

3.3.2 Private cloud

Private cloud on nimensä mukaisesti jonkin tahon yksityisessä käytössä. Yritysten private cloudit ovat yleisiä ja siihen riittää esimerkiksi firman intra ja tietokannat. Private cloudin ominaispiirteisiin kuuluu, että sekä pilven suunnittelun, toteutuksen että ylläpidon hoitaa usein pilven omaava yhtiö. Private cloud tulee usein tarpeeseen, jos yritys hakee esimerkiksi parempaa turvaa datalleen, tiettyjä järjestelmävaatimuksia tai lakipykälien noudattamista. (Loeffler 2011.)

Private cloudin toteutusmallit ovat seuraavat: self-hosted (itse ylläpidetty), hosted (ulkoistettu) sekä appliance. Self-hosted pilvi tarjoaa mm. pilven käyttäjälle täydellisen kontrollin sekä pilven arkkitehtuuriin että ohjelmistoon. Self-hosted pilvi myös sijaitsee hyvin usein samoissa toimitiloissa muun firman kanssa ja näin pääsy fyysisille laitteille on helppoa. (Loeffler 2011.)

Hosted cloudin erot tulevat pääasiassa siitä, että pilven fyysinen laitteisto on kolmannen osapuolen hallussa, samoin kuin ylläpitovastuu. Toisaalta hosted cloud tarjoaa

myös datakeskuksen tuomat edut, kuten suuret siirtonopeudet sekä varman tietoturvan. (Loeffler 2011.)

Kolmas yksityisen pilven muoto appliance on kahden edellisen sekoitus. Pilvi hankitaan sen toimittajalta käyttäjän mieltymysten mukaisena. Pilven hallintaa ja ylläpitoa voi joko ulkoistaa tai pitää firman sisällä. Appliance-pilven käyttöön otossa on usein alhaiset riskit, jos pilven käyttäjä on tilausvaiheessa tiennyt mitä tilaa. Myös tietoturvan helpompi (yhtiön sisäinen) kontrolli on appliance-pilven etu. (Loeffler 2011.)

3.3.3 Public cloud

Public cloud on luonnollisesti yksityisen vastakohta. Public cloudin palvelut toimitetaan internetverkon yli ja palvelut itsessään hankitaan halutun palvelun toimittajalta. Public cloudissa on tiettyjä etuja verrattuna private cloudiin. Sen käyttäjä saa palvelut usein nopeasti itselleen ja sovellukset kehittyvät jatkuvasti. Lähes kaikilla public cloudin sovelluksilla on hyvä tietoturva, ne ovat jatkuvasti saatavilla ja sovellusten käyttö on vakaata. (Loeffler 2011.)

Public cloudin muodot jaetaan kahteen kategoriaan: shared (jaettu) sekä dedicated (omistettu) cloud. Shared cloudin suurin etu on sen valtava skaalautuvuuspotentiaali. Shared cloudista tilan ostaminen on yleensä aluksi halpaa ja pilven käyttöönotto on nopeaa. Pilven hallinnasta vastaa pilven tarjoava taho ja pilven fyysiset laitteet ovat suurimmissa infrastruktuureissa hajautettu maantieteellisesti eri paikkoihin (serverihallit). Pilven arkkitehtuuri, muokkaus ja tietoturva ovat myös pilven tarjoajan vastuulla. (Loeffler 2011.)

Dedicated cloud on yleensä osoitettu tietylle taholle/käyttäjälle. Infrastruktuuriltaan ja arkkitehtuuriltaan se saattaa muistuttaa hyvinkin paljon jaettua pilveä, kun taas hintatasoltaan omistettu pilvi saattaa olla kalliimpi kuin jaettu. Tietoturva, suorituskyky ja muokattavuus voivat olla paremmalla tasolla mitä shared cloudissa. (Loeffler 2011.)

3.3.4 Muut pilvet

Hybrid cloud yhdistelee useampia pilviä ja niiden osina voi olla sekä private että public cloudeja. Data on usein tehokkaasti saatavilla. Hybridipilvi on tätä nykyä vanhentunut malli, sillä yhä useampi yritys käyttää täysin ulkoisia pilvipalveluita. Tämä tosin altistaa yrityksen datan herkemmin ulkoisille uhille. Community Cloud (yhteistöpilvi) on puolestaan tietyn yhteisön käytössä oleva pilvi. Pilveä hallitsee jokin yhteisössä mukana oleva tai kolmannen osapuolen taho. (Loeffler 2011.)

4 PILVIPALVELUIDEN TIETOTURVA

4.1 Yleistä

Ehkä tärkein asia, jota pilvipalveluita hankittaessa kannattaa ottaa huomioon, on palvelun tietoturvan taso. Heikko tietoturva altistaa paitsi hyökkäyksille, myös datan menetykselle ja kustannusten nousulle. Pahimmassa skenaariossa koko pilveä käyttävän tahon (yleensä yritys) data sekä palvelut menetetään ja näin pilvipalveluiden edut nollautuvat täysin. (Cloud Standards Customer Council, lyh. CSCC, 2015.)

Kun yritys aikoo siirtää palveluitaan pilveen, tulisi firman miettiä tarkkaan mitä he pilveltä haluavat ja tehdä laajamittaista yhteistyötä pilven tarjoajan kanssa. Näin kummankin osapuolen välille syntyy realistinen kuva siitä mitä, yhteistyöltä voi odottaa. Eri pilvipalvelumalleilla (SaaS, IaaS ja PaaS) on erilaisia vaatimuksia tietoturvan suhteen, joten yhteistyön olisi oltava laajaa myös tämän seikan takia. Usein pilvipalveluita ostava taho ei ole kovinkaan tietoinen eri palvelumalleihin liittyvistä tietoturvariskeistä. Pilven tietoturva itse voidaan jakaa yleismaallisesti käyttäjien toimiin sekä itse datan hallintaan. (CSCC, 2015.)

4.2 Riskit

Vaikka useat pilven riskit ovat saman tyyppisiä tai aivan samoja kuin muillakin it-toimialoilla, vaatii pilvipalvelut luonteensa takia erityistä huomiota muutamissa aihealueissa. Käyttäjiin ja suoraan heidän toimiinsa liittyviä riskejä ovat mm. vastuun epäselvä jako, palvelun hallinnan menetys, heikko käyttäjäautentikointi, eri maiden lakipykälät pilveen liittyen, virhetilanteiden hallinta, palvelun tarjoajan tekemät virheet sekä pilven käyttäjän itsensä tahallaan aiheuttama vahinko. Enemmän tekniikan ja sovellusten piikkiin voidaan laittaa mm. palvelun eristyksen pettäminen, palvelun käyttöliittymän virheet, sovelluksen tietoturva ja palvelun odottamaton alasajo. Viimeksi mainitut tekniikkaan liittyvät virheet ovat usein viime kädessä ihmisestä riippuvia asioita, mutta ne on suurilta osin automatisoitu. (CSCC, 2015.)

4.3 Käyttäjien rooli

Kun otetaan tiettyjä erityisesti pilvipalveluiden tietoturvaan vaikuttavia tekijöitä esiin, nousee sieltä usein esiin käyttäjä suuri rooli. Käyttäjä on kuitenkin se pala tietojärjestelemissä, joka viime kädessä kontrolloi kaikkea. Siksi onkin erityisen tärkeää varmistaa, että käyttäjien motiivit ja päämäärät ovat selvät pilvipalveluiden tietoturvan näkökulmasta ja muutenkin vastuullisessa roolissa.

4.3.1 Pilvipalveluiden hallinnollinen puoli

Lähes kaikilla yrityksillä on firman sisäiset säännöt ja menetelmät tietoturvan ja hallinnon suhteen. Edellä mainitut säännöt ja menetelmät on tehty kokemuksen kautta ja valmistavat yritystä mahdollisiin ongelmatilanteisiin. Nämä samat säännöt eivät enää päde, jos yritys siirtää toimiaan pilvipalveluiden puolelle, sillä riskit eroavat hieman muusta it-osastosta. Tällöin tulisi varmistaa, että säädökset päivitetään ja asiantuntija-apua kysytään joko palveluntarjoajalta tai muulta kolmannen osapuolen ammattilaiselta. (CSCC, 2015.)

Edellä mainitut riskit liittyvät siihen, kuka pilveä oikeasti hallinnoi. Vastuuta voidaan jakaa sekä asiakkaalle että palveluntarjoajalle, mutta rajat on tehtävä selviksi. Vastuunjakoon vaikuttaa eniten se, minkä tyyppinen pilvipalvelu on kyseessä. IaaS-tyyppisessä ratkaisussa tarjoaja antaa yrityksen käyttöön vain infrastruktuurin, joten asiakkaan huolehdittavaksi jää alusta ja sovellus. Vastakohtana taas SaaS-tyyppinen ratkaisu tarjoaa sovellusta myöten kaikki pilven osat suoraan asiakkaalle painon ollessa itse sovelluksessa. Ensisijaisesti pilveä hallinnoi yleensä tarjoaja ja asiakas vain antaa viitteet sille, mihin suuntaan he haluavat pilvipalvelunsa kanssa edetä. Pilven hallinto on dokumentoitava tarkasti, jotta myöhemmin eteen tulevissa ongelmatilanteissa pystytään osoittamaan, mikä asia on kenenkin vastuulla. (CSCC, 2015.)

Pilvipalveluiden hallintoon liittyy monesti asiakkaan datan sijainnin osoittamisen vaikeus. Data sijaitsee todennäköisesti useassa eri datakeskuksessa ja joissain tapauksissa eri maissa, mikä tarkoittaa sitä, että samaan dataan saattaa päteä erilaiset lait, johtuen valtioiden tavoista käsitellä tietoturvaa. Pilvipalvelua ostava asiakas ei varmastikaan ole tietoinen siitä, missä talletettu data sijaitsee. Tällä tiedolla on merkitystä sikäli, että valtioilla on eri lait yksityisyyden ja datan suojelun suhteen. (CSCC, 2015.) Datan sijainnin suhteen hyvän esimerkin tarjoaa Brexit, sillä monen briteissä toimivan pilvipalvelun tarjoajan arki meni uusiksi Britannian EU-lähdön myötä. Brexit toi ennen muuta epävarmuutta siihen, miten tietosuojan lait tulevat muuttumaan ja uusien datakeskuksien suunnitteluja ollaankin Britanniassa laitettu jäihin. (Dignan, 2016.) Myös palveluiden hinnat ovat jo kallistuneet epävarmojen aikojen takia. Microsoftin ”rankaisi” Britanniaa erosta nostamalla Azure-palvelunsa hintoja. Toiset firmat, kuten Amazon ja Cisco, laskuttavat asiakkaitaan USA:n dollareissa ja hinnat nousivatkin heti dollari-euro-kurssin vaihtelun takia. (Orlowski, 2016.)

4.3.2 Käyttäjien roolit

Koska pilvi on sekä asiakkaan että tarjoajan yhteinen projekti, on selvää, että käyttäjien rooleilla on suuri osa tietoturvaa. Pilven käyttö tarkoittaa sitä, että palvelun tarjoajan tulee päästää asiakkaan käyttäjiä tekemään operaatioita omiin järjestelmiinsä jossakin määrin kuin myös päinvastoin, eli tarjoajalla on oikeus päästä käsiksi asiakkaan dataan riittävissä määrin. Pilven tarjoajan on varmistettava, että asiakas voi määritellä

tarpeelliset roolit omille käyttäjilleen ja asiakkaan on puolestaan otettava selvää siitä, että palveluntarjoajalla on selvät rajat sille, kuka asiakkaan dataan pääsee käsiksi ja miten. Palveluntarjoajalla on myös oltava turvallinen järjestelmä käyttäjien identiteetin salassa pitämiseksi. (CSCC, 2015.)

Kun yritys määrittää käyttäjien rooleja ja oikeuksia palveluntarjoajan kanssa, voidaan miettiä esimerkiksi sellaisia asioita kuin miten palveluntarjoaja hoitaa edellä mainitun identiteetin salauksen, käyttäjien luotettavan autentikoinnin, palveluun sisään- ja uloskirjautumisen turvallisuuden sekä ylipäätään käyttäjien hallinnan. Yritysten ei esimerkiksi kannata replikoida käyttäjätietokantojaan turhaan moniin pilvipalveluihin, mikäli se on jo kerran tehty jonkun toisen tahon kanssa. (CSCC, 2015.) Myös käyttäjien seurannalla voidaan tehostaa tietoturvaa, sillä se vähentää tahallisen haitallisen toiminnan määrää ja tehostaa käyttäjien työntekoa, sillä käyttäjät keskittyvät olennaiseen tietäessään, että heidän toimiaan saatetaan seurata. Käyttäjäseuranta auttaa myös ongelmatilanteissa, sillä ongelman johtuessa käyttäjästä syy pystytään seurannan avulla paikallistamaan helpommin. (Chickowski, 2015.)

4.4 Datan hallinta

Käyttäjien rooli pilven tietoturvassa on suuri ja yhtä suuri painoarvo voidaan antaa itse datan suojelulle. Data on merkittävä osa minkä tahansa yrityksen toimintaa tänä päivänä, toimialasta riippumatta. Siksi on ensiarvoisen tärkeää, että suojaus on kunnossa ja sen ylläpito pysyvää. Pilvipalveluiden kohdalla datan suojaus korostuu, sillä pilvipalveluiden rakenne on erilainen kuin muualla it-maailmassa ja – kuten edellisissä kappaleissa todettua – pilveä hallinnoi useampi kuin yksi taho. Datan suojauksesta puhuttaessa tarkoitetaan usein ennalta ehkäisyä ja torjumista, kuten tietomurtoja, varkauksia, tai tunkeutumisia dataan. (CSCC, 2015.)

4.4.1 Eri palvelumallien erot datan suojauksessa

Pilven palvelumallista riippuu, kenelle vastuu datasta pääasiallisesti jakautuu. IaaS-palveluissa vastuu on usein enemmän asiakkaan puolella, sillä tarjoaja antaa vain alustan palveluiden toteutukselle. SaaS puolestaan sysää vastuuta palveluntarjoajalle, sillä

kyseinen taho on vastuussa kaikesta sovellustasosta alaspäin. Mutkikkaamman haasteen tarjoaa PaaS, sillä sovelluspuolen tekee asiakas ja alustan sekä infrastruktuurin tarjoaa palveluntarjoaja. On tärkeää ymmärtää, miten data käyttäytyy missäkin osassa PaaS-toteutusta, jotta vastuu voidaan osoittaa oikealle taholle. (CSCC, 2015.)

4.4.2 Toimia datan suojaamiseksi

Datan suojaamisen parantamiseksi on olemassa useita keinoja, kuten esimerkiksi datakartan muodostaminen, kaiken tyyppisen datan huomioiminen, erilaiset standardit suojaukseen sekä identiteettien ja kulun valvonta. Datakartan muodostamisella tarkoitetaan sitä, että kaikki dataa sisältävät ja käsittelevät resurssit tunnistetaan, niiden käyttöön perehdytään ja rakennetaan kaiken kattava kuvaus datan käytöstä yrityksessä. Tähän kuuluu myös taloudelliset ja lailliset puolet datan käytöstä sekä eri dataa käsittelevien laitteiden ja sovellusten vuorovaikutussuhteet. (CSCC, 2015.)

Kaiken tyyppisen datan huomioiminen on puolestaan itsestään selvän tärkeää, mutta saattaa jäädä huomiotta joko tahattomasti tai käyttäjän laiskuuden vuoksi. Jos esimerkiksi yritys käsittelee harvinaisia tiedostotyyppejä tai erittäin laajaa kirjoa dataa, ei käyttäjillä ole välttämättä tietoa kaiken datan ominaisuuksista. Eri standardeilla puolestaan on merkitystä siinä mielessä, että ne pitävät sisällään lakiasiat. Eri maissa on eri käytännöt datan ja yksityisyyden suhteen ja yrityksen olisi hyvä ottaa selvää, missä päin juuri heidän datansa sijaitsee, vaikka tehtävä on vaikea pilven sirpaleisen luonteen vuoksi. Kuten jokaiseen asiaan, myös datan suojaamiseen on olemassa tarkoin kirjattuja standardeja, kuten ISO/IEC 27018, joka ohjeistaa juuri datan suojaamisessa. (CSCC, 2015.)

Identiteettien ja kulun valvonta toistaa hieman lukua 4.3.2, mutta sillä on merkittävä osa datan suojaamista. Jotta dataan pääsee käsiksi, on käyttäjällä ehdottomasti oltava luotettava tapa tunnistautua ja kirjautua sisään sekä ulos palvelusta, jossa käsiteltävää dataa on. Aiemmin samassa luvussa mainittiin käyttäjien valvonnasta ja kyseinen seikka pätee myös datan suojaamiseen. Kun käyttäjistä jää jälki lokitietoihin ja rekistereihin, mitä he ovat tehneet, on helpompi hakea vastuussa olevia käyttäjiä ongelmien ilmetessä. (CSCC, 2015.)

4.4.3 Verkon suojaus

Pilvipalveluiden kohdalla verkon suojaus eroaa muusta it-maailmasta siinä, että palveluntarjoaja ei välttämättä tiedä, minkälaista dataa asiakas lähettää heidän laitteistoonsa. Siksi pilven tarjoajan on pidettävä tietoturvansa ehdottoman korkealla tasolla. Vaikka asiakkaan data olisikin palvelun tarjoajalle vaikeasti suojattavaa, asiakkaan pitäisi odottaa palveluntarjoajaltaan korkeaa ulkoisen tietoturvan tasoa. Pilven tarjoajalta pitäisi odottaa ainakin laadukasta liikenteen seurantaa, hyvää tunkeutumisen havainnointia ja estämistä, sekä varautumista palvelunestohyökkäyksiin. (CSCC, 2015.)

Osa verkkoliikenteestä on taatusti pahanlaatuista ja tätä pyritään torjumaan pääasiassa palomuurien tai ohjelmistojen avulla. Liikenteen valvonnan tehtävänä on luonnollisesti varmistaa, että liikenne pysyy puhtaana. Yrityksen, joka on siirtymässä pilveen, kannattaa ottaa selvää palveluntarjoajan valvontamenetelmistä. Esimerkiksi tuki IPv6-liikenteelle on tulevaisuudessa tärkeä seikka, sillä yhä useammat laitteet tukevat kyseistä protokollaa ja saattavat kiertää tavallisen IPv4-palomuurin hyökkäystä tehdessä. Palveluntarjoajalta on myös hyvä pyytää ns. blokkilistaa, josta käy ilmi estetyn verkkoliikenteen määrä ja osoitteet pilven toimittajan puolelta. (CSCC, 2015.)

Mitä taas tulee tunkeutumisen havainnointiin ja estämiseen, monet palomuurit pitävät nykyään sisällään ns. IDS/IPS (Intrusion Detection System/Intrusion Protection System)-järjestelmiä, joiden tehtävänä on tarkkailla verkkoliikennettä muutenkin kuin lähtöpaikan, osoitteen tai portin perusteella, mitä yksinkertaisemmat ja vanhat palomuurit tekevät. IDS/IPS-laitteet tarkkailevat datavirtaa tuttujen kaavojen kautta, joiden myötä laitteet pystyvät aiempaa tehokkaampaan torjuntaan. Laitteet myös tutkivat itse datan sisällään pitämiä viestejä. Tunkeutumisen estoon osallistuvat osaltaan myös sovellustason välityspalvelimet, kuten esimerkiksi sähköpostien yhdyskäytävät. (CSCC, 2015.)

Palvelunestohyökkäykset koettelevat vähän väliä eri voimakkuuksilla pilvipalveluiden tarjoajia, ja onkin hyvä ottaa selvää, miten eri tarjoajat niitä torjuvat ja miten niistä toivutaan. Palvelunestohyökkäykset ovat luonteeltaan sellaisia, että en saattavat uhata koko yrityksen toimintaa lyhyen aikavälin sisällä. Tämän takia palveluntarjoajan olisi

tehtävä yhteistyötä itse internetoperaattorin kanssa, jotta mahdolliset hyökkäykset torjuttaisiin nopeasti, eikä yritykset kärsisi palvelun alhaalla olosta lainkaan enemmän kuin on välttämätöntä. (CSCC, 2015.)

5 PALVELUNESTOHYÖKKÄYKSET

5.1 Yleistä

Kuten nimestä pystyy jotakuinkin päättelemään, palvelunestohyökkäyksen (DoS, Denial-of-Service) pääasiallinen tarkoitus on estää jonkin internetpalvelun käyttö hyökkäämällä palvelun kimppuun. Palvelun käyttö estetään tukkimalla verkkoliikenne kohteena olevaan palveluun ja seurauksena tästä on palvelun hidastuminen tai sen kaatuminen. Palvelunestohyökkäykset aiheuttavat massiivisia taloudellisia menetyksiä yrityksille, sillä palvelun alhaallaoloaika on aina menetettyä rahaa. Hyökkäyksen kohteena voi olla mikä tahansa internettiin kytköksissä oleva laite ja kohde riippuu täysin siitä, mitkä ovat hyökkääjän motiivit teon suorittamiseen. Suurimmat hyökkäykset saavat laajaa mediahuomiota ja esimerkiksi Suomessa otsikoihin nousee vuosittain esimerkiksi eri pankkeihin tai mediataloihin kohdistuneita palvelunestohyökkäyksiä.

Palvelunestohyökkäykset ovat luonteenomaisia siitä, että hyökkääjät pyrkivät verkkoliikenteen tukkimisella estämään tavallisten palvelun käyttäjien pääsyn palveluun. Hyökkäykset eivät siis esimerkiksi vahingoita palvelun rakennetta tai ohjelmistoa, joskin hyökkäyksen aikana datan sekaan voidaan ujuttaa vahingollista materiaalia. Tilannetta voi verrata esimerkiksi tukkeutuneeseen kulkuväylään konsertissa. Kun väylä yhteen suuntaan tukkeutuu, ei kukaan pääsee etenemään mihinkään tai eteneminen tukoksen ohi on hidasta.

5.2 Tekniikka

Palvelunestohyökkäykset voidaan jakaa karkeasti kolmeen eri tyyppiin, jotka ovat volyymi-, protokolla- ja sovelluskerrosperustaisia. Volyymiperustainen hyökkäys on kaikista yksinkertaisin palvelunestohyökkäyksen muoto. Hyökkääjä vain lähettää useita datapaketteja kohdeosoitteeseen ja näin "vie" käyttöönsä kaikki kohdekoneen resurssit. Resurssit saattavat olla niinkin yksinkertainen asia kuin verkon kaistanleveys tai prosessorin laskentateho. Usein volyymihyökkäyksissä käytetään ICMP- (Internet Control Message Protocol) tai UDP- (User Datagram Protocol) pyyntöjä, jotka on helppo lähettää koneesta toiseen. Monimutkaisempaa palvelunestohyökkäystä edustaa protokollapohjaiset hyökkäykset. Nämä hyökkäykset kohdennetaan ennemmin itse kohdepalvelimen resursseihin (esim. laskentatehon käyttö) kuin sen kaistan tukkimiseen. Protokollahyökkäyksillä voi vaikuttaa myös palvelimen vaikutusalueen laitteisiin, kuten päätelaitteisiin, palomuureihin ja kytkimiin. Kolmantena hyökkäystyyppinä sovelluskerroksen hyökkäykset tähtäävät suoraan sovellukseen lähettämällä verkko- ja kuljetuskerroksen ohi pyyntöjä sovellukselle, tarkoituksenaan kaataa palvelu. Esimerkiksi Apache HTTP -palvelin tai Microsoftin IIS ovat sovellushyökkäysten kohteena. (Null Byte, 2015.)

5.2.1 Hyökkäyksen välineet

Palvelunestohyökkäykset ovat siitä ilkeä hyökkäysmuoto, että niitä on erittäin helppo toteuttaa ja hyökkäyksen voi tehdä kuka tahansa käyttäjä, jolla on pääsy internettiin. Laitteeksi riittää tietokoneen sijaan vaikka älypuhelin tai tabletti. Suuria hyökkäyksiä toteuttaa pääasiassa vain hakkeriryhmät tai järjestöt ja niitä suunnitellaan pitkään, mutta helpoimmillaan palvelunestohyökkäyksen saa toteutettua lataamalla siihen sopiva sovellus koneelle ja asentamalla sen. Sen jälkeen käyttäjän tarvii vain syöttää kohde-IP ja painaa "Start". (Null Byte, 2015.)

Hyökkäyksiä varten on olemassa satoja erilaisia sovelluksia, mutta jotkut ovat nousseet kirkkaasti ylitse muiden. Ehkä kaikista suosituin sovellus palvelunestohyökkäyksen toteuttamiseen on LOIC (Low Orbit Ion Canon). Kyseinen sovellus on helppo asentaa ja se on ilmainen, esimerkiksi hakkeriryhmä Anonymous on toteuttanut tällä

sovelluksella useita hajautettuja palvelunestohyökkäyksiä viime vuosien aikana. Sovelluksen toiminta perustuu UDP-, HTTP- tai TCP-pyyntöjen lähettämiseen kohdepalvelimelle, käyttäjän pitää ainoastaan tietää kohdeosoite ja syöttää se sovellukselle. Loput hoitaa LOIC. Sovellus suunniteltiin alun perin stressityökaluksi verkon kuormittamisen testaamiseksi, mutta sen käyttötarkoitus on sittemmin muuttunut radikaalisti. LOICista on jatkokehitelty uusia versioita, kuten XOIC ja HOIC. Molemmat versiot ovat tehokkaampia LOICiin nähden, esimerkiksi HOIC tehostaa toteutettua hyökkäystä käyttämällä boosteritiedostoja datan lähetykseen. (Shandkhar, 2016.)

Muita laajassa käytössä olevia sovelluksia ovat mm. HULK, RUDY, Tor's Hammer ja PyLoris. HULK (HTTP Unbearable Load King) kaataa tehokkaasti palvelimia, sillä se käyttää hyväkseen salattua palvelimeen menevää liikennettä. HULK lähettää salatun liikenteen seassa satunnaisesti generoituja pyyntöjä, jotka pääsevät kohteeseensa varsin helposti. Sovelluksen kehittäjä testasi luomustaan IIS 7 palvelimeen, jossa oli 4 gigatavua keskusmuistia. Palvelin kaatui alle minuutissa. (Shandkhar, 2016.) RUDY (R-U-Dead-Yet) puolestaan käyttää toiminnassaan hyväksi http-protokollan POST-metodia. Sovellus pyrkii avaamaan suhteellisen vähän yhteyksiä kohdekoneeseen ja pitämään niitä auki niin pitkään kuin mahdollista. Hyökkäykset RUDYlla kestävät yleensä pitkään ja ovat volyymiltaan pieniä. Siksi käynnissä oleva hyökkäys saattaa jopa jäädä huomaamatta. (Incapsula, 2016.) Pythonilla kirjoitettu Tor's Hammer käyttää hyväkseen tavallisen verkon lisäksi myös TOR-verkostoa, joten hyökkääminen kyseisellä sovelluksella on varsin huomaamatonta. Tor's Hammerin hyökkäykset ovat tehokkaita, sillä Apache- tai IIS-palvelimen saa kaadettua sekunneissa sen avulla. (Shandkhar, 2016.) PyLoris on hieman toista maata edellä mainittuihin sovelluksiin nähden, sillä sen pääasiallinen tarkoitus on toimia palvelinten testauksessa, mutta sillä voi toteuttaa myös palvelunestohyökkäyksiä. Sovellus pystyy käyttämään SSL-suojattuja yhteyksiä hyökkäyksissään ja hyökkäykset voivat kohdistua useisiin protokolliin, kuten http, FTP, SMTP ja Telnet. Useista muista palvelunestosovelluksista poiketen PyLoris hyökkää suoraan palvelun kimppuun, ei niinkään sen käyttämään verkkoon. (Shandkhar, 2016.)

5.3 Hajautettu palvelunestohyökkäys

Palvelunestohyökkäyksen monista tekniikoista hajautettu palvelunestohyökkäys (DDoS, Distributed Denial-of-Service) saa kaikista eniten huomiota ja se aiheuttaa myös erittäin usein suurinta vahinkoa kohteelleen. Hajautetussa hyökkäyksessä on yhden laitteen sijaan monta laitetta hyökkäämässä saman kohteen kimppuun. Tämä toteutetaan siten, että hyökkääjä asentaa huomaamatta verkon kautta useisiin koneisiin ohjelmiston, jolla hyökkäys toteutetaan. Sen jälkeen, kun tarpeeksi monta konetta on saastutettu, hyökkääjä aloittaa palvelunestohyökkäyksen kaikista saastuneista koneista yhtä aikaa. Tällaisen hyökkäyksen alkuperää on erittäin vaikea selvittää, jos hyökkääjä osaa reitittää liikenteen monen laitteen kautta. Hyökkääjän käyttämää verkkoa sanotaan zombi- tai bottiverkoksi. Tekniikaltaan hajautettu hyökkäys on samanlainen kuin yksittäinenkin, mutta massiivinen koneiden määrä aiheuttaa suuret vahingot, sillä niiden aiheuttama dataliikenteen määrä on usein mahdoton torjua. Suurimpiin zombiverkkoihin voi kuulua jopa satoja tuhansia saastuneita laitteita. (Shandkhar, 2016.)

Hajautettu hyökkäys suunnataan joko verkkokerrokseen sen ylikuormittamiseksi, tai sovelluskerrokseen, jolloin sitä tykitetään palvelupyynnöillä. Yleensä media huomioi hyökkäyksissä vain ”uhrina” olevan yrityksen ja niiden palvelimille aiheutuneen vahingon, mutta yleensä hajautetussa hyökkäyksessä on myös muita uhreja, kuten yksityiset käyttäjät ja heidän omaisuutensa (saastuneet laitteet). Bottiverkon osana toimiva kone on silti niin pieni palanen isoa hyökkäystä, että koneen käyttäjä ei läheskään aina edes huomaa, että oman koneen verkkoliikenteessä on jotakin ylimääräistä mukana. Salakavalan ja tehokkaan luonteensa ansiosta hajautettu palvelunestohyökkäys on nostettu jopa internetin suurimmaksi uhaksi tietoturvan suhteen. Näin ovat tehneet ainakin tietoturvaan erikoistuneet firmat Kaspersky ja Symantec. (Rouse, 2013.)

5.4 Muut palvelunestohyökkäyksen tekniikat

Edellä mainituissa luvuissa käytiin läpi yleisimmät sovellukset palvelunestohyökkäysten toteuttamiseen sekä yleisesti esitettiin muutama eri toteutustapa. Seuraavassa käydään läpi, millaisia protokollia tai pyyntöjä nuo edellä mainitut tekniikat ja sovellukset

käyttävät pääasiassa ja mitä ne konkreettisesti tekevät hyökkäyksen aikana. Hyökkäykset voidaan toteuttaa ainakin HTTP-, ICMP- ja TCP-protokollalla ja ping-komennoilla käyttämällä niitä eri tavoin.

5.4.1 HTTP Flood

HTTP Flood -hyökkäys toteutetaan POST- ja GET-pyynnöillä. Ne ovat usein hajautettuja, sillä hyökkäävien laitteiden ei tarvitse tehdä muuta kuin lähettää kyseisiä pyyntöjä kohdepalvelimelle. Tästä johtuen POST- ja GET-pyynnöillä toteutetut hyökkäykset ovat usein volyymiperustaisia, nopeita toteuttaa, helppo ylläpitää, eivätkä ne vaadi suurta kaistanleveyttä. Näiden hyökkäysten alustaminen vaatii kuitenkin jonkin verran asiantuntijuutta kohdesivusta tai palvelimesta, sillä niiden on tarkoitus osua sovelluskerrokseen ja liikenteen on kuitenkin kuljettava läpi verkko- ja kuljetuskerroksen onnistuneesti. Yleensä HTTP Flood –hyökkäykset ovat vaikeita estettäviä, sillä POST- ja GET-pyyntöjen blokkaus on haastavaa ja HTTP-liikenne rakentuu niiden varaan, ne käyttävät tavallisia URL-pyyntöjä toimiessaan. (Impreva Incapsula, 2016.)

5.4.2 ICMP-hyökkäykset

ICMP-protokollaa käytetään lähinnä virheilmoitusten lähettämiseen laitteiden, kuten kytkinten ja reittimien välillä. Ne kuvailevat järjestelmässä kohdattuja virheitä ja lähettävät siitä datagramin eteenpäin järjestelmänvalvojille. ICMP:tä käyttää myös kaksi varsin yleistä komentotyökalua: Ping ja Traceroute-komennot. Tänä päivänä verkon valvojat (it-henkilöstö) haluavat useimmiten ottaa ICMP-liikenteen pois käytöstä, sillä sen avulla pystytään toteuttamaan tehokkaita palvelunestohyökkäyksiä lähettämällä joko massiivisia ping-paketteja kohdekoneeseen tai vaihtoehtoisesti päinvastoin hidasta ja lähes huomaamatonta ping-virtaa jatkuvalla syötöllä. (Branch, 2016.)

Yleisimpiä ICMP-hyökkäyksinä voidaan pitää ns. smurf-hyökkäystä, ping floodia sekä BlackNursea. Smurf-hyökkäyksessä (smurffing) lähetettävät datapaketit muodostetaan siten, että ne näyttävät tulevan eri osoitteesta kuin oikeasti. Paketit sisältävät ICMP ping –pyynnön, joka lähetetään IP:n lähetysosoitteeseen (broadcast address), eli halutun palvelimen koko verkkoon. Tämän ping-pyynnön kaiku (echo) suuntautuu

kohdekoneeseen ja näin tukkii verkkoliikenteen, kun pyyntöjä lähetetään sarjana. (Rouse, 2007). Ping flood puolestaan on hyökkäys, jossa kohteeseen lähetetään useita ping-pyyntöjä, ilman, että kohde vastaa niihin takaisin. Hyökkäyksen tarkoituksena on sekä kuluttaa kohdepalvelimen laskentatehoa, että kaistan käyttöä. (Branch, 2016). BlackNurse taas on melko tuore tulokas, sillä se ”havaittiin” vasta vuonna 2016. Kyseisen hyökkäyksen aikana hyökkääjä lähettää alhaisen volyymin (40 000-50 000 pakettia sekunnissa) ICMP-paketteja kohteeseensa, jotka on suunniteltu erityisen tehokkaiksi prosessoreja vastaan. Liikenne ei tuki esimerkiksi palomuureja, sillä se on kevyttä. Isku tapahtuu vasta koneessa. (Khandelwal, S. 2016)

5.4.3 TCP-hyökkäykset

TCP (Transform Control Protocol) –protokolla on kuljetuskerroksen protokolla, ja sitä käyttää hyväkseen muutamat palvelunestohyökkäystekniikat. Shrew attack –nimisenä tunnettu hyökkäys lähettää kohteeseen lyhyitä, vahingollisia datapiikkejä. Dataa lähetetään hitaasti ja se on ajastettu tarkasti siten, että TCP-protokollaan sisällytetty timeout-ominaisuus menettää merkityksensä ja häiritsee näin liikenteen perille pääsyä. Liikenteen seuranta on vaikeaa, sillä se kulkee muun TCP-liikenteen seassa. (Kuzmanovic, 2004.) Niin sanottu slow read –hyökkäys tekee sen, mitä nimestä pystyy päättelemään. Se lähettää sinänsä oikeita pyyntöjä sovelluskerrokseen, mutta pyynnöt luetaan niin hitaasti, että kohdepalvelin täyttyy aktiivisista pyynnöistä, joita ei pystytä suorittamaan loppuun. Hyökkäys on volyymiltaan pieni. (Shekyan, 2012.). Hidas, mutta pitkäkestoinen palvelunestohyökkäys puolestaan voi olla vaarallinen, sillä se syö kohdekoneen resursseja ilman, että hyökkäystä edes huomataan. Tämä tapahtuu avaamalla yhteyksiä kohteeseen ja sen jälkeen avatut yhteydet pidetään auki verkkokerrokseen niin pitkään kuin mahdollista. Hyökkäys ei vaadi juuri tietotaitoa hyökkääjän puolelta ja se onkin helppo käynnistää ja suunnata kohteeseen. (Mendon, 2016.) SYN Flood –niminen hyökkäys aiheuttaa normaaliin tapaan palvelun liikenteen tukkiutumista, mutta tekee sen lähettämällä toteutumattomia SYN (Synchronize)-pyyntöjä kohteeseen. SYN-pyynnöillä avataan yhteyksiä laitteiden välille, ensin kysytään lupa yhteyden muodostamiselle, johon kohdekoneen pitäisi vastata, mutta SYN Floodissa jo lähetysosoite on väärennetty, mistä johtuen kohdekone ei voi lähettää vastausta takaisin kysyjälle. (Impreva Incapsula, 2016.) Hyökkäyksen aikana hyökkääjä

lähettää TCP-pyyntöjä nopeammin kuin mitä vastaanottaja ehtii käsittelemään. SYN Flood voi kuormittaa kohdepalvelimen lisäksi koko sisäverkkoa, johon se on liitetty. (Weiss, 2012.)

5.5 Torjunta ja suojautuminen

Kuten jo aiemmista luvuista on käynyt ilmi, palvelunestohyökkäyksiltä suojautuminen on erittäin hankalaa ja joidenkin hyökkäystekniikoiden osalta jopa mahdotonta, sillä tekniikat käyttävät verkkoyhteyksien rakennuspalikoita toimintaansa. Varmin keino suojautua hyökkäyksiltä olisi katkaista kaikki tietoliikenneyhteydet koneesta ja poistaa niitä ylläpitävät komponentit koneesta. Se taas ei tule kysymykseen missään yrityksessä. Hyökkäysten torjuminen on pitkälti ennakointia ja varautumista siihen, vaikka osan hyökkäyksistä pystytään torjumaan täysin.

Nyrkkisääntöinä voidaan pitää seuraavia asioita: verkkoliikennettä tulisi monitoroida, hyökkäysten varalta, verkkopalvelun tarjoajan tulisi olla yhteydessä internetoperaattoriinsa ja koostaa suunnitelma hyökkäysten varalle. Paras puolustus palvelunestohyökkäystä vastaan on sen huomaaminen ajoissa. Kuten aiemmin todettua, hyökkäysten huomaaminen ei ole aina helppoa. Siksi mm. tietoturvalaitteiston tulisi olla hyvällä tasolla, esimerkiksi osa nykyisistä palomuureista pystyy tunnistamaan haitallisen liikenteen muutenkin kuin vain IP-osoitteen tai porttinumeron kautta. Hyökkäysten varalle tulisi laatia suunnitelma ja koko firman tulisi tietää keinoista, miten hyökkäyksen sattuessa kohdalle toimitaan. Suunnitelmaa ja käytäntöjä pitää harjoitella. (Ferrillo, 2016.)

Yksi vaihtoehto on myös kääntyä palvelunestohyökkäämisen torjuntaan erikoistuneisiin toimijoihin, mutta ne ovat erittäin kalliita – usein yhden hyökkäyksen torjumisesta veloitetaan viisinumeroisia summia - verrattuna siihen, että mahdollinen hyökkäys kestää ehkä päiviä. Mitä taas tulee internetoperaattoriin, he usein pystyvät näkemään, kulkeeko heidän verkkonsa läpi ylimääräistä liikennettä ja heillä pitäisi olla myös laitteisto siihen. Operaattori voi hyökkäyksen sattuessa reitittää liikenteen uudelleen ja näin pyrkiä minimoimaan hyökkäyksen vaikutuksia. Tässä tapauksessa tosin myöskään sivuston/palvelun käyttäjät eivät pääse käsiksi palveluun. Yrityksellä olisi hyvä

olla myös varavaihtoehto internetoperaattorin suhteen, mikäli ensisijainen operaattori epäonnistuu pahoin tehtävässään. (Ferrillo, 2016.)

5.5.1 Laitteisto

Myös yrityksen sisällä voidaan tehdä erilaisia asioita hyökkäysten torjunnan suhteen. Palomuuri on tärkeä osa torjuntaa, ja nykymuurit ovatkin varsin ”älykkäitä” verkkoliikenteen tarkkailun suhteen. Myös reitittimissä on usein NAT (Network Address Translation) -palomuuri, mutta se ei välttämättä suojaa läheskään niin tehokkaasti kuin itse verkkopalvelimen palomuurin tulisi suojata. Verkkoliikennettä voidaan myös tasapainottaa siirtämällä sitä useammalle palvelimelle ja näin saada hieman lisää tilaa kaistaan (mikäli hyökkäys siis kohdistuu vain tiettyihin palvelimiin). Liikenne voidaan ohjata myös pilvipalveluntarjoajalle, jolla on käytössään leveä kaista. (Ferrillo, 2016.)

Yksittäisestä kohteesta tulevan palvelunestohyökkäyksen saa torjuttua sen tekniikasta riippuen eri tavoin. Yksinkertainen keino hyökkäyksen torjumiseen on blokata joko palomuurin tai internetoperaattorin avulla tietystä IP-osoitteesta tulevat HTTP-pyynnöt. Blokkauksen kanssa pitää silti olla tarkkana, ettei vahingossa lyö asiakkaan reittiä lukkoon palveluun. Usein blokkauksen jälkeen asiakas yrittää uudestaan vielä muutamia kertoja minuuttien sisään, mutta mahdollinen hyökkäys voi tulla jo eri IP-osoitteesta. Haitalliset osoitteet kannattaa lisätä omalle mustalle listalle tulevaisuuden varalta. ICMP-hyökkäysten varalle it-laitteisto on kehittynyt jo niin paljon, että niiden torjuminen onnistuu palvelimelta käsin. Palvelimet voidaan konfiguroida tunnistamaan mahdollisia hyökkäyksiä niitä vastaan. Sovellustasolla kehitys on saman suuntaista, sillä ne voivat blokata hyökkäyksen jopa heti kun ne alkavat. (Weiss, 2012)

5.6 Motiivit

Motiivit palvelunestohyökkäysten tekemiseen ovat samoja kuin muussakin maailmassa haitallisten asioiden teossa. Ne liittyvät joko oman edun ajamiseen, kuten kiristykseen, oman firman aseman parantamiseen tai kybersodankäyntiin tai muuten kohteen vahingoittamiseen, kuten vandalismiin ja haktivismiin (hakkerointi aktivismin

muotona). Kirityksen toimiessa motiivina hyökkääjä käyttää usein hajautettua hyökkäystä ja joko tekee ensin pienen kokeilun haluamaansa kohteeseen ja vaatii rahaa tai suurempi hyökkäys tapahtuu. Toinen vaihtoehto on se, että hyökkääjä tykittää palvelun tukkoon suurella datamäärällä ja vaatii rahaa hyökkäyksen lopettamiseksi. Yrityksen ajaessa omaa etuaan hyökkäyksen muotona on usein hajautettu hyökkäys. Tarkoituksena on kaataa vastustajan palvelin ja näin saada asiakkaat hylkäämään kyseinen palvelu ja mahdollisesti siirtää heidät käyttämään omaa palvelua. Yritysten välinen palvelunestäminen ei ole kovin yleistä, mutta se on nousussa. Oman edun ajamisen suurin muoto on kybersodankäynti ja siinä käytetään tarkoituksesta riippuen tekniikkaa kuin tekniikkaa. Yritystasolla ei ole kovin todennäköistä, että sodankäynti yltäisi sinne asti, vaikka toki valtioiden suurimpia yrityksiä se koskettaa. Hyökkäykset ovat tarkoin varjeltuja ja hyvin rahoitettuja. Ne suunnataan joko toisen maan hallintoa vastaan tai omassa maassa hiljentämään valtion vihollisia. (Impreva Incapsula, 2016.)

Kybervandalismi ei sinänsä liity oman edun ajamiseen vaan enemmän kohteen vahingoittamiseen tai kiusantekoon. Yleensä teon takana oleva käyttäjä hyökkää jotakin järjestöä, virastoa tai henkilöä vastaan, koska kokee joutuneensa kokemaan vääryyttä. Vandaalit hyökkäävät usein yhtä konetta käyttäen ja käyttävät valmiiksi tehtyjä sovelluksia ja skriptejä. Haktivismiin osaa ottavat taas tekevät usein oman järjestönsä/organisaationsa kautta laajaa huomiota saavia hyökkäyksiä ja haktivistit julistautuvat erilaisten hyökkäysten tekijöiksi ympäri sosiaalista mediaa. Ehkä tunnetuin haktivistiryhmä on nimeltään Anonymous, joka on maailman median otsikoissa toistuvasti. Ryhmä on virallisesti puolueeton ja se on hyökännyt niin länsimaisten medioiden kuin Isiksenkin kimppuun ja tehnyt myös hakkerointia hyväntekeväisyyden nimissä. Haktivistit hyökkäävät useasti jotakin järjestöä, firmaa tai virastoa vastaan osoittaakseen kritiikkiä kyseisille tahoille. (Impreva Incapsula, 2016.)

6 PALVELUNESTOHYÖKKÄYKSET PILVIPALVELUISSA

Tällä vuosikymmenellä palvelunestohyökkäysten saama mediahuomio on kasvanut moninkertaiseksi aiempiin vuosiin nähden. Hyökkäysten volyymien kasvaessa ne ovat

yhä suurempia ja suurempia ja vaikuttavat tavallisten ihmisen elämään enenevässä määrin. Aivan viimeisen muutaman vuoden aikana mukaan on tullut ns. IoT (Internet of Things) –laitteita, jotka ovat aivan tavallisia kodin välineitä, joilla on pääsy internettiin. Tämän takia kyseiset laitteet ovat myös alttiina kaappauksille ja niitä käytetäänkin paljon bottiverkoissa hyökkäysten toteuttamiseen heikomman tietoturvan takia. Tämä näkyi mm. 2016 syksyllä toteutetussa, historian suurimmassa palvelunestohyökkäyksessä.

6.1 Dyn-hyökkäys 2016

Lokakuun 21. päivänä 2016 tapahtui toistaiseksi suurin palvelunestohyökkäys, mitä tähän mennessä ollaan maan päällä koettu. Hyökkäyksen kohteena oli yhdysvaltalainen Dyn-yhtiö, joka toimii DNS (Domain Name System) –operaattorina. DNS:n pettäessä iso osa internetiä oli alhaalla ja miljoonat käyttäjät ympäri maailmaa huomasivat vaikutuksen. Hyökkäyksen vaikutukset tuntuivat eniten Usa:n itärannikolla (Euroopassa ja muualla Usa:ssa vaikutukset olivat lievempiä) ja useita suuria palveluja kaatui lähes koko päivän ajaksi. Isoja kärsijöitä olivat esimerkiksi Amazon, PayPal, Netflix, Spotify, Reddit, CNN, New York Times, The Wall Street Journal ja The Guardian. Hyökkäyksen tekijöiksi julistautuivat sekä Anonymous että New World Hackers. (Johnston, Thielman, 2016.)

Hyökkäys toteutettiin hajautettuna palvelunestohyökkäyksenä ja siinä oli mukana arviolta yli 100 000 saastunutta laitetta. Massiiviseen hyökkäykseen käytettiin Mirai-nimistä bottiverkkoa, joka on koostettu sadoista tuhansista IoT-laitteista. Hyökkäys suunnattiin ainoastaan Dynin DNS-palvelimiin ja ne tulivat kolmessa aallossa. Hyökkäjien kohde itse on kriittinen koko internetin toiminnalle, sillä Domain Name System kääntää numeromuodossa olevat IP-osoitteet itse domain-nimiksi ja mahdollistaa näin osoitteiden kirjoittamisen monimutkaisten numerosarjojen muistamisen sijaan. DNS:n tehtävänä on siis nimetä koneita verkossa ja se on yksi internetin toiminnan kulmakivistä. Dyn hoitaa suurinta osaa maailman DNS-toiminnasta ja varsinkin Usa:ssa sillä on suuri merkitys ihmisten netin selaamiseen. (Woolf, 2016.)

Hyökkäyksen jälkimainingeissa on noussut esille IoT-laitteiden aiheuttama tietoturvauhka. IoT-laitteet kun ovat arkipäiväisiä esineitä internetyhteydellä varustettuna, kuten kameroita, konsoleita tai soittimia. Dyn-hyökkäyksen jälkeen firman asiantuntijat totesivat, että todellista puolustuskeinoa tällaista hyökkäystä vastaan ei ole sen lisäksi, että hyökkäyksen tekijöitä ei välttämättä saada koskaan kiinni. Sen verran tekijästä pystyttiin päättelemään, että mikään valtio ei ole iskun takana. Se on samalla lisähuoli, sillä jonkun valtion rahoituksella pystyttäneen tekemään vielä paljon isompi hyökkäys. Tietoturvariskiä lisää vielä se, että hyökkäyksessä käytetyn Mirai-verkon lähdekoodi julkaistiin kaikkien saataville aiemmin viime lokakuussa. Tämä tarkoittaa sitä, että lähitulevaisuudessa vastaavanlaisia iskuja tultaneen näkemään enenevässä määrin ja torjuntamekanismien puuttuessa ne ovat varsin tuhoisia. (Woolf, 2016.)

6.2 Hyökkäykset Ruotsiin

Ruotsin mediat ja virastot ovat saaneet osakseen suuria palvelunestohyökkäyksiä, joihin myös Dyn-hyökkäys vaikutti osan siitä kohdistuessa Ruotsin kuninkaalliseen perheeseen. Myös vuosina 2012 ja 2016 varsinkin paikalliset suurmediat saivat osakseen isoja iskuja. 5. lokakuuta 2012 Anonymous hyökkäsi ruotsalaisia virastoja (mm. hallituksen sivuja, poliisia ja pankkeja) vastaan noin kello 14:30, tuntia ennen etukäteen ilmoitettua hyökkäysajankohtaa. Hyökkäys toteutettiin sql-käskyjä käyttämällä ja teon motiivina epäiltiin olleen poliisin PRQ:n palvelinsaliin tekemän kotietsinnän kostaminen sekä Julian Assangen pidätysmääräys. (Konttinen, 2016.)

19. maaliskuuta 2016 useat ruotsalaiset suurmediat, kuten Aftonbladet, Dagens Nyheter, Expressen, Svenska Dagbladet sekä Sydsvenskan joutuivat suurten palvelunestohyökkäysten kohteeksi. Hyökkäys oli hyvin järjestelmällinen ja merkit viittasivat siihen, että data tulee Venäjältä. Ruotsalaisissa medioissa oli hieman aikaisemmin julkaistu Venäjän vakoiluun liittyviä raportteja ja hyökkäysten motiivi liittyi todennäköisesti kyseisiin julkaisuihin. Twitteristä löytyi ennen hyökkäyksiä viesti, jonka mukaan ”seuraavien päivien hyökkäykset tähdätään hallitukseen ja mediaan, jotka jakavat väärää informaatiota.” (Konttinen, 2016.)

6.3 OP-Pohjolan hyökkäys 2014-15

Uudenvuoden aattona 2014 Osuuspankin pankkipalveluihin kohdistettiin palvelunestohyökkäys, joka jumitti liikenteen täysin loppupäivän ajaksi. Verkkoliikenteen ongelmat kuitenkin jatkuivat vielä lähes viikon tämän jälkeen ja 3.1.2015 OP ryhtyi rajoittamaan ulkomailta tulevaa dataliikennettä parantaakseen palveluidensa toimivuutta. Vahingollista dataa OP:n palvelimille tuli sekä kotimaasta että ulkomailta ja pankki avasi avustuspuhelimen pelkästään hyökkäyksen takia. (Konttinen, 2016.)

Suurta närää hyökkäyksessä aiheutti se, että se esti OP-ryhmään rekisteröityjä pankkikortteja toimimasta automaateilla tai maksupäätteissä. Asiakaskunta ihmetteli, miksi kortit olivat sidonnaisia verkkopankkien järjestelmiin siten, että palveluestohyökkäys pystyi kaatamaan sekä käteisnostot että päätemaksamisen. Tämä esto johtui siitä, että pankkikortteihin liitetyt järjestelmät käyttivät samoja järjestelmän komponentteja kuin hyökkäyksen kohteeksi joutuneet palvelimet. Teoista otettiin kiinni kaksi nuorta helsinkiläismiestä ja heidän syytteisiinsä lukeutuivat törkeä tietoliikenteen häirintä sekä törkeä kiristysyritys. (Konttinen, 2016.)

7 OHJEITA YRITYKSELLE

Jo edellä olevissa luvuissa on todettu palvelunestohyökkäysten torjumisen vaikeus niiden monimuotoisuuden ja tehokkuuden takia. Tässä työssä käytetyt lähteet ovat olleet lähes kaikki pohjois-amerikkalaisia ja Usa:ssa ongelmat ovatkin hyökkäysten kanssa suurempia mitä Euroopassa ja erityisesti Suomessa. Silti, myös täällä yritykset joutuvat palvelunestohyökkäysten kohteeksi, joskin pienemmässä määrin kuin Keski-Euroopassa tai Atlantin toisella puolella. Suomessa kohteina ovat olleet pääasiassa pankit ja suuret mediat. Valmius hyökkäysten torjumiseen etenkin internetoperaattoreilla on hyvällä tasolla, vaikka uhka onkin muuhun maailmaan verrattuna pieni täällä Pohjolassa. Yritysten varautumisen taso palvelunestohyökkäyksiin sen sijaan vaihtelee.

7.1 Yleistoimet

Yrityksen tulisi varmistua, että tietoturva on kaikin puolin ajanmukainen. Hyvä yleistietoturva luo perustaa myös palvelunestohyökkäysten torjumiseen ja luvussa kaksi kuvattuja toimia tulisi soveltaa yrityksen toimintaan. It-henkilöstön tulee olla perillä yrityksen sisällä kulkevasta verkkoliikenteestä, kuten kaistan käytöstä sekä eri protokollien toimivuudesta. Tämä auttaa hyökkäystilanteessa, sillä verkon monitoroinnilla saavutettu tieto auttaa nopeammin osoittamaan, onko käynnissä mahdollinen hyökkäys. Monitorointi paljastaa myös liikenteen alkuperän ja mihin porttiin liikenne kulkee.

Mitä tulee verkon suojaukseen, VPN:n käyttöönotto saattaa helpottaa hyökkäystilanteissa, sillä firman sisäisessä verkossa voidaan toimia erikseen VPN:n avulla. Hyökkäyksestä kärsivän yrityksen asiakkaille siitä ei ole iloa, mutta itse työntekijät saavat tehdä töitään sen minkä VPN:n avulla voivat. Verkkoratkaisut tulisi muutenkin toteuttaa niin, että itse palvelut ovat erillään työstettävästä datasta, sillä se vähentää palvelunestohyökkäyksen taloudellisia haittavaikutuksia. Mahdollista hyökkäystä varten tulisi olla valmiina myös yksityiskohtainen suunnitelma, sillä tulevaisuudessa palvelunestohyökkäykset yleistyvät myös suomalaisissa yrityksissä. Varsinkin it-henkilöstön tulee olla perillä siitä, millaisia tekniikoita hyökkääjät mahdollisesti käyttävät sekä miten eri hyökkäystyyppejä torjutaan. Suunnitelmaan kuuluu myös yhteistyö internetoperaattorin kanssa.

Palvelunestohyökkäyksille on luonteenomaista, että hyökkääjä vaihtelee ja väärentää ip-osoitteita vaikeuttaakseen uhrin puolustamista. Puolustamista vaikeuttaa myös se, jos hyökkääjä tauottelee hyökkäystään ja jatkaa jonkin ajan kuluttua uudestaan, uudelleen reititetyllä ja organisoidulla hyökkäyksellä. Tämä tosin antaa myös uhrille aikaa valmistautua uuteen datapiikkiin. Yhtäjaksoisen hyökkäyksen torjuminen on helpompaa, sillä liikennettä saadaan usein suodatettua ajan myötä pois kohteesta esimerkiksi internetoperaattorin avustuksella. (Konttinen, 2016.)

7.2 Laitteisto

Firman it-laitteistoon sekä sovelluksiin tulisi asentaa uusimmat päivitykset, sillä korjaustiedostot lisäävät ominaisuuksien ja toimivuuden parantamisen lisäksi myös tietoturvapäivityksiä. Nuo päivitykset pätevät myös palvelunestohyökkäysten kohdalla ja esimerkiksi TCP/IP-protokollaa käyttäviä hyökkäyksiä on onnistuttu blokkaamaan pelkkien ohjelmistopäivitysten avulla. Myös palvelukapasiteettia voidaan mitoittaa ylimittaiseksi tarkoituksella, jotta hyökkäyksen laajuus ei vaikuttaisi koko yrityksen toimintaan niin paljoa, että se esimerkiksi kaatuisi. Hyökkäyksen ollessa päällä sen kohteeksi joutuneen palvelimen tulisi vähän kerrallaan menettää palvelutasoaan, eikä romahtaa kerralla. Myös varayhteyksien tulee olla helposti saatavilla, sillä hyökkäys alkaa usein ilman mitään ennakkovaroitusta. Varayhteyksien avaaminen on hyvä ensiaputoimi ja niiden tulee olla valmiiksi määriteltyinä. (Konttinen, 2016.)

Sovelluskerrokseen kohdistuvat hyökkäykset poikkeavat muista hyökkäyksistä siten, että ne ovat yleensä alhaisemmalla volyymilla tehtyjä ja ne tähdätään tarkasti. Siksi myös suojaus tulee suunnitella niitä varten erikseen. Suojaus hoidetaan firman sisäisesti ja sen päätukijalka on tarkka paketinvalvonta, miten data käyttäytyy sovelluskerroksessa ja mistä se tulee. Koko sovelluskerroksen toimintaa tulee monitoroida, jotta hyökkäykset saadaan torjuttua. (Sockrider, 2013.)

7.3 Internetoperaattorin rooli

Operaattoreilla on hyvin usein suuri rooli palvelunestohyökkäyksien torjumisessa ja suomalaiset internetoperaattorit tarjoavat torjuntapalveluja pienyrityksistä alkaen aina maan suurimmille firmoille asti. Kun yritys sopii verkkoyhteyden toimittamisesta operaattorin kanssa, puheeksi tulee ottaa myös palvelunestohyökkäykset ja sopia toimintatavoista hyökkäystilanteessa. Hyökkäyksen tullessa vastaan operaattori voi reitittää hyökkäyksen (ja samalla muun yritykseen menevän liikenteen) suoraan roskakoriin (ns. null point). Tämä tietenkin estää kaiken palvelun käytön, mutta nollaa myös hyökkääjän toimet. Operaattoreilta on myös saatavilla ohjelmistoja haittaliikenteen poistamiseen ja heidän kautta kulkevaan verkkoliikenteeseen voidaan asentaa tunniste, minkä ansiosta ip-osoitteet eivät näy maailmalle, vaan liikenne kulkee sekä sisään että

ulos yrityksestä vain kotimaan sisällä. Operaattorin vastuusta palvelunestohyökkäyksien kanssa tulee kirjoittaa kirjallinen sopimus. (Konttinen, 2016.)

Mikäli operaattorin kanssa ei olla päästy sopuun hyökkäystilanteista, voivat jotkut pilven tarjoajat tarjota ekstrakaistaa lyhyelle aikavälille, jotta hyökkäyksen vaikutus pienenisi. Mm. Microsoft Azure ja Amazon Web Services ovat tällaisia palveluja, joilta voi pyydettäessä saada apua. Tästä ratkaisusta on iloa lähinnä SaaS- ja ehkä hieman vähemmän PaaS-palvelumallia käyttäville yrityksille. Tämänkaltaiset ratkaisut ovat hyvä kompromissi sellaisille yrityksille, jotka eivät ole valmiita lisäämään omaa kaistaansa pelkästään hyökkäysuhan takia, sillä lisätty kaista on aina uusi kulu yritykselle. Ylimääräisen kaistan käyttö tulee silti ajoittaa tarkasti, koska pilvipalveluiden tarjoajat perivät suuria summia lisäkaistoista eikä kaistan lisääminen välttämättä edes auta, jos hyökkäys on laajamittainen. Lisäksi Azure ja Amazon ovat alttiita hyökkäyksille siinä missä heidän asiakkaansakin. (Chapple, 2013.)

7.4 Yhteenveto

Loppupäätelmänä voidaan todeta, että hyökkäysten torjumisessa suurimman hyödyn saa yhdistelemällä eri torjuntatoimia yhteistyössä internetoperaattorin kanssa. Mikäli hyökkäyksiä yrittää torjua ilman operaattoria, vaatii se suurta rahallista panostusta itse firmalta. Kaistaa tulisi olla mieluummin enemmän, mitä normaaliin liikenteeseen tarvitaan ja varayhteyksien tulee olla helposti avattavissa. Ennalta ehkäisevänä ominaisuutena liikenteen monitorointi ja nopea tiedonvälitys ovat avainasemassa. Ennakointi on paras puolustus palvelunestohyökkäyksiä vastaan. Lisäksi firman henkilöstön tulee tietää, miten työnteko muuttuu, jos hyökkäys osuu kohdalle, jotta taloudelliset menetykset jäisivät mahdollisimman pieniksi.

8 TULEVAISUUS

Yleisesti ottaen voidaan todeta, että pilveen kohdistuvat palvelunestohyökkäykset tulevat lisääntymään tulevien vuosien aikana kiihtyvään tahtiin, sillä tekniikka niiden tekemiseen sekä helpottuu että halpenee. Suurimman uhan tullee aiheuttamaan IoT-laitteiden valtava tulva, ja mikäli niiden tietoturvaa ei paranneta, tulemme näkemään massiivisia hyökkäyksiä IoT-laitteista muodostetuilla bottiverkoilla. Puolustustekniikoissa tapahtuu koko ajan kehitystä, mutta myös hyökkääjät parantavat omia menetelmiään. Tämä kilpajuoksu kehityksessä tarkoittaa sitä, että myös jatkossa palvelunestohyökkäysten torjuminen tulee olemaan haasteellista sen kohteeksi joutuville tahoille.

8.1 Internet of Things

Kuten jo luvussa 6.1 todettiin, Dyn-hyökkäyksessä käytetty Mirai-bottiverkko oli rakennettu yli 100 000 esineiden internettiin kuuluvasta laitteesta, jotka olivat pitkälti nettikameroita, joissa tietoturva on olematon. Dyniin kohdistunutta iskua voidaan pitää tulevaisuuden hyökkäyksien esiasteena, sillä hyökkääjille IoT-laitteet ovat valtava mahdollisuus, koska tänä päivänä laitteita on arviolta noin 6,4 miljardia ja vuoteen 2020 mennessä jopa 20 miljardia. Parannukset niiden tietoturvaan ovat välttämättömiä, sillä koko internet saattaa olla vaarassa kaatua jossakin kohtaa tulevaisuutta, mikäli bottiverkot jatkavat kasvamistaan. Noin 70% IoT-laitteista on jo nyt vakavia tietoturvaheikkouksia. Yrityskäytössä IoT-laitteiden käyttöä tulee miettiä erityisellä varovaisuudella myös tulevaisuudessa. IoT-laitteiden uhkiin kuuluu mm. heikko salaus, viruksen torjunnan puute sekä mahdollisten uhkien havainnointi sekä ennaltaehkäisy ongelmatilanteissa. Yksi suuri ongelma laitteissa on myös se, että suuri osa käyttäjistä pitää laitteita automaattisesti turvallisina. (Raware, 2016.)

Ääriesimerkkinä tulevaisuuden palvelunestohyökkäyksistä on terveydenhuoltopiirien pilveen tehtävät iskut. Joulukuussa 2016 brittimedia The Register uutisoi, että eräät

uusista sydämentahdistimista ovat alttiita palvelunestohyökkäyksille, jotka voivat hyvin olla hengenvaarallisia potilaalle. Uutisen mukaan tutkijaryhmä oli ryhtynyt tutkimaan tahdistimia ilman mitään ennakkotietoa niistä. He olivat onnistuneet mallintamaan tahdistimet ja näin saaneet selville niiden toimintaperiaatteen. Tahdistimien tiedonsiirto oli suojaamatonta ja se mahdollistaa esimerkiksi palvelunestohyökkäyksen tekemisen suoraan tahdistimeen. Näillä hyökkäyksillä – joita kutsutaan elämänestohyökkäyksiksi - voidaan käytännössä tappaa potilas. (Pauli, 2016.)

8.2 Yleisemmin hyökkäysten muuttumisesta

Hyökkäykset tulevat muuttumaan tarkemmin organisoiduiksi ja ajoitetuiksi, mitä tähän mennessä ollaan nähty. Hyökkäyksillä tullaan koettelemaan lähes kaiken kokoisia firmoja ja virastoja, mutta varsinkin suuriin internetin kulmakiviin tullaan tähtäämään enemmän iskuja. Muutamana viime vuonna nähdyt suuret hyökkäykset ovat olleet ikään kuin kokeiluja siitä, millaisia puolustusmekanismeja hyökkäyksen uhreiksi joutuvilla tahoilla on ja kuinka helposti heidän palvelunsa saadaan alas. Todennäköisesti Dyn-hyökkäyksen kaltaisia iskuja tehdään lähivuosina useammin ja koko internetin palvelukapasiteettia koetellaan. Tämän kokoisten iskujen tekijöinä voi hyvin olla hakkeriryhmien sijaan valtiot ja niillä on myös taloudelliset mahdollisuudet suuriskujen tekoon. (Turton, 2016.)

LÄHTEET

Bloor ,R., Halper ,F., Hurwitz ,J. & Kaufman ,M. 2016. How to Use Virtualization with Cloud Computing. Viitattu 2.1.2017 Saatavissa: http://www.dummies.com/how-to/content/how-to-use-virtualization-with-cloud-computing.html

Branch, D. 2016. ICMP: The Good, The Bad and The Ugly. Viitattu 16.1.2017. Saatavissa: https://blog.securityevaluators.com/icmp-the-good-the-bad-and-the-ugly-130413e56030#.rsf9aaspu

Butler ,B. 2013. PaaS primer: What is platform as a service and why does it matter? Viitattu 2.1.2017. Saatavissa: http://www.infoworld.com/article/2613027/paas/paas-primer--what-is-platform-as-a-service-and-why-does-it-matter-.html

Chapple, M. 2013. The Three Elements of Defense Against Denial-of-Service Attacks. Viitattu 7.2.2017. Saatavissa: http://www.biztechmagazine.com/article/2013/02/three-elements-defense-against-denial-service-attacks

Chickowski Erica, 2015. 10 Security Questions To Ask A Cloud Service Provider. Viitattu 7.1.2017. Saatavissa : http://www.darkreading.com/informationweek-home/10-security-questions-to-ask-a-cloud-service-provider/d/d-id/1320377?image_number=2

Cloud Standards Customer Council, 2015. Security for Cloud Computing: 10 Steps to Ensure Success. Viitattu 7.1.2017. Saatavissa: http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Dignan, L. 2016. Brexit spells turbulence for cloud computing: six stormy scenarios. Viitattu 26.1.2017. Saatavissa: http://www.zdnet.com/article/brexit-spells-turbulence-for-cloud-computing-6-stormy-scenarios/

Ellingwood, J. 2015. Seven Security Measures to Protect Your Servers. Viitattu 25.1.2017. Saatavissa: https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers

Ferillo, P. 2016. Defending Your Network Against DDoS Attacks. Viitattu 17.1.2017. Saatavissa: https://www.tripwire.com/state-of-security/security-awareness/defending-your-network-against-ddos-attacks/

Impreva Incapsula, 2016. R.U.D.Y. (R.U-Dead-Yet?). Viitattu 13.1.2017. Saatavissa: https://www.incapsula.com/ddos/attack-glossary/rudy-r-u-dead-yet.html

Impreva Incapsula, 2016. HTTP Flood. Viitattu 16.1.2017. Saatavissa: https://www.incapsula.com/ddos/attack-glossary/http-flood.html

Impreva Incapsula, 2016. TCP SYN Flood. Viitattu 17.1.2017. Saatavissa: https://www.incapsula.com/ddos/attack-glossary/syn-flood.html

Interroute 2015. What is SaaS. Viitattu 2.1.2017. Saatavissa:

http://www.interoute.com/what-saas

Johnston, C. Thielman, S. 2016. Major cyber attack disrupts internet service across Europe and US. Viitattu 22.1.2017. Saatavissa: https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

Kelvin 2014. Basic Overwiev on Cloud Computing. Viitattu 2.1.2017 Saatavissa: http://www.hostdepartment.com/blog/wp-content/uploads/2014/07/plan.jpg

Khandelwal, S. 2016. Even A Single Computer Can Take Down Big Servers Using BlackNurse Attack. Viitattu 16.1.2017. Saatavissa: http://thehackernews.com/2016/11/dos-attack-server-firewall.html

Konttinen, H. 2016. Palvelunestohyökkäys. Viitattu: 31.1.2017. Saatavissa: https://www.secmeter.com/turvatieto/palvelunestohyokkays.html

Kuzmanovic, A. 2004. Shrews: Low-Rate TCP-Targeted Denial of Service Attacks. Viitattu 16.1.2017. Saatavissa: http://www.cs.northwestern.edu/~akuzma/rice/shrew/

Legal Information Institute, 44 U.S. Code § 3542 – Definitions. Viitattu 22.12.2016 Saatavissa: https://www.law.cornell.edu/uscode/text/44/3542#

Loeffler ,B. 2011. Cloud Computing: What is Infrastructure as a Service. Viitattu 2.1.2017. Saatavissa: https://technet.microsoft.com/en-us/magazine/hh509051.aspx

Mendon, S. 2016. Slow DOS Attack: Why It Is Dangerous and How to Detect Using a SIEM. Viitattu 25.2.2017. Saatavissa: http://paladion.net/how-to-detect-slow-dos-attack-using-siem/

Mell ,P Grance ,T. 2012 The NIST Definition of Cloud Computing. Viitattu 2.1.2017. Saatavissa: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Null Byte, 2015. Denial-of-Service (DoS) Tools & Techniques. Viitattu 12.1.2017 Saatvissa: http://null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699/

Orlowski, A. 2016. It's Brexploitation! Microsoft punishes UK for Brexit with cloud price-gouging. Viitattu 26.1.2017. Saatavissa: http://www.theregister.co.uk/2016/12/02/its_brexploitation_microsoft_punishes_uk/

Paasisafad.com ,2013. PaaS Triangle Graphic. Viitattu 2.1.2017. Saatavissa: http://paasisafad.com/wp-content/uploads/2013/03/paas_triangle_graphic.png

Pauli, D. 2016. Fatal flaws in ten pacemakers make for Denial-of-Life attacks. Viitattu 14.2.2017. Saatavissa: http://www.theregister.co.uk/2016/12/01/denial_of_life_attacks_on_pacemakers/

Radware, 2016. Internet of Things or Internet of Threats? Viitattu 15.2.2017. Saatavissa: https://blog.radware.com/security/2016/11/internet-things-internet-threats/

Rouse, M. 2013. Definition distributed denial-of-service attack (DDoS). Viitattu 15.1.2017. Saatavissa: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Rouse, M. 2007. Definition smurfing. Viitattu 16.1.2017. Saatavissa: http://searchsecurity.techtarget.com/definition/smurfing

SANS Policy Team, 2014. Workstation Security (For HIPAA) Policy. Viitattu 22.12.2016. Saatavissa: https://www.sans.org/security-resources/policies/server-security/pdf/workstation-security-for-hipaa-policy

Shankdhar, P. 2016. DOS Attacks and Fre DOS Attaking Tools. Viitattu 12.1.2017. Saatavissa: http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

Shekyan, S. 2012. Are you ready for slow reading? Viitattu 17.1.2017. Saatavissa: https://blog.qualys.com/securitylabs/2012/01/05/slow-read

Sockrider, G. 2013. Seven essentials for defending against DDoS attacks. Viitattu 10.2.2017. Saatavissa: http://www.csoonline.com/article/2133613/malware-cybercrime/7-essentials-for-defending-against-ddos-attacks.html

Stirckland ,J. How Cloud Computing Works. 2.1.2017 Saatavissa: http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm

Tutorials Point, 2016. Network Security – Overview. Viitattu 27.12.2016 Saatavissa: https://www.tutorialspoint.com/network_security/network_security_overview.htm

Turton, W. 2016. Today's Brutal DDoS Attack Is the Beginning of a Bleak Future. 16.2.2017. Saatavissa: http://gizmodo.com/todays-brutal-ddos-attack-is-the-beginning-of-a-bleak-f-1788071976

Weiss, A. 2012. How to Prevent DoS Attacks. Viitattu 18.1.2017. Saatavissa: http://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html

Woolf, N. 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. Viitattu 22.1.2017. Saatavissa: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet