Seppo Honkanen

Palvelunestohyökkäykset tietoturvauhkana

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

6.5.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Seppo Honkanen Palvelunestohyökkäykset tietoturvauhkana 31 sivua + 1 liitettä 6.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	yliopettaja Matti Puska

Insinöörityön tavoitteena oli tutkia palvelunestohyökkäysten tarkoitusperiä, perehtyä niiden torjuntaan ja tutkia niiden yleistymistä Suomessa. Lisäksi työssä käsiteltiin myös lyhyesti muita yleisiä tietoturvauhkia, joita yritykset, yhteisöt ja muut organisaatiot toimintansa yhteydessä kohtaavat.

Palvelunestohyökkäyksiä on viime aikoina tehty monille suurille www-sivustoille ja ne ovat saaneet myös merkittävää julkisuutta. Palvelunestohyökkäykset ovat melko yleinen tapa aiheuttaa vahinkoa yritysten julkisuuskuvalle tai estää yrityksen verkkopalveluiden käyttöä. Osaavalle käyttäjälle palvelunestohyökkäys on melko helppo ja edullinen toteuttaa.

Palvelunestohyökkäysten yleistymistä Suomessa tutkittiin tutustumalla Suomen Viestintäviraston alaisen tietoturvaviranomaisen CERT:n tiedotteisiin palvelunestohyökkäyksiä koskien. Hyökkäysten yleistymistä tutkittiin analysoimalla CERT:n julkaisemien tietoturvatiedotteiden määriä eri vuosien aikana.

Tutkimuksen perusteella palvelunestohyökkäykset eivät ole viime vuosien aikana lisääntyneet merkittävästi verrattuna muihin tietoturvauhkiin. Palvelunestohyökkäykset ovat kuitenkin toiseksi yleisin uhka tietoturvalle ja palvelunestohyökkäyksiin varautumisen todettiin olevan tarpeellista yrityksille ja organisaatioille niiden toiminnan turvaamiseksi.

Avainsanat	palvelunestohyökkäys, tietoturva, CERT

Author	Seppo Honkanen
Title	Denial of Service attacks as a threat to network security
Number of Pages	31 pages + 1 appendices
Date	6 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Information Networks
Instructor	Matti Puska, Principal Lecturer

The aim of this thesis is to study Denial of Service (DoS) attacks and determine how the attacks can be prevented. Additionally, some of those network security threats which companies or organizations nowadays face are briefly covered.

Major websites have recently been targets of Denial of Service attacks with a receiving high publicity. DoS attacks are a common way to cause harm for the public image of a company or prevent the use of network services. For a talented user, a DoS attack is a quite easy and inexpensive to put into practice.

The announcements of the National Cyber Security Centre operating under the Finnish Communications Regulatory Authority regarding Denial of Service attacks are studied in this thesis. Through this material the change of the frequency of the DoS attacks over time is evaluated.

Based on the study, the number of Denial of Service attacks has not increased recently when compared to other network security threats. Nevertheless, Denial of Service attacks are the second most common network security threat and preventing them is considered to be worth the effort in order to secure the operations of companies and organizations.

Keywords	denial of service attack (DoS), network security, CERT

Sisällys

Lyhenteet

Boink	Palvelunestohyökkäyksiin käytettävä työkalu. Paranneltu versio Bonk-työkalusta.
Bonk	Palvelunestohyökkäyksiin käytettävä työkalu, jonka toiminta perustuu TCP/IP pakettien muokkaukseen. Muokatut paketit ylikuormittavat hyökkäykseen kohteen.
Bottiverkko	*Botnet*. Hyökkääjän kaappaamien tietokoneiden verkosto.
CERT	*Computer Emergency Responce Team*. Suomessa CERT-FI on Viestintäviraston alainen tietoturvaviranomainen, joka tutkii ja havaitsee tietoturvaloukkauksia sekä tiedottaa erityyppisistä tietoturvauhista.
DNS	*Domain Name System*. Nimipalvelujärjestelmä Internetissä, joka muuttaa verkkotunnukset IP-osoitteiksi.
DoS	*Denial of Service*. Palvelunestohyökkäys
DDoS	*Distributed Denial of Service*. Hajautettu palvelunestohyökkäys
ICMP	*Internet Control Message Protocol*. TCP/IP-mallissa IP-kerroksen päällä toimiva kontrolliprotokolla.
ICT	*Information and Communication Technology.* Tieto- ja viestintätegnologia.
IRC	*Internet Relay Chat.* Suosittu pikaviestinpalvelu, jolla käyttäjät voivat reaaliaikaisesti viestiä keskenään.
TCP/IP	*Transmission Control Protocol / Internet Protocol.* Internetissä käytettävä verkkoprotokollayhdistelmä.
Teardrop	Palvelunestohyökkäyksiin käytettävä työkalu, jonka toiminta perustuu kohdekoneen muistin ylikuormittamiseen.

UDP	*User Datagram Protocol*. Yhteydetön tiedonsiirtoprotokolla, jota käytetään esimerkiksi DNS-pyyntöjen lähettämiseen.
WWW	*World Wide Web.* Internetin käytetyin palvelumuoto

1 Johdanto

Tietoturva on vakiintunut tärkeäksi osaksi yritysten ja yhteisöjen toimintaa. Palveluliiketoiminta on soveltuvilta osin kokonaan verkoissa tai siirtymässä sinne. Monien tuotantoyritysten viestintä, myynti ja asiakaspalvelutoiminnot tapahtuvat verkossa. Myös yhdistysten ja erilaisten etujärjestöjen toiminnasta suuri osa tapahtuu verkossa.

Verkkoon siirtynyt toiminta on mahdollistanut uudentyyppisten uhkien syntymisen. Verkossa tapahtuvaa viestintää voidaan vääristää, sitä voidaan hidastaa tai se voidaan joissain tapauksissa estää kokonaan. Tällaisen toiminnan motiivina voi olla lähes mikä tahansa aina satunnaisesta kokeilunhalusta sotilaalliseen toimintaan asti.

Järjestelmissä on erityyppisiä haavoittuvuuksia, joita hyödyntämällä pyritään aiheuttamaan haittaa näiden järjestelmien haltijoille. Haavoittuvuuksia hyödyntävät paitsi tietokoneharrastajat, myös tiedustelutoiminta tai ammattimaiset rikolliset.

Monista tieturvauhista palvelunestohyökkäykset ovat tänä päivänä merkittävä riski monille yrityksille ja yhteisöille, koska niiden toteuttaminen on kohtuullisen helppoa ja siksi niitä voidaan toteuttaa ilkivaltatyyppisesti, varsin vähäisiin syihin perustuen. Palvelunestohyökkäykset aiheuttavat järjestelmien ylläpitäjille paljon ylimääräistä työtä ja myös taloudellisia menetyksiä.

Tämän työn tarkoituksena on selvittää Suomen Viestintäviraston alaisen tietoturvaviranomaisen CERT:n (Computer Emergency Responce Team) tiedotteisiin perustuen palvelunestohyökkäysten yleistymistä. Samoin työssä esitetään erilaisia löydettyjä tapoja torjua palvelunestohyökkäyksiä sekä niiden toimivuutta. Lisäksi työssä kuvataan erilaisia keinoja minimoida palvelunestohyökkäysten aiheuttamia haittoja yhteisöille tai yrityksille.

2 Tietoturvallisuuden peruskäsitteitä

2.1 Tietoturvan lähtökohdat organisaatiossa ja yrityksissä.

Organisaatiot ja yritykset kohtaavat nykypäivänä entistä enemmän erityyppisiä verkkouhkia. Verkkouhat ovat kasvaneet tekniikan yleistyessä entistä enemmän, ja yritysten hyvä tietoturvasuunnittelu onkin hyvin tärkeä osatekijä koko yrityksen toimivuuden kannalta. [2.]

2.1.1 Tietoturvapolitiikka

Tietoturvasuunnittelun tärkeä osa on luoda organisaatiolle tarkka tietoturvapolitiikka, joka muodostuu ylimmän johdon tavoitteista ja käytännöistä tietoturvallisuuden saavuttamiseksi. Tietoturvapolitiikassa kuvataan yleisellä tasolla, mikä on organisaation tai yrityksen liiketoiminnan kannalta tarvittava tietoturva-aste, miten tälle asteelle päästään ja miten tietoturvaa ylläpidetään sekä kehitetään edelleen. Tietoturvapolitiikka on organisaation tieto- ja viestintäpolitiikan (ICT-politiikka) osa, mutta sen laatiminen on ylimmän johdon vastuulla. [8; 14.]

Tietoturvapolitiikkaan ei ole tarkoitus sisällyttää tietoturvallisuuden toteuttamiseen liittyviä teknisiä ratkaisuja, ja se tarkistetaan yleensä noin vuosittain, jotta se vastaisi parhaiten sen hetkistä turvallisuuden tarvetta. Tietoturvapolitiikassa määritetään käytännöt yrityksen tai organisaation toimintaprosesseissa. [8; 14.]

Käytännöksi kutsutaan menetelmäkokonaisuutta, johon sisältyy useita erilaisia käytänteitä. Esimerkiksi tietyn hallinnon osaston työntekijöiden pääsy yrityksen tai organisaation tietoihin rajataan ja heiltä vaaditaan luotettava tunnistautumismenetelmä. Tarkemmat tekniset ratkaisut ja hallinnolliset ratkaisut määritellään organisaation tietoturvasuunnitelmassa. [8; 14.]

2.1.2 Tietoturvasuunnitelma

Tietoturvasuunnitelma poikkeaa tietoturvapolitiikasta siten, että se sisältää ne konkreettiset käytänteet, joilla saavutetaan haluttu tietoturvan taso. Siinä määritellään tarkasti niitä teknisiä ratkaisuja sekä työmenetelmiä, joita kussakin tietojärjestelmässä tullaan

käyttämään. Tietoturvasuunnitelma laaditaan lyhyemmällä aikavälille kuin tietoturvapolitiikka. Sen lähtökohtana on tietoturvapolitiikassa yleisellä tasolla asetetut suuntaviivat. Tietoturvasuunnitelmaa on syytä tarkistaa ja päivittää vähintään kerran vuodessa sekä aina kun organisaation tietojärjestelmissä tapahtuu suuria muutoksia. Suunnitelman laativat organisaation yleisestä turvallisuudesta vastaavat henkilöt yhdessä ICT-osaston kanssa. Tietoturvasuunnitelma voidaan luokitella salaiseksi sen sisältämien yksityiskohtaisten tietoturvaratkaisujen vuoksi. [8; 14.]

Hyvä tietoturvasuunnitelma sisältää usein paljon päivittäisen rutiinityön kannalta vähemmän merkityksellisiä yksityiskohtia, jotka eivät sellaisenaan sovellu tavallisen käyttäjän ohjeiksi. Usein organisaation tietojärjestelmän tavallisia käyttäjiä varten tietoturvasuunnitelmasta laaditaan erillisiä ohjeita, joista on karsittu teknisiä yksityiskohtia sekä ratkaisuja. [8; 14.]

2.2 Tietoturvan osatekijät

Tietoturvan tarkoituksena on suojata tietyt tiedot, palvelut, järjestelmät ja tietoliikenne. Yleisesti tietoturva on jaettu kolmeen eri osatekijään, joita ovat tiedon käytettävyys, luottamuksellisuus sekä eheys. Näiden osatekijöiden lisäksi tietoturvaan liitetään usein myös tiedon kiistämättömyys, tunnistus ja todennus. [1; 8.]

> Luottamuksellisuudella (condifentality) tarkoitetaan sitä, että tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. Käytettävyys (avaibility) merkitsee sitä, että tiedot ovat saatavissa tietojärjestelmässä oikeassa muodossa ja riittävän nopeasti. Eheys (integrity) tarkoittaa laajasti ymmärrettynä sitä, että tietojärjestelmän sisältämät tiedot pitävät paikkansa eivätkä sisällä tahallisia tai tahattomia virheitä. [8, s. 4.]

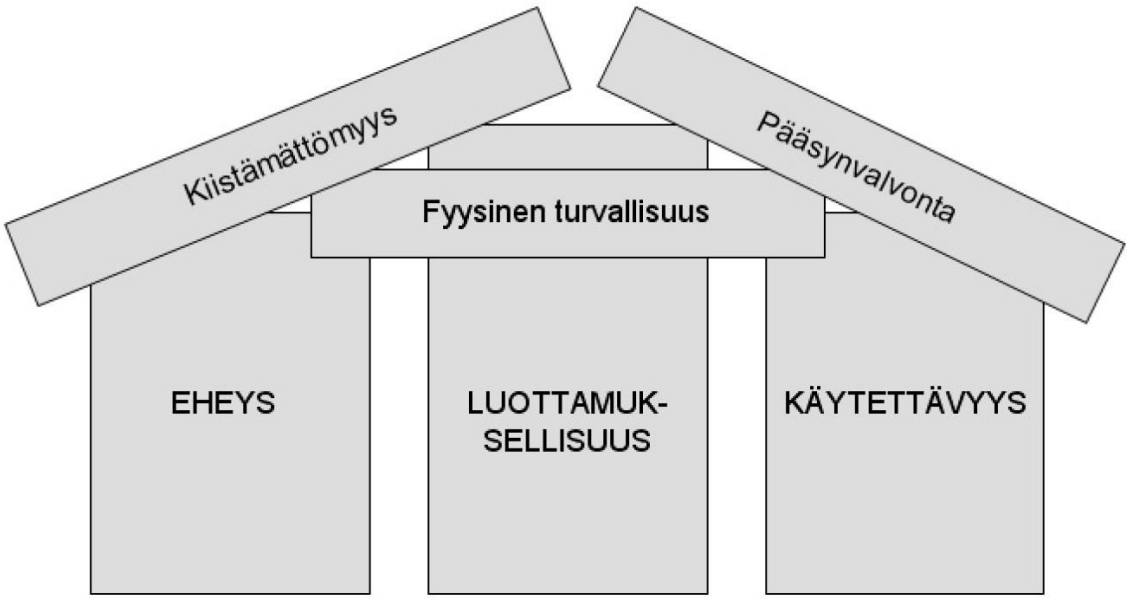
Tiedon luottamuksellisuutta pidetään yllä esimerkiksi suojaamalla tärkeät järjestelmät ja laitteet salasanoilla sekä käyttäjätunnuksilla. Erityisen arkaluontoisia ja arvokkaita järjestelmiä voidaan suojata myös erilaisilla salausmenetelmillä. [8; 14.]

Tiedon käytettävyyttä ylläpidettäessä on tärkeää huolehtia, että käytettävät laitteet ja järjestelmät ovat tarpeeksi tehokkaita tiedon hallinnointiin. Myös tiedon hallinnoinnissa käytettävien ohjelmistojen pitää soveltua riittävän hyvin haluttujen tietojen käsittelyyn. Käytettävyyden parantamiseen liittyy olennaisesti myös tietojen saatavuuden automati-

sointi. Automatisoinnin avulla käyttäjä saa haluamansa tiedot käyttöön haluamassaan muodossa mahdollisimman helposti, esimerkiksi valmiina raportteina tai yhteenvetoina. [8; 14.]

Tiedon eheys toteutetaan yleisesti ohjelmistojen kautta. Tiedon muokkaamiseen tarkoitettuihin ohjelmiin voidaan lisätä esimerkiksi erilaisia rajoituksia, tarkistuksia sekä käyttäjältä pyydettäviä välivarmistuksia. Eheyttä valvotaan myös laitteistotasolla käyttämällä hyväksi esimerkiksi virheenkorjaavia muisteja ja väyliä. Tietoliikenteessä virheiden estämisessä käytetään hyväksi protokollia ja laitteita, jotka tunnistavat ja korjaavat havaitut virheet. [8; 14.]

Edellä mainittujen kolmen osatekijän lisäksi nykyisin tietoturvan ylläpidossa huomioidaan myös tiedon kiistämättömyys ja pääsynvalvonta. Tämä tietoturvan osatekijöiden laajempi rakenne on esitetty kuvassa 1. Tiedon kiistämättömyydellä tarkoitetaan järjestelmien kykyä tunnistaa tietoja käyttävän henkilön identiteetti. Tämä on tärkeää esimerkiksi silloin, kun järjestelmän ylläpitäjä joutuu selvittämään tiedon alkuperää tai tietojen luvatonta käyttöä silloin, kun tietojen luvatonta käyttöä havaitaan. Tietojen kiistämättömyyttä valvotaan käyttämällä käyttäjän tunnistusmekanismeja. Tällaisia tunnistusmekanismeja voivat olla esimerkiksi käyttäjällä luovutettavat tunnistekortit tai muut pienet laitteet, joihin tallennetaan sallitun käyttäjän henkilötiedot, käyttöoikeuksien laajuus ja niiden voimassaoloaika. Nykyisin käyttäjän identifioitiin käytetään myös biometrisiä tunnisteita, kuten esimerkiksi sormenjälki- ja silmänpohjatunnisteita. [8; 14.]



Kuva 1. Tietoturvallisuuden osatekijät. [8. s. 6.]

Pääsynvalvonta liittyy osaltaan tietojen luottamuksellisuuteen. Sillä voidaan rajoittaa tietojenkäsittelyinfrastruktuurin käyttöä. Erityyppiset organisaatiot ja järjestöt pyrkivät estämään laitteidensa ja verkkoyhteyksiensä käytön ulkopuolisten henkilöiden omiin tarkoituksiinsa. Luvattomat käyttäjät kuormittavat organisaatioiden verkkoja ja laitteita ja näin ollen heikentävät merkittävästi niiden käytettävyyttä. Luvattoman käytön seurauksena kasvaa myös riski erilaisten haittaohjelmien leviämiseen organisaation sisällä. Langattomien tietoverkkojen lisääntyessä pääsynvalvonnan merkitys on kasvanut entisestään, koska langattoman verkon luvaton käyttö heikentää sen käytettävyyttä organisaation oman henkilökunnan työtehtävissä. [8; 14.]

3 Palvelunestohyökkäysten taustaa

3.1 Palvelunestohyökkäysten historiaa

Ensimmäisenä merkittävänä palvelunestohyökkäyksenä pidetään Yhdysvalloissa vuonna 1988 Morris-madolla tehtyä verkkohyökkäystä. Madon suunnitteli Cornell-yliopiston opiskelija Robert Morris, joka onnistui saastuttamaan madollaan yhteensä noin 6000 tietokonetta. Hyökkäyksen kohteeksi joutuneet tietokoneet olivat pääasiassa yhdysvaltalaisyliopistojen verkkoon kytkettyjä tietokoneita. Morris piti matoaan tahattomana kokeiluna, jonka ei pitänyt aiheuttaa haittaa kellekään. Morris tuomittiin kolmen vuoden ehdonalaiseen vankeustuomioon, ja hän joutui maksamaan noin 10 000 dollaria sakkoja. [3.]

Seuraavien vuosien aikana palvelunestohyökkäyksiä tehtiin useita kymmeniä, ja ne alkoivat yleistyä laajemmin maailmassa. Myös etähallittavia DoS-työkaluja alkoi tulla 1990-luvun puolivälissä saataville. Näiden työkalujen myötä alkoivat yleistyä suuret salasanavarkaudet erityisesti yliopistojen tietoverkoissa. Vuosina 1996–1997 tehtiin laajoja palvelunestohyökkäyksiä IRC-verkkoihin. Näissä hyökkäyksissä käytettiin hyväksi uusia työkaluja, joita olivat esimerkiksi boink, bonk ja teardrop. [4.]

Myöhemmin 2000-luvun alussa palvelunestohyökkäykset alkoivat keskittyä entistä suurempiin verkkoinfrastruktuureihin, kuten valtiohallinnollisiin tietoverkkoihin. Myös tärkeisiin Internetin DNS-palvelimiin (Domain Name System) kohdistui laajoja palvelunestohyökkäyksiä. Suuriin infrastruktuureihin kohdistuneiden hyökkäysten vaikutus kesti usein vain lyhyen aikaa, suurimmillaan vain yhdestä tunnista muutamaan tuntiin. [4.]

Nykyisin palvelunestohyökkäyksiä tehdään entistä enemmän suuriin infrastruktuureihin ja verkkojen ylläpitäjät joutuvat varautumaan DoS-hyökkäysten uhkiin entistä perusteellisemmin.

3.2 Viime vuosina median uutisoimia palvelunestohyökkäyksiä

Viime vuosina palvelunestohyökkäykset ovat tulleet laajalti esille myös mediassa. Hyökkäyksiä on tehty entistä suurempiin verkkoinfrastruktuureihin, esimerkiksi valtionhallinnon, suurten mediatalojen ja järjestöjen www-sivuille.

Sanomakonserni

Sanoma Oyj:n palveluihin kohdistui 11.9.2012 merkittävä palvelunestohyökkäys. Hyökkäys vaikutti noin tunnin ajan, jonka aikana monet Sanomakonsernin palvelut, kuten esimerkiksi Helsingin Sanomien ja Iltasanomien www-sivut olivat tavoittamattomissa. Tapaus sai paljon julkisuutta Suomen mediassa, ja tapauksen motiiveja sekä sen tekijöitä pohdittiin laajalti. Sanomakonsernin palomuureista vastaavan Stonesoftin mukaan hyökkäys olisi tullut Ukrainasta. Stonesoftin mukaan myös valtiohallinnon tietojärjestelmistä vastaavan Haltikin palveluihin olisi kohdistunut samantyyppinen palvelunestohyökkäys. [14.]

YLE

Yleisradion www-sivut joutuivat 27.12.2012 palvelunestohyökkäyksen kohteeksi. Hyökkäys todettiin puolenpäivän aikoihin, ja www-sivut olivat tavoittamattomissa noin puolitoista tuntia. YLE vahvisti tuolloin kyseessä olleen hajautettu palvelunestohyökkäys. YLE esti aluksi pääsyn sivuilleen ulkomailta, mutta purki eston saman päivän iltana saatuaan www-sivut toimimaan. YLE teki hyökkäyksestä rikosilmoituksen vahingonteosta. [15.]

Useaan suomalaiseen mediataloon keskittynyt hyökkäysaalto

Joulukuussa 2012 monet suomalaiset mediatalot Yleisradion lisäksi joutuivat palvelunestohyökkäysten kohteiksi. YLE:n lisäksi hyökkäyksen kohteiksi joutuivat monet suuret mediatalot, kuten Iltasanomat, Iltalehti ja MTV3. Hyökkäykset kohdistuivat mediatalojen www-sivustoihin. Sivut olivat pahimmillaan tavoittamattomissa usean tunnin ajan. Hyökkäysliikenne oli kaikissa hyökkäyksissä samankaltaista liikenneprofiililtaan ja -määrältään. Tästä syystä uskotaan hyökkäysten takana olleen sama taho. Hyökkäyksissä käytettiin hyväksi väärennettyjä lähdeosoitteita ja hyökkäävän liikenteen havaittiin tulevan ulkomailta. Hyökkäysten motiiveista ei ole saatu varmaa tietoa. [16.]

DNS-palvelimien hyväksikäyttö Spamhaus-palvelua kohtaan

Yhdysvaltalaisen CloudFlare-palveluntarjoajan verkkoon kohdistui alkuvuodesta 2013 palvelunestohyökkäys. Hyökkäyksen tarkoituksena oli häiritä roskapostin torjuntaan

keskittyneen Spamhaus-palvelimen toimintaa. Hyökkäyksessä käytettiin hyväksi kaikille käyttäjille avoimia DNS-nimipalvelimia. Hyökkäys oli suuruudeltaan massiivinen. New York Timesin mukaan hyökkäys oli yksi Internetin historian suurimpia julkisesti ilmoitettuja hyökkäyksiä. [17; 18.]

Julian Assange ja Pirate Bay-verkkosivusto

Ruotsissa hyökättiin lokakuussa 2012 useisiin www-palvelimiin monen päivän ajan. Hyökkäysten tekijäksi ilmoittautui Anonymous-niminen ryhmittymä, jonka tavoitteina on muun muassa sananvapauden edistäminen. Hyökkäysten syyksi ryhmä ilmoitti Wikileaks-verkkosivuston perustajan Julian Assangen oikeudenkäynnin sekä tiedostonjakoon keskittyneen Pirate Bay-verkkosivuston perustajien omistamien palvelimien takavarikoinnin. Ruotsin piraattipuolue kritisoi julkisuudessa palvelunestohyökkäyksiä kertoen, että ne ovat puoleen ajamien sananvapaustavoitteiden vastaisia. [14.]

3.3 Motiivit

3.3.1 Kiusanteko

Palvelunestohyökkäykset olivat erityisesti niiden alkuvaiheessa monesti harmittomiksi tarkoitettuja piloja, kuten esimerkiksi suuria kävijämääriä keräävien www-sivujen kaatamisia. Hyökkääjille oli tyypillistä myös keskinäinen kilpailu, jossa pyrittiin osoittamaan omaa osaamista ja siten hakemaan arvostusta ja kunnioitusta oman tuttavapiirin keskuudessa. Palvelunestohyökkäyksen kohteeksi valikoituu usein sivusto, josta hyökkäyksen tekijä ei syystä tai toisesta pidä.

3.3.2 Taloudelliset syyt

Palvelunestohyökkäyksillä tavoitellaan toisinaan taloudellista hyötyä kiristämällä haluttua kohdetta hyökkäyksellä. Yhdysvaltalain suurimman teleoperaattorin AT&T:n mukaan palvelunestohyökkäyksillä kiristäminen on jo niin yleistä, etteivät hyökkäyksen kohteeksi joutuneet uhrit enää ylläty kiristysyrityksistä. Operaattorin mukaan uhrit vaikenevat monesti kiristysyrityksistä, eikä näitä tämän vuoksi käsitellä usein julkisuudessa. Myös oikeustapauksia tällaisista kiristyksistä on vähän. Yhdysvaltain liittovaltion keskusrikospoliisi FBI (Federal Bureau of Investigation) tutkii verkkouhkiin liittyviä kiris-

tystapauksia lähes päivittäin. Yhdysvalloissa rahasummat vaihtelevat kiristystapauksissa muutamista tuhansista jopa useisiin miljooniin dollareihin. [20.]

3.3.3 Poliittiset syyt

Erääksi motiiviksi palvelunestohyökkäyksiä suunniteltaessa ja toteutettaessa ovat nykyisin nousseet erilaiset poliittiset syyt. Hyökkäyksiä tehdään esimerkiksi valtiohallinnon sivustoihin ja palvelimiin, joille hyökkääjä tai hyökkääjät haluavat aiheuttaa haittaa. Esimerkiksi ihmisoikeusloukkaukset, yhteiskunnan eriarvoistuminen ja jopa sotatoimet voivat olla syitä, jonka vuoksi tietty taho haluaa aiheuttaa pahennusta.

Vuonna 2014 Ukrainassa vallitsevan Krimin kriisin aikana on tehty palvelunestohyökkäyksiä erilaisiin kriisiin liittyvien tahojen www-sivustoille. Mediassa on uutisoitu muun muassa hyökkäykset Venäjän presidentin ja keskuspankin www-sivuja kohtaan. Myös sotilasliitto NATO:n (North Atlantic Treaty Organization) www-sivuja kohtaan on hyökätty kriisin aikana. [5; 6.]

4 Palvelunestohyökkäysten toteutustapoja

4.1 Palvelunestohyökkäys

Palvelunestohyökkäyksiä (Denial of Service) voidaan toteuttaa monin eri tavoin. Seuraavassa luvussa esitellään yleisimpiä tapoja tehdä palvelunestohyökkäys. Hyökkäyksiä voidaan toteuttaa monin eri tavoin ja niiden torjuntaan käytettävät tekniikat vaihtelevat hyökkäystapojen mukaan. Suomen rikoslain 38. luvun 5. pykälän mukaan palvelunestohyökkäys tulkitaan tietoliikenteen häirinnäksi ja on rangaistava teko. Tämä rikoslain osa on säädetty voimaan 1.9.1995.

> Tietoliikenteen häirintä
>
> Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. [12.]

4.2 Resurssien kuluttaminen

Resurssien kuluttamisella tarkoitetaan yrityksen verkkoliikenteen ruuhkauttamista ja sen kapasiteetin loppuun kuluttamista. Hyökkääjän tavoitteena on ruuhkauttaa hyökkäyskohteen verkkokapasiteettiä niin, etteivät oikeat ja luotettavat pyynnöt tai vastaukset kohdepalvelimelle pääse perille. Verkkoliikennettä ei välttämättä tarvitse saada täysin toimimattomaksi vaan usein riittää jo se, että hyökkääjä pystyy hidastamaan kohdepalvelinta tarpeeksi. Erään tulkinnan mukaan palvelin koetaan käyttökelvottomaksi, mikäli siltä kestää vastata pyyntöön kauemmin kuin 10 sekuntia.

Verkon suorituskykyä voidaan kuormittaa monin eri tavoin. Yleisiä kuormitustapoja ovat erilaiset tulvitustekniikat. Näissä tekniikoissa hyökkääjä lähettää kohteeseen useita tuhansia pyyntöjä tai lähettää roskasähköpostia kohteen palvelimelle. Näiden aiheuttaman verkkoliikenteen ansiosta haluttu kohdeverkko tai palvelin ruuhkautuu käyttökelvottomaksi. [4.]

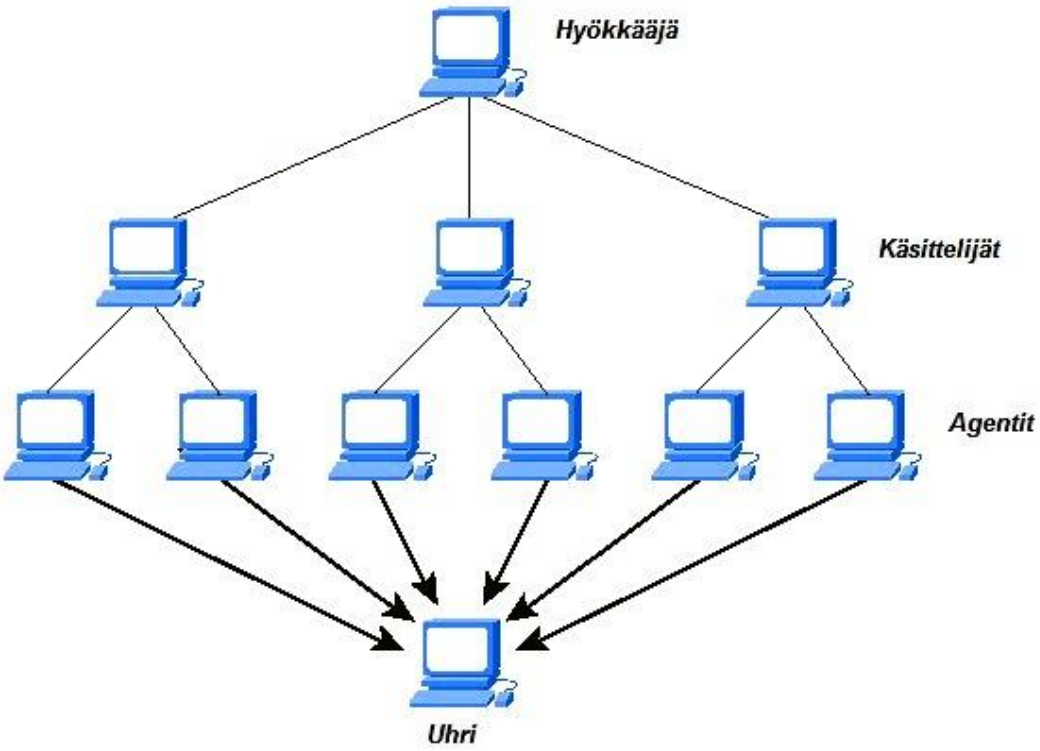
4.3 Hajautettu palvelunestohyökkäys

Hajautetussa palvelunestohyökkäyksessä (Distributed Denial of Service, DDoS) hyökkääjä käyttää hyväkseen useaa lähdettä hyökätessään kohdepalvelimeen. Yleinen tapa toteuttaa DDoS-hyökkäys on muodostaa suuri etähallittava tietokoneiden verkosto eli bottiverkko. Bottiverkossa voi olla useita tavallisten käyttäjien omistamia tietokoneita ilman, että he tietävät olevansa osa bottiverkkoa. [10.]

Hajautetun palvelunestohyökkäyksen suunnittelu käsittää kaksi vaihetta. Aluksi hyökkääjän tavoitteena on löytää tarpeeksi suuri määrä hallittavia koneita, joilla hän voi toteuttaa hyökkäyksen. Hyökkääjä etsii verkosta koneita, joissa on hallintaanoton mahdollistavia haavoittuvuuksia. Hyökkääjä voi etsiä haavoittuvuuksia sisältäviä koneita verkosta manuaalisesti tai automatisoimalla esimerkiksi skriptejä etsimään tietynpiirteisiä haavoittuvuuksia. [4.]

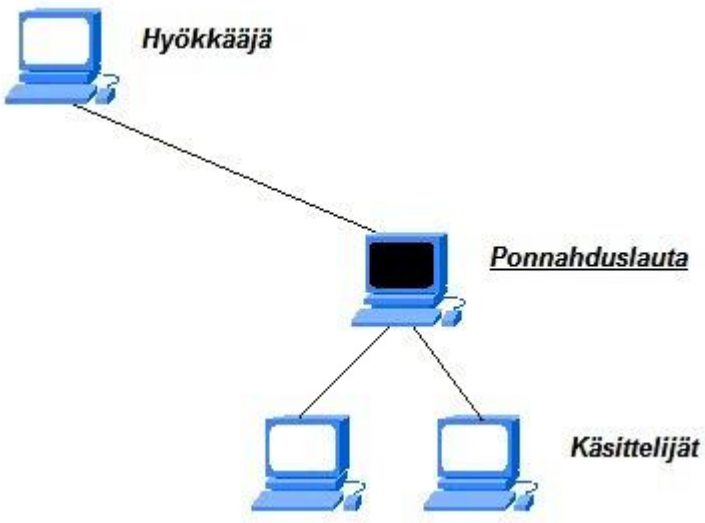
Saatuaan riittävän määrän koneita hallintaansa hyökkääjä siirtyy hyökkäysvaiheeseen. Hyökkääjän on pohdittava, millaisen vaikutuksen hän haluaa aiheuttaa hyökkäyskohteeseensa. Hyökkäyskohde voidaan lamauttaa täysin hukuttamalla se verkkoliikenteeseen tai vain hidastaa sen toimintoja merkittävästi. Esimerkiksi www-sivuja hidastamalla voidaan aiheuttaa niille huonoa mainetta niiden toimintakyvystä, kuin että ne kaadettaisiin kokonaan toimintakyvyttömiksi. [4.]

Hyökkäyksessä yleinen toimintamalli on käyttää käsittelijä-agentti-mallia. Hyökkääjä on yhteydessä agenttikoneisiin käsittelijöiden kautta. Käsittelijät voivat olla yleisiä palvelimia, ja agentit ovat kaapattuja bottikoneita. Agenteiksi kaapattuja koneita kutsutaan toisinaan myös zombeiksi. Agenteille hyökkääjä lähettää hyökkäystietoja sekä haavoittuvien koneiden etsintätietoja. Kuvassa 2 on esitetty hajautetun palvelunestohyökkäyksen toimintaperiaate.



Kuva 2. Hajautettu palvelunestohyökkäys.

Hyökkääjä käyttää jälkiensä peittämiseen niin kutsuttua ponnahduslautaa, kuten kuvassa 3 voidaan nähdä. Ennen käsittelijäkoneisiin liittymistä hyökkääjä kirjautuu ensin useisiin toisiin koneisiin, joiden kautta hän ottaa yhteyden käsittelijöihin. Näin hyökkääjän jäljittäminen ja seuraaminen vaikeutuu merkittävästi, koska ponnahduslautoina käytettävät koneet sijaitsevat jopa eri mantereilla. Jälkien seuraamista vaikeuttaa esimerkiksi eri maiden välinen lainsäädäntö, joka voi estää esimerkiksi lokitietojen luovuttamisen viranomaisille.



Kuva 3. Ponnahduslauta hyökkääjän apuna.

4.4 Reitityksen ja nimitietojen muuttaminen

Palvelunestohyökkäyksiä voidaan tehdä verkon infrastruktuuria kohtaan, kuten esimerkiksi reitittimiä ja DNS-nimipalvelimia. Näiden reitittimien ja palvelimien häirintä vaikuttaa usein nopeasti laajaan käyttäjäkuntaan ja on tästä syystä hyökkääjälle houkutteleva kohde. Esimerkiksi nimipalvelimen tietojen muuttaminen vaikuttaa välittömästi tavallisen käyttäjän käyttökokemukseen, kun web-liikenne ohjautuu vääriin osoitteisiin. Hyökkääjä voi asettaa esimerkiksi halutun www-sivun ohjautumaan toiselle sivulle, jossa käyttäjältä voidaan kalastella tietoja tai pyytää asentamaan haittaohjelmia koneeseensa.

Reitittimiä hyökkääjä voi yrittää hukuttaa pakettitulvaan lähettämällä esimerkiksi bottiverkon kautta niille suuria määriä yhteyspyyntöjä. Suuri liikennemäärä alentaa merkittävästi reitittimien käytettävyyttä. Hyökkääjä voi myös yrittää hidastaa reititysprotokollan toimintaa täyttämällä reititystauluja epäolennaisella tiedolla, jolloin kriittiset tiedot hukkuvat niihin ja reitittimen toiminta hidastuu.

4.5 Smurf-hyökkäys

Smurf-hyökkäyksessä hyökkäyskohde pyritään ruuhkauttamaan lähettämällä sille ICMP-paketteja (Internet Control Message Protocol), joihin hyökkääjä on väärentänyt uudet lähetystiedot. Kohdekone hukkuu ICMP-pakettien aiheuttamaan pyyntötulvaan.

ICMP-tulvituksessa hyökkääjä lähettää kohteeseen isoja määriä ICMP-paketteja, joissa on lähetyskoneen osoitteeksi vaihdettu kohdepalvelimen osoite. Tämä aiheuttaa sen, että kohdepalvelin vastaa itse itselleen kaksinkertaisen määrän mitä tavallisesti tekisi. Toinen tapa on lähettää saman verkon alaisille koneille ICMP-paketteja, joihin on väärennetty lähettäjän tiedoiksi kohdepalvelimen yhteystiedot. Näin ollen kaikki kohdeverkon koneet vastaavat hyökkääjän haluamalle kohdepalvelimelle, joka ruuhkautuu pyyntöjen suuresta määrästä. [9.]

Smurf-hyökkäykseen voidaan ICMP-pakettien sijaan käyttää myös UDP-paketteja (User Datagram Protocol). Tässä tavassa toimintaperiaate on sama, kuin ICMP-tulvituksessa. UDP-paketit voivat sisältää esimerkiksi vääriä DNS-pyyntöjä. UDP-paketteihin perustuvaa Smurf-hyökkäystä kutsutaan myös hyökkäysmenetelmän lähdekoodin mukaan Fraggle-hyökkäykseksi. [9.]

5 Palvelunestohyökkäyksiltä suojautuminen

5.1 Ennaltaehkäisy

Tehokkain tapa suojautua palvelunestohyökkäyksiltä on tehokas ennaltaehkäisy. On syytä muistaa, että taitavia hyökkääjiä kohtaan kaikki organisaation toteuttamat ennaltaehkäisyn toimenpiteet eivät välttämättä pysty täydellisesti suojaamaan organisaation verkkoinfrastruktuuria. Tästäkin huolimatta niin sanotut perussuojauskeinot ovat välttämättömiä tänä päivänä yritysmaailmassa. Erityisesti asiakaspalveluun perustuvissa liiketoiminnoissa järjestelmien ja yritysverkon käytettävyys on todella tärkeää. Vaikka suojauskeinot eivät täysin estäisikään kaikkia tietoturvahyökkäyksiä, ne vaikeuttavat kuitenkin niiden tekemistä merkittävästi ja nostavat tietoverkon turvallisuustasoa.

5.1.1 Peruskeinoja hyökkäyksiltä suojautumiseen

Hyviä perussuojauskeinoja organisaatioissa ja yrityksissä ovat esimerkiksi ohjelmistoissa tunnistettujen tietoturva-aukkojen korjaaminen, huonojen verkkoprotokollien päivittäminen ja resurssienhallinnan kehittäminen. Yleisestikin on hyvä tapa pyrkiä pitämään yrityksen verkkoinfrastruktuuri mahdollisimman yksinkertaisena ja hyvin organisoituna. Tämä auttaa merkittävästi myös verkon ylläpidossa. [4.]

Organisaatiot ja yritykset pystyvät varautumaan palvelunestohyökkäyksiin jo pelkästään mitoittamalla verkkoyhteydet ja järjestelmät yli vaaditun tarpeen. Toisaalta järjestelmien ylimitoittaminen on kallista, eikä se yksinään pysty estämään tarpeeksi suuria palvelunestohyökkäyksiä. Järjestelmien ylimitoittamista halvempi vaihtoehto yrityksissä on pyrkiä hajauttamaan palvelunestohyökkäyksen vaikutus monen eri palvelimen kesken. Tätä varten verkkolaitteet tulee konfiguroida tarkasti ja huolehtia siitä, että tietoturvapäivitykset ovat ajan tasalla. [4.]

5.1.2 Hajautetuilta palvelunestohyökkäyksiltä suojautuminen

Yrityksen verkkoinfrastruktuurin hyvä organisointi auttaa estämään myös hajautettuja palvelunestohyökkäyksiä (DDoS). Ensimmäisenä toimenpiteenä verkon kriittiset kohdat tulee paikallistaa ja niihin tulee kohdistaa erityisiä toimenpiteitä. Yrityksen verkko tulisi organisoida siten, että kriittisiä sovelluksia jaetaan usean palvelimen kesken ja näiden

palvelimien tulisi sijaita eri aliverkoissa. Tämä aiheuttaa hyökkääjälle sen, että saavuttaakseen palvelunestovaikutuksen hyökkäyksen pitäisi kohdistua jokaiseen palvelimiin erikseen. Sovellusten jakamisen lisäksi yritysverkossa ei pitäisi kerryttää yhdelle palvelimelle useita tehtäviä, vaan jokaisella palvelimella tulisi olla yksi selkeä määritelty tehtävä. Tämä helpottaa merkittävästi palauttamaan hyökkäyksen kohteeksi joutunutta verkkoa, koska hyökkäyksen kohteeksi joutunut palvelin voidaan eristää ja korvata toimivalla. Näin palveluntaso ja käytettävyys eivät heikkene merkittävästi, vaikka verkkoa kohtaa hyökättäisiin. [4.]

5.1.3 Hyökkäyksien havainnointi ja niihin reagointi

Palvelunestohyökkäyksiltä on vaikeaa suojautua täysin aukottomasti. Monet suojausjärjestelmät vaativat paljon työtä ja voivat olla kalliita suhteessa niiden hyötyyn. Mikäli hyökkäyksiä ei tapahdu kovin usein, on järkevämpää keskittyä hyökkäyksiltä suojautumisen sijaan niihin reagointiin. Tehokas reagointi ei kuitenkaan tarkoita, että suojautumiskeinot voisi jättää kokonaan väliin. Monesti voidaan joutua pyytämään ulkopuolista apua hyökkäyksiltä suojautuessa, jopa viranomaisille voidaan joutua tekemään yhteydenotto. [4.]

Organisaation järjestelmien tulee olla tarkkoja, jotta ne pystyvät määrittelemään sen miten minkinlaiseen hyökkäykseen varaudutaan ja mitä suojautumiskeinoja käytetään. Nykyisin suuri osa hyökkäyksistä on taitavasti toteutettuja, joten hyvä oman verkon toiminnan ymmärtäminen ja hallinta ovat tärkeä osa suojautumista. Puolustautumisen pitäisi alkaa heti, kun järjestelmän havainnointimekanismi antaa varoituksen mahdollisesti hyökkäyksestä. Tässä vaiheessa riittää se, että hyökkäys saadaan pysäytettyä tai ainakin vähennettyä sen vaikutusta merkittävästi. [4.]

Hyökkäyksien havainnoinnissa hyviä keinoja ovat esimerkiksi oman verkkoliikenteen monitorointi, ulkopuolisten käyttäjien lukumäärän ja käyttäytymisen seuranta sekä palvelimen kuormituksen ja resurssien valvonta. Kun hyökkäys on havaittu, se kategorisoidaan ja aloitetaan sen tarkempi tarkastelu. Tähän vaiheeseen kuuluvat verkkoprotokollien, sovellusten, laitteiden, osoitetietojen sekä pakettien pituuksien ja sisällön tunnistus. Näillä arvoilla voidaan helpommin rajoittaa liikennemäärää sekä suodatuksia ja asettaa uusia sääntöjä.

Hyökkäyksen havaitsemisen ja tunnistamisen jälkeen aloitetaan hyökkäykseen vastaaminen. Yleinen keino rajoittaa hyökkäystä on pudottaa sisään tulevaa epämääräistä liikennettä. Tämä on haastavaa, koska tällöin voidaan vahingossa pudottaa myös oikeutettua verkkoliikennettä. Tästä syystä hyvä tekniikka on suodattaa liikennettä tai rajoittaa kaistaa. Epäilyttävät paketit luokitellaan ja tiputetaan suodatuksen avulla pois. Kaistaa rajoittamalla epäilyttäville paketeille säädetään oma kaista. Se kumpaa keinoa käytetään, riippuu verkkoliikenteen luokittelun tarkkuudesta. Mikäli verkkoliikenne on tarkkaan luokiteltua, haitallisen liikenteen pudottaminen pois on melko yksinkertaista ja helppoa. Mikäli tarkkuus ei ole riittävä, turvallisempi tapa vastata hyökkäykseen on vain rajoittaa kaistaa. Näiden toimenpiteiden jälkeen hyökkäystä voidaan alkaa jäljittää.

Joissain tapauksissa hyökkääjä on voinut saada hallintaansa organisaation verkossa toimivia laitteita. Tämä on mahdollista havaita seuraamalla ulospäin suuntautuvaa verkkoliikennettä. Tähän liittyy usein myös lähdeosoitteen väärentäminen. Mikäli tällaista havaitaan, voidaan ulospäin suuntautuvaa verkkoliikennettä suodattaa samalla periaatteella kuin sisäänpäin tulevaa. Hyökkäykselle altistuneet laitteet on poistettava verkosta, tutkittava, varmuuskopioitava tärkeät tiedot ja lopulta puhdistaa laitteet. Hyökkäyksissä käytettävät haittakoodit ovat usein taitavasti piilotettuja, joten laitteen puhdistaminen tulee tehdä huolellisesti.

Havaitut hyökkäykset tule myös ilmoittaa operaattorille, sekä joissain tapauksissa myös viranomaisille. Ilmoittamalla operaattorille epäillystä hyökkäyksestä varmistutaan siitä, ettei verkkoliikenteen toimimattomuus johdu omasta käyttövirheestä tai laiteviasta. Mikäli todetaan kyseessä olleen aito palvelunestohyökkäys, tästä on hyvä ilmoittaa myös Viestintäviraston alaiselle tietoturvaviranomaiselle CERT:lle. Yhteydenoton saatuaan CERT päättää, käynnistääkö se tapauksesta oman tutkintansa.

5.2 Ulkoistettu tietoturva

Yritysten ja organisaatioiden on mahdollista ulkoistaa oma tietoturvaosaamisensa silloin, kun yrityksellä ei ole resursseja oman verkkoliikenteensä valvomiseen. Monet pienemmän yritykset keskittyvät omaan ydinosaamiseensa ja hankkivat muita tarvittavia toimintoja ulkopuolisilta toimittajilta. Resurssien puutteen lisäksi ulkoistamisen syynä voi olla asiantuntijaosaamisen puute. Liiketoiminnan kannalta tärkeiden tietojen käsittely voi olla vaativaa, ja sen vuoksi tähän toimeen halutaan tietoturvan asiantuntijoiden

apua. Ulkoistaminen voi joissain tapauksissa olla myös halvempaa kuin palkata yritykseen oma tietoturva-asiantuntija. Ulkoistamisen etuna on myös palveluntarjonnan laajuus. Ulkoiset toimijat ovat usein tavoitettavissa joka vuorokausi mihin kellon aikaan tahansa. [13.]

Yritykset ulkoistavat paljon muitakin toimintojaan, mutta ulkoistamiseen liittyy aina tietoturva. Yleisimpiä ulkoistuksen kohteita on yrityksen tietohallinto. Tietohallinnon osa-alueista ulkoistettavia toimintoja voivat olla esimerkiksi järjestelmänhallintapalvelut, laitteiston ylläpito, tietoliikenneyhteydet, sovellusvuokraukset sekä monet muut suunnitteluun, asennuksiin ja konsultointiin liittyvät palvelut. Yleisiä tietoturvan ulkoistamiskohteita ovat palomuuri- ja etäyhteyspalvelut ja näiden tuki- ja ylläpitopalvelut. Hyvistä tietoturvan ulkoistamispalveluista huolimatta kaikkea tietoturvaa ei voi ulkoistaa. Lopullinen vastuu yrityksen tietoturvasta on aina sen johdolla. [13.]

Ulkoistamisessa on olemassa aina riskejä. Suurin ongelma tietoturvaa ulkoistettaessa on vastuun määrittely. Vastuun osa-alueet on määriteltävä todella tarkasti. Toinen riski ulkoistamisessa on se, että yritys joutuu ulkoistamistapauksissa luovuttamaan omia tietojaan ulkopuolisen toimijan haltuun. Tästä syystä ulkopuolisen toimijan tulee olla luotettava ja asiantunteva. Ulkoistetut palvelut on tapana kilpailuttaa ja näin saada yritykselle paras kustannustehokkain toimintaympäristö. [13.]

6 Palvelunestohyökkäysten yleistyminen Suomessa

6.1 Tutkimuksen lähtökohdat

Palvelunestohyökkäysten yleisyyttä voidaan arvioida erilaisten tilastojen avulla. Tässä työssä on käytetty Viestintäviraston alaisena toimivan tietoturvaviranomaisen CERT:n haavoittuvuustiedotteita ja niiden kautta tutkittu palvelunestohyökkäysten yleistymistä Suomessa. CERT luokittelee nykyisin omat tiedotteensa varoituksiin ja haatoittuvuuksiin. Tässä työssä esitettyjä tiedotteita seurattaessa on keskitytty CERT:n julkaisemiin haavoittuvuuksien tiedonantoihin, koska palvelunestoihin annettuja tietoturvavaroituksia ei ole juurikaan annettu. Tiedotteet kuvaavat parhaalla mahdollisella tavalla kansallisesti havaittuja tietoturvaloukkauksia. Kuvaajissa käytetyt tarkat numeroarvot on haettu käsin CERT:n tiedotetietokannasta, ja ne on liitetty nähtäväksi liitesivulle 1.

CERT on ottanut käyttöön nykyisen haavoittuvuusluokittelun maaliskuussa vuonna 2007. Tästä syystä tilastoissa on havaittavissa merkittävä tiedotteiden kokonaismäärän kasvu. CERT:n julkaisemat haavoittuvuustiedotteet luokitellaan kohteena olevien palvelimien, hyökkäysten, haavoittuvuuden hyväksikäytön aiheuttamien vahinkojen ja ongelman korjaavien toimenpiteiden mukaisesti. Näiden haavoittuvuutta kuvaavien tietojen perusteella voidaan arvioida sen aiheuttaman tietoturvauhan vakavuus. [19.]

6.2 CERT-tiedotteiden seuranta

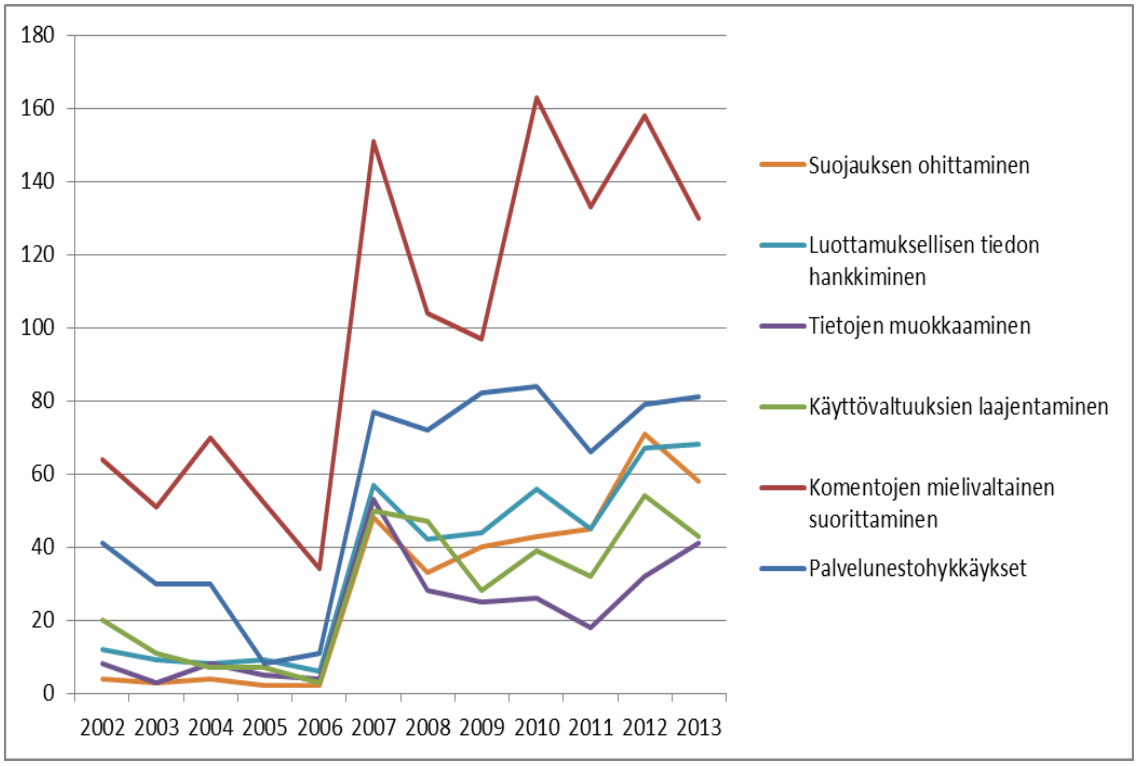
Palvelunestohyökkäysten yleistymistä on arvioitu CERT-tiedotteissa kuvattujen palvelunestohyökkäysten absoluuttisten ja suhteellisten määrien avulla. Kuvassa 4 on esitetty raportoitujen palvelunestohyökkäysten suhteellinen osuus CERT:n julkaisemista haavoittuvuuksista. Palvelunestohyökkäysten osuus kaikista haavoittuvuuksista on vaihdellut noin 10–60 % välillä. Alimmillaan palvelunestohyökkäysten osuus on ollut vuonna 2005 ja korkeimmillaan 2009.

Kuva 4. Raportoitujen palvelunestohyökkäysten suhteellinen osuus CERT:n julkaisemista haavoittuvuuksista.

Kuvassa 5 on esitetty tiedotteiden kokonaismäärän kehitys. Kuvassa on havaittavissa vuonna 2007 tapahtunut haavoittuvuusluokittelun muutos, jonka vuoksi tiedotteiden kokonaismäärä on noin kaksinkertaistunut.

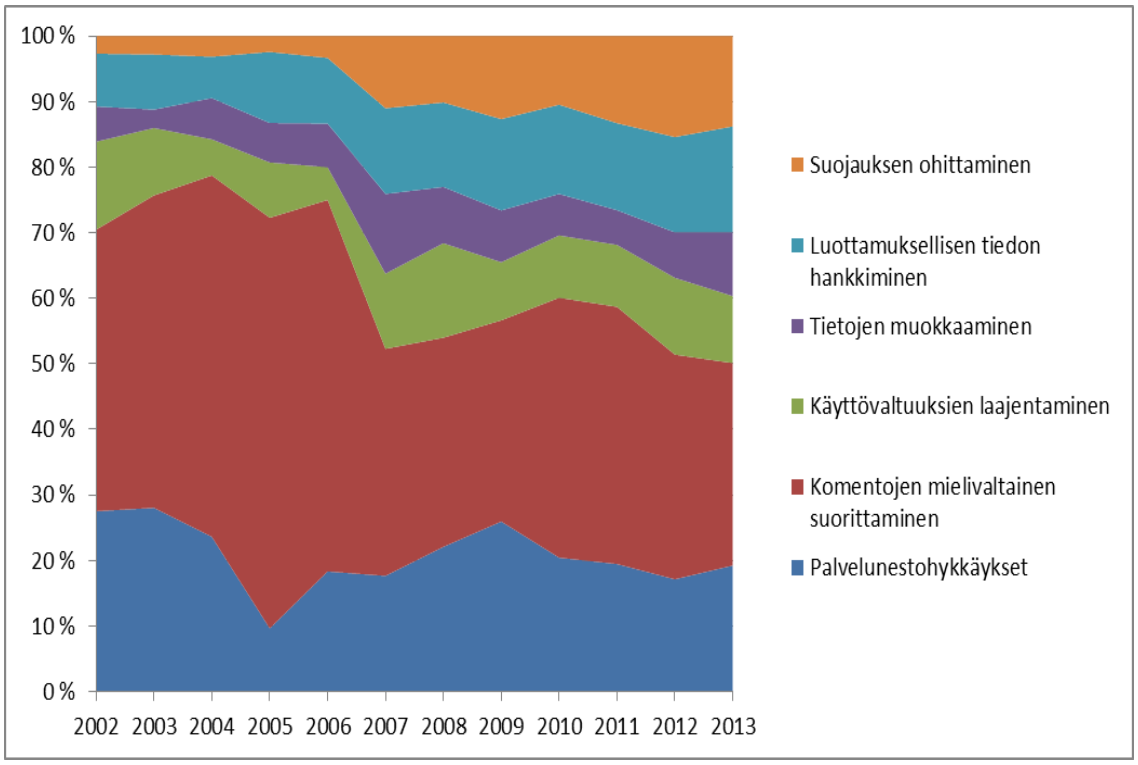
Kuva 5. CERT:n julkaisemien haavoittuvuuksien kokonaismäärän kehitys vuosina 2002-2013.

Kuvassa 6 on esitetty raporteissa kuvattujen tietoturvauhkien kokonaismäärien kehitys vuosina 2002–2013. Yksi tiedote voi sisältää useamman tietoturvauhan, josta syystä tietoturvauhkia on merkittävästi enemmän kuin tietoturvatiedotteita. Kuvassa 6 on nähtävissä myös sama ilmiö kuin kuvassa 5 eli tiedotteiden ja sitä myötä myös tietoturvauhkien kokonaismäärän kasvu. Tilastoituja palvelunestohyökkäyksiä on vuodesta 2007 eteenpäin ollut joitakin kymmeniä vuosittain.



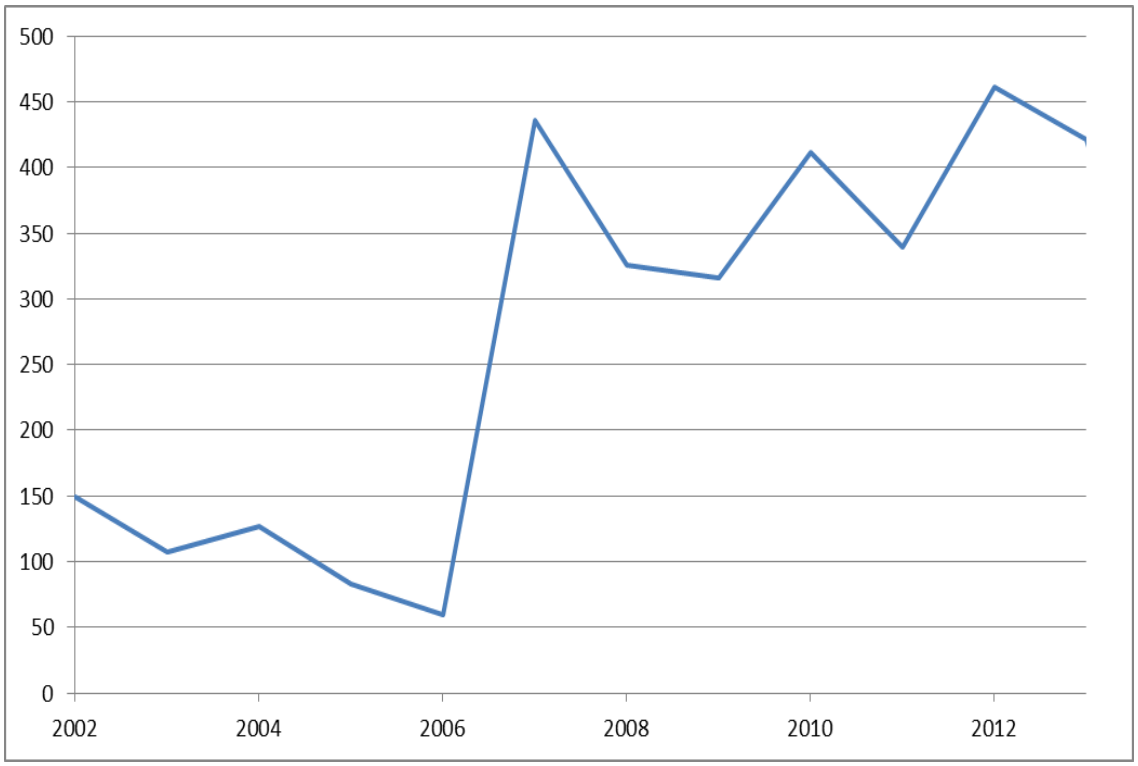
Kuva 6. Raporteissa kuvattujen tietoturvauhkien kokonaismäärien kehitys vuosina 2002-2013.

Kuvassa 7 on esitetty CERT-raporteissa kuvattujen tietoturvauhkien suhteellisten osuuksien kehityksiä vuosina 2002–2013. Palvelunestohyökkäykset ovat jo pitkään olleet toiseksi suurin tietoturvauhka. Tietoturvauhkien suhteelliset osuudet ovat säilyneet suunnilleen samanlaisina vuodesta 2007 alkaen, tosin suojauksen ohittaminen on yleistynyt jonkin verran.



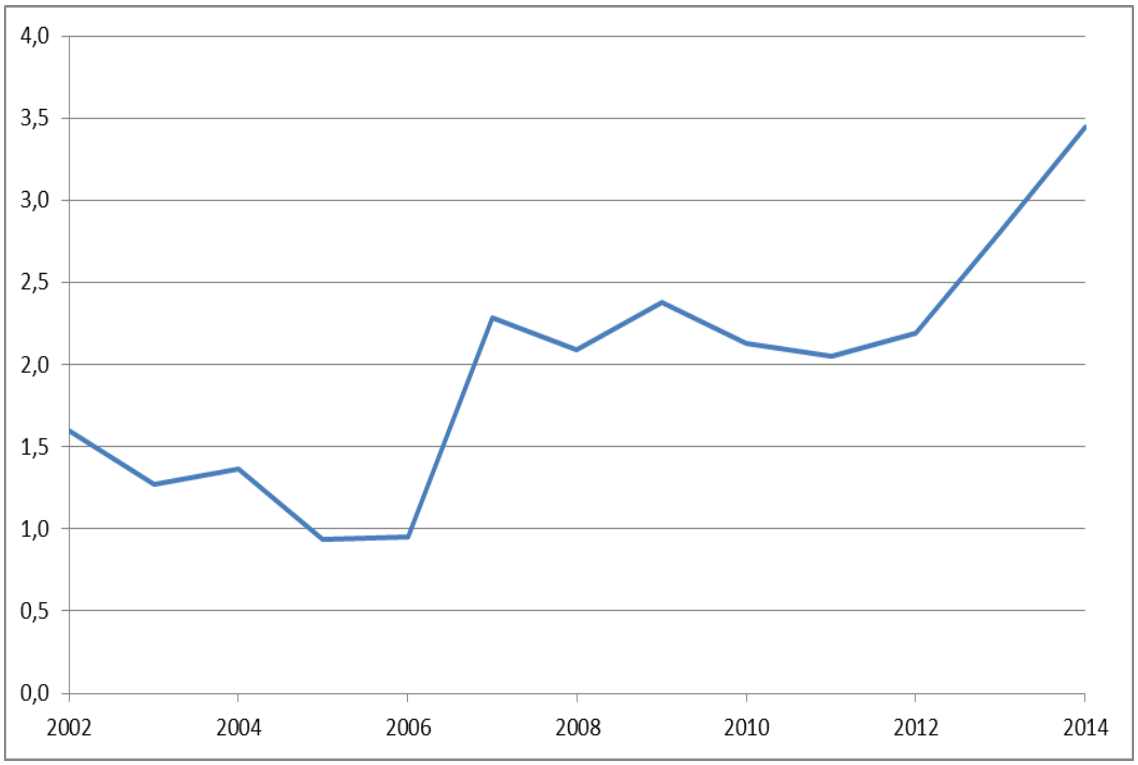
Kuva 7. Raporteissa kuvattujen tietoturvauhkien suhteellisten osuuksien kehitys vuosina 2002-2013.

Kuvassa 8 on tarkasteltu tietoturvauhkien kokonaismäärän kehitystä vuosina 2002–2013. Kokonaismäärä on kasvanut haavoittuvuuksien luokittelumuutoksen yhteydessä vuonna 2007 noin kolminkertaiseksi ja säilynyt suunnilleen samalla tasolla sen jälkeen.



Kuva 8. Raporteissa kuvattujen tietoturvauhkien kokonaismäärä vuosina 2002-2013.

Kuvassa 9 on esitetty yhdessä tietoturvatiedotteessa raportoitujen tietoturvauhkien keskimääräisen lukumäärän kehitys vuosina 2002–2014. Kuviosta on nähtävissä, kuinka vuonna 2007 tehty haavoittuvuuksien luokittelumuutos on nostanut keskimääräisen tiedotekohtaisen tietoturvauhkamäärän yli kolmeen uhkaan tiedotetta kohden.



Kuva 9. Yhdessä tiedotteessa raportoitujen tietoturvauhkien keskimääräisen lukumäärän kehitys vuosina 2002-2014.

6.3 Johtopäätökset

Kuvaajista voidaan havaita palvelunestohyökkäyksillä olevan merkittävä osuus kaikissa havaituissa tietoturvauhissa. Tiedotteiden kokonaismäärä on vuonna 2007 CERT:n toteuttaman haavoittuvuuksien luokittelumuutoksen jälkeen pysynyt suurin piirtein samalla tasolla. Kokonaismäärän nousu johtuu myös siitä, että yhteydenotot CERT-yksikköön ovat kasvaneet viime vuosien aikana ja tietoturvahaavoittuvuuksista raportoidaan entistä tarkemmin. Tämän ansiosta myös itse tiedotteet ovat tarkempia ja niiden taustalla tehty tutkimus laadukkaampaa. Yhteen havaittuun tietoturvauhkaan voidaan nykyisin liittää useita eri haavoittuvuuden luokituksia. Kuten kuvasta 9 voidaan nähdä, näiden yksittäisten luokituksien määrä tiedotetta kohti onkin noussut yhdestä noin kolmeen.

Erityyppiset haavoittuvuustyypit ovat pysynet määriltään melko samoina viime vuosina. Pientä kasvua on ollut havaittavissa suojauksen ohittamisessa ja luottamuksellisen tiedon hankinnassa. Haavoittuvuustyypeistä komentojen mielivaltainen suorittaminen ja tietojen muokkaaminen ovat laskeneet hieman viime vuosina (kuva 7.). Vaikka tietojen muokkaamisen suhteellinen osuus kaikista haavoittuvuustyypeistä on laskenut, niiden kokonaismäärä on vuodesta 2011 lähtien noussut joka vuosi (kuva 6.).

Palvelunestohyökkäysten osuus havaituista haavoittuvuuksista on pysynyt viime vuosina suurin piirtein samana. Vuonna 2007 tapahtuneen haavoittuvuuksien luokittelumuutoksen jälkeen palvelunestohyökkäysten suhteellinen määrä tiedotteissa on hieman vähentynyt. Vuonna 2012 palvelunestohyökkäysten suhteellinen määrä alkoi jälleen kasvaa ja sen kasvu on jatkunut vuoteen 2014 saakka. Kuten kuvasta 7 voidaan havaita, palvelunestohyökkäysten osuus muista haavoittuvuustyypeistä on toiseksi suurin. Näin ollen palvelunestohyökkäysten voidaan nähdä tänäkin päivänä olevan varsin yleinen tietoturvauhka.

7 Yhteenveto

Insinöörityön tarkoituksena oli perehtyä palvelunestohyökkäyksiin tietoturvauhkana. Työssä pyrittiin selvittämään niiden tarkoitusperiä, torjuntaa sekä yleistymistä Suomessa. Aluksi perehdyin työssä tietoturvan peruskäsitteisiin organisaatioiden ja yritysten näkökulmasta. Tietoturvan peruskäsitteissä kävin läpi tietoturvan osatekijöitä ja tietoturvan rakennetta yleisesti. Pyrin käsittelemään tietoturvaa erityisesti yritysten näkökulmasta, koska työn aiheena olevat palvelunestohyökkäykset kohdistuvat pääasiassa niihin. Alussa kävin läpi, miten tietoturvaa yrityksissä suunnitellaan, rakennetaan, ylläpidetään ja kehitetään eteenpäin. Esittelin tässä yhteydessä tietoturvasuunnittelun perusmalleja yritysmaailmasta, joihin kuuluvat esimerkiksi yrityksen tietoturvapolitiikka ja tietoturvasuunnitelma.

Seuraavaksi tutustuin tarkemmin itse palvelunestohyökkäyksiin ja niiden taustoihin. Aluksi kävin lyhyesti läpi palvelunestohyökkäysten historiaa sekä esittelin muutamalla esimerkillä mediassa julkisuutta saaneita merkittäviä palvelunestohyökkäyksiä. Tutkin myös palvelunestohyökkäysten motiiveja ja jaoin ne kolmeen luokkaan: kiusantekoon, taloudelliseen hyötyyn ja poliittisiin tarkoitusperiin.

Selvitettyäni palvelunestohyökkäysten taustoja perehdyin niiden tekniseen toteutukseen. Perehdyin siihen, millä palvelunestohyökkäyksiä voidaan toteuttaa ja mitä erityyppisillä hyökkäyksillä voidaan saada aikaan. Esittelin erilaisia tapoja toteuttaa palvelunestohyökkäys ja kerroin niiden teknisestä toteutuksesta.

Näiden jälkeen tutustuin siihen. kuinka palvelunestohyökkäyksiltä voidaan suojautua. Tutustuin erityyppisiin ennaltaehkäisymenetelmiin ja siihen, kuinka toteutuneisiin hyökkäyksiin voitaisiin reagoida tehokkaasti. Toin esille myös ulkoistetun tietoturvan vaihtoehdon ja esittelin sen etuja ja haittoja.

Lopuksi tutkin palvelunestohyökkäysten yleistymistä Suomessa käyttämällä hyväksi Viestintäviraston alaisen tietoturvaviranomaisen CERT:n julkaisemia tietoturvahaavoittuvuuksia. Aluksi kerroin lyhyesti CERT:n toimintaperiaatteesta ja haavoittuvuuksien tilastoinnista. Esitin tutkimuksen tulokset erilaisilla kuvaajilla, joiden avulla arvioin CERT:n julkaisemien tieturvahaavoittuvuuksien kehitystä vuosina 2002–2013.

Työn tarkoituksena oli perehtyä palvelunestohyökkäysten taustoihin ja niiden yleistymiseen sekä tutustua tietoturvan peruskäsitteisiin yritysten näkökulmasta. Työlle asetut tavoitteet täyttyivät onnistuneesti. Työssä käytiin selkeästi läpi palvelunestohyökkäysten taustoja ja tarkoitusperiä. Työ antaa myös hyvän kuvan palvelunestohyökkäysten merkittävyydestä verrattuna muihin tietoturvauhkiin. Työ on hyvä yleisteos yhdestä nykypäivän merkittävästä tietoturvauhasta, joka vaikuttaa monen yrityksen ja organisaation onnistuneeseen tietoturvakokonaisuuteen.

Lähteet

1. Tietoturva. 2013 Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Tietoturva>. Luettu 4.3.2014.

2. Järvinen Petteri. 2006. Paranna tietoturvaasi. Porvoo: Docendo.

3. Morris worm. 2014 Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Morris_worm>. Luettu 10.3.2014.

4. Koskinen Jukka, Komssi Tuukka, Peltotalo Jani, Peltotalo Sami, Viitanen Tommi. 2005. Palvelunestohyökkäyksen havaitseminen ja torjuminen – Seminaariraportti. Tampereen teknillinen yliopisto.

5. YLE Uutiset 2014 Verkkodokumentti. YLE. <http://yle.fi/uutiset/hakkerit_kaatoivat_kremlin_ja_venajan_keskuspankin_nettisivut/7137157>. Luettu 22.3. 2014.

6. MTV3 Uutiset. 2014 Verkkodokumentti. MTV3 <http://www.mtv.fi/uutiset/it/artikkeli/naton-nettisivuille-tehty-verkkohyokkayksia-/3105326>. Luettu 22.3.2014.

7. Talouselämä Uutiset. 2014 Verkkodokumentti. Talouselämä. <http://www.talouselama.fi/uutiset/sijoittajien+paniikki+ja+palvelunestohyokkays++virtuaaliraha+bitcoinin+katastrofi+syvenee/a2179302>. Luettu 22.3.2014.

8. Hakala Mika, Vainio Mika, Vuorinen Olli. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo.

9. Smurf attack. 2014 Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Smurf_attack>. Luettu 7.4.2014.

10. Tietoturva nyt! 2007. Verkkodokumentti. CERT.
<https://www.cert.fi/tietoturvanyt/2007/05/P_12.html>.
Luettu 7.4.2014.

11. Tietoturva nyt! 2012. Verkkodokumentti. CERT.
<https://www.cert.fi/tietoturvanyt/2012/12/ttn201212281525.html>.
Luettu 8.4.2014.

12. Rikoslaki. 1995. Verkkodokumentti. Finlex
<http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001>.
Luettu 9.4.2014.

13. Juppi Eetu, Juppi Elmo. 2008 Palvelunestohyökkäykset ja muut yrityksen tietoturvauhat. Opinnäytetyö. Kajaanin ammattikorkeakoulu.

14. CERT Tietoturvakatsaus 2/2012. 2012. Verkkodokumentti. CERT.
<https://www.cert.fi/katsaukset/2012/tietoturvakatsaus_2-2012/ddos.html>.
Luettu 13.4.2014.

15. YLE Uutiset. 2012. Verkkodokumentti. YLE.
<http://yle.fi/uutiset/ylen_nettisivut_toimivat_jalleen/6429805>.
Luettu 12.4.2014.

16. Tietoturva nyt! 2012. Verkkodokumentti. CERT.
<https://www.cert.fi/tietoturvanyt/2012/12/ttn201212271548.html>.
Luettu 12.4.2014.

17. Tietoturva nyt! 2013. Verkkodokumentti. CERT.
<https://www.cert.fi/tietoturvanyt/2013/03/ttn201303251530.html>.
Luettu 12.4.2014.

18. New York Times Technology. 2013. Verkkodokumentti. New York Times.
<http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=1&>.
Luettu 12.4.2014.

19. Kyberturvallisuuskeskus – Haavoittuvuudet. 2010. Verkkodokumentti. CERT. <https://www.cert.fi/haavoittuvuudet.html>. Luettu 13.4.2014.

20. Digitoday Tietoturva. 2005. Verkkodokumentti. Digitoday <http://www.digitoday.fi/tietoturva/2005/05/17/palvelunestolla-kiristaminen-on-jo-arkipaivaa/200511543/66>. Luettu 13.4.2014.

Kuvaajissa käytetyt tarkat numeroarvot.

	Kaikki tiedotteet	Palvelunesto-hyökkäykset	Komentojen mielivaltainen suorittaminen	Käyttöoikeuksien laajentaminen	Tietojen muokkaaminen	Luottamuksellisen tiedon hankkiminen	Suojauksen ohittaminen	Yhtensä
2014	47	27	28	17	24	26	40	162
2013	150	81	130	43	41	68	58	421
2012	210	79	158	54	32	67	71	461
2011	165	66	133	32	18	45	45	339
2010	193	84	163	39	26	56	43	411
2009	133	82	97	28	25	44	40	316
2008	156	72	104	47	28	42	33	326
2007	191	77	151	50	53	57	48	436
2006	63	11	34	3	4	6	2	60
2005	89	8	52	7	5	9	2	83
2004	93	30	70	7	8	8	4	127
2003	84	30	51	11	3	9	3	107
2002	93	41	64	20	8	12	4	149
Yht.	1667	688	1235	358	275	449	393	3398