Ohje 3/2016 Palvelunestohyökkäysten ehkäisy ja torjunta

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Palvelunestohyökkäys voi haitata liiketoimintaa

Palvelunestohyökkäysten (englanniksi denial of service, DoS) merkitys on kasvanut sitä mukaa, kun yhteiskunta ja liiketoiminta ovat tulleet riippuvaisemmiksi internetistä. Palvelunestohyökkäykset tulee tuntea sekä ilmiönä että tekniikaltaan, jotta niiltä voi suojautua tehokkaasti. Tässä ohjeessa asioita käsitellään hyökkäykseen varautuvan yrityksen ja sen liiketoiminnan näkökulmasta, mutta sama näkökulma pätee missä tahansa varautuvassa organisaatiossa ja sen ydintehtävässä.

Palvelunestohyökkäys estää tietojen saatavuutta

Palvelunestohyökkäykset ovat jokapäiväinen ilmiö internetissä. Palvelunestohyökkäyksessä tyypillisesti luodaan keinotekoisesti ruuhkaa palveluun esimerkiksi täyttämällä palvelun käyttämän nettiliittymän kaista tai aiheuttamalla jollekin palveluketjussa olevalle laitteelle niin paljon prosessointikuormaa, että palvelu hyytyy siihen (distributed denial of service, DDoS). Pullonkaulaksi voi muodostua paitsi verkkopalvelin myös esimerkiksi palomuuri.

Tietojärjestelmän häiritseminen niin, etteivät palvelua tarvitsevat henkilöt pysty käyttämään sitä, on siis selvästi tietoturvapoikkeama. Palvelunestohyökkäyksen seuraukset palvelun käyttäjille vaihtelevat huomaamattomasta kiusallisen kautta aina katastrofiin asti. Seuraukset riippuvat siitä, miten paljon käyttäjä tarvitsee palvelua hyökkäyksen aikana ja miten nopeasti palvelu pystyy palautumaan normaaliin tilaan.

Palvelunestohyökkäys ei kuitenkaan tarkoita murtautumista palveluun eikä se vaikuta muihin tietoturvallisuuden keskeisiin mittareihin: tietojen luottamuksellisuuteen ja eheyteen.

Hyökkäysten motiiveja

Suurin osa palvelunestohyökkäyksistä on tehty jonkin aatteen tai erimielisyyden vuoksi. Tällaista toimintaa kutsutaan haktivismiksi. Yksinkertaistaen kyse on mielenosoittamisesta tietoteknisten tietoturvaloukkausten välityksellä. Joku voi hyökätä siksi, että pitää kohteen toimintaa tai toimimatta jäämistä epäeettisenä, toinen siksi, että on muuten vain vihainen.

Kasvava trendi on palvelunestohyökkäyksen uhalla kiristäminen eli puhtaasti rahalliseen hyötyyn tähtäävä rikollinen toiminta. Hajautetun palvelunestohyökkäyksen tekeminen on halpaa eikä se nykyään vaadi tilaajaltaan erityistä teknistä taitoakaan. Kiristyksen dilemma on, ettei uhan todellisuutta pysty ennakolta luotettavasti arvioimaan, jolloin varautumista on vaikea mitoittaa sopivasti. Rikollisten tiedetään kiristäneen yrityksiltä rahaa pelkillä uhkausviesteillä ilman mitään seurauksia lunnaiden maksamatta jättämisestä.

Jos palvelussa on tietynlainen ohjelmistohaavoittuvuus, palvelu voidaan saattaa palvelunestohyökkäykseltä näyttävällä liikenteellä tilaan, jossa myös tietojen luottamuksellisuus tai eheys voi vaarantua. Palvelunestohyökkäykseltä näyttävässä tilanteessa on siis tarkastettava myös palvelinten lokitiedot ja sisältö tunkeutumisten varalta. Palvelunestohyökkäyksiä tiedetään myös käytetyn hämäyksenä, jotta palvelua suojelevien henkilöiden huomio saadaan kiinnitettyä pois päähyökkäyksestä.

Myös yritysten väliseen kilpailuun liittyvät motiivit voivat olla palvelunestohyökkäysten takana. Verkkokaupassa voi riittää se, että kauppasivuston toimintaa hidastetaan, jolloin asiakkaat alkavat siirtyä kilpailevaan verkkokauppaan.

Poliittiset ja diplomaattiset selkkaukset näkyvät nykyään myös kybermaailmassa. Osa selkkausten motivoimista hyökkäyksistä on varmasti koordinoimatonta haktivismia, mutta palvelunestohyökkäyksistä voidaan puhua myös kybersodankäynnin välineenä.

Joskus palvelunestohyökkäyksillä on myös sivullisia uhreja. Tietotekniikan keskittyessä useita yrityksiä palvelevien IT-yritysten palvelinsaleihin (ns. hosting-yritykset) voi toista yritystä kohtaan tehty hyökkäys haitata muiden samaa palvelua käyttävien yritysten toimintaa.

Palvelunestohyökkäyksen voi toteuttaa usealla tavalla

Tavallisimmin palvelunestohyökkäykset ovat hajautettuja eli hyökkäys tapahtuu lähettämällä kohteeseen tietoliikennettä samanaikaisesti useista lähteistä. Hyökkääjä voi suoraan hallita liikenteen lähteitä tai hän voi käyttää sivullisia osapuolia hyökkäyksen välikappaleina.

Puolustajan on tärkeä tuntea hyvin tietojenkäsittelyjärjestelmänsä ja palvelunsa. Hyökkäyksen vaikutukset saattavat näkyä ensin jossakin korkean tason palvelussa esimerkiksi toiminnan hidastumisena tai ajoittaisena katkeiluna. Häiriön juurisyy voi kuitenkin olla jossakin aivan muualla. Torjuntatoimien onnistuminen on paljolti kiinni siitä, osataanko alkusyytä etsiä oikeasta paikasta ja ymmärretäänkö häiriön leviämismekanismi. Hätäisillä torjuntatoimilla saatetaan jopa pahentaa hyökkäyksen vaikutuksia entisestään.

Hyökkäystyypit voidaan karkeasti jakaa matalan tason tietoliikenneprotokollilla tehtäviin liikennetulviin, keskitason protokollilla tehtäviin palvelinten ja verkkolaitteiden muistiresursseja kuluttaviin hyökkäyksiin sekä sovellustason protokollia hyödyntäviin hyökkäyksiin. Mitä korkeamman tason hyökkäyksestä on kyse, sitä enemmän palvelun omistajalla ja ylläpitäjällä on vaikutusmahdollisuuksia torjuntaan. Vastaavasti matalan tason hyökkäysten torjunnassa tarvitaan yleensä internetoperaattoreiden apua.

Palvelunestohyökkäysten tekniikkaa käsitellään tarkemmin tämän ohjeen liitteessä 1; katso Lisätietoja-luku.

Tunnista varautumistarpeesi

Internetissä tarjottavien palvelujen suojaamiseksi voi tehdä paljonkin. Aina ei täydelliseen suojaukseen edes kannata pyrkiä, mutta jos esimerkiksi yrityksen liiketoiminta perustuu sen tarjoamiin sähköisiin asiointipalveluihin, väärinkäytöksiltä suojautumiseen kannattaa panostaa. Kyse ei ole sen kummemmasta kuin organisaation riskien hallinnasta samaan tapaan kuin varaudutaan onnettomuuksiin ja tavanomaisiin rikoksiin.

Kannattaa miettiä, mitkä omista palveluista voivat olla palvelunestohyökkäyksen kohteena ja millainen merkitys sillä on liiketoimintaan ja maineeseen. Minkä palveluiden tulee toimia myös kuormitustilanteessa? Miltä tilanne näyttäisi, jos siitä joutuisi lukemaan lehden pääuutisesta?

Palvelunestohyökkäyksen tehokas torjuminen voi vaatia sellaista asiantuntemusta ja laitteistoa, jota ei normaalisti ole käytettävissä. Jos palvelun toimivuus on yritykselle tärkeää, on poikkeustilanteisiin varautuminen otettava huomioon jo palvelun toteutusta suunniteltaessa — vähintään on tiedettävä, mistä ja minkälaisella aikataululla asiantuntija-apua on saatavilla.

Suojaudu jo etukäteen

Tärkeimmät toimenpiteet palvelunestohyökkäysten torjumiseksi ja niistä toipumiseksi tehdään ennen hyökkäyksiä.

Rakenna palvelut sietokykyisiksi

Testaa ja tutki verkkopalvelun haavoittuvuudet ja ominaisuudet, joita voidaan käyttää palvelunestohyökkäyksen toteuttamiseen. Esimerkiksi jos palvelu sallii kirjautumattoman käyttäjän suorittaa rajoittamattoman määrän hakuja, joista aiheutuu pitkäkestoinen tietokantakysely, palvelua voi kuormittua hyvin yksinkertaisella tavalla.

Jos webbipalvelulle pystyy aiheuttamaan palvelunestotilan helposti tekemällä esimerkiksi dynaamiselle sisällönhallintajärjestelmälle (CMS) paljon rinnakkaisia sivulatauksia, kannattaa miettiä reverse-proxy- tai välimuistiratkaisuja. Niissä sivulataukset lähtökohtaisesti palvellaan nopeasti välimuistista ja varsinaiseen CMS:ään asti mennään vain tarvittaessa. CDN:t toimivat usein tällä tavalla.

Kuormitustestaukseen on olemassa valmiita työkaluja ja niitä kannattaa käyttää suorituskyvyn varmistamiseen. Jos testaus tehdään internetin yli, asiasta kannattaa sopia etukäteen teleoperaattorin kanssa, jotta sen verkonvalvonnassa ei tehdä testistä väärää hälytystä.

Ei kaikkia munia samaan koriin

Jos palvelunestoliikenne julkisiin verkkosivuihin käyttää samaa kaistaa kuin organisaation etätyöntekijöiden tai alihankkijoiden VPN-yhteydet, voi verkkosivuihin kohdistuva DDoS lamauttaa koko organisaation toiminnan.

Sijoita palvelut siten, että ulkoisten palveluiden estyminen ei vaikuta sisäisten palveluiden toimintaan. Ulkoiset verkkopalvelut kannattaa segmentoida tai sijoittaa ulkoisten palveluntarjoajien verkkoon tai content delivery networkiin (CDN) siten, että DDoS:lla olisi mahdollisimman vähän vaikutusta organisaation omaan toimintaan ja mahdollisesti pienempiin rajatuille ryhmille tarjottuihin tärkeisiin palveluihin. Huomioi omat kriittiset viestintäkanavasi, jotta saat hyökkäyksen aikana yhteyden esimerkiksi teleoperaattoriisi.

Hyökkäysten vaikutuksia voi pienentää myös se, että palvelu ei ole vain yhden koneen ja osoitteen varassa. Palvelinten kesken kuormaa tasaavat ja yhteyksien määrää rajoittavat laitteet voivat pitää palvelun toiminnassa, vaikka sen käyttäminen hyökkäyksen aikana hidastuisikin. Hajauttamiseen voidaan käyttää myös nimipalvelusta samalla nimellä löytyviä eri IP-osoitteissa toimivia palvelimia.

Todella laajalti käytetyt ja suositut palvelut, kuten hakukoneet, on hajautettu maantieteellisesti niin, että samaa palvelua tarjotaan eri puolilla maailmaa olevilta palvelimilta. Käyttäjien yhteydet ohjataan verkon kannalta otollisimmassa paikassa olevalle palvelimelle.

Yksinkertainen tapa jakaa kuormaa on kopioida suosittua tietosisältöä eri palvelimille ja ohjata käyttäjät hakemaan tietoa eri paikoista esimerkiksi www-sivulla olevan linkkilistan avulla. Monia suosittuja ohjelmistoja jaetaankin peilaamalla (mirror) jaettavat tiedostot eri palvelimille.

Palveluiden hajauttamiseksi suojaan palvelunestohyökkäyksiltä voi kääntyä suojauspalvelua tarjoavien yritysten puoleen (kansainvälisesti tunnettuja

palveluntarjoajia ovat esimerkiksi Cloudflare ja Akamai) tai rakentaa vastaava kyky itse. Keskeinen tekniikka hajautuksen toteuttamisessa on jokulähetykseksi kutsuttu reititystapa (englanniksi anycast).

Sopivasti kapasiteettia

Yksinkertainen — joskaan ei aina halpa — tapa suojautua palvelunestohyökkäyksiltä on järjestelmien ja verkkoyhteyksien reipas ylimitoittaminen niin, että vain kaikkein suurimmilla hyökkäyksillä on vaikutusta palvelutasoon. Järjestelmän osien tulee kuitenkin olla ominaisuuksiltaan tasapainossa. Jos palvelinten tai palomuurin kapasiteetti on pieni tietoliikenneyhteyksien nopeuteen verrattuna, liittymän nopeuden keinotekoinen rajaaminen teleyrityksen päässä voi auttaa pitämään ne pystyssä.

Toisaalta siirtotienkin voi saada tukkoon yksinkertaisella liikennetulvalla. Sallitun liikenteen yksilöiminen sekä hyökkäysliikenteen tunnistaminen ja suodattaminen pitkin siirtotietä ja palvelun eri vaiheessa on tärkeä osa tasapainoista varautumista.

Suodata ylimääräinen liikenne

Suojautua voi myös pyrkimällä erottelemaan vihamieliset yhteydet palveluiden normaalikäyttäjistä. Hajautettujen hyökkäysten torjuminen pelkästään IP-osoitteiden perusteella ei useinkaan ole tehokasta, koska hyökkääjä voi käyttää suurta määrää osoitteita ja samalla suodattimeen voi osua oikeitakin palvelun asiakkaita. IP-osoitteiden maantieteellisen sijainnin perusteella tehtävä suodatus on toisinaan toimiva ratkaisu, sillä suurin osa boteista sijaitsee Suomen ulkopuolella.

Protokollan vastaiset yhteydet voidaan kuitenkin usein tunnistaa, jolloin niiden pääsy palvelimia kuormittamaan on mahdollista estää. Tämä edellyttää joko varta vasten verkko- tai sovellusliikenteen suodattamiseen tarkoitettuja laitteita tai ainakin siihen soveltuvia ominaisuuksia esimerkiksi palomuurilta. Usein käytettyjä suodatusperusteita ovat liian isot paketit tai ylimääräiset kentät.

Palvelimille ei pitäisi normaalitilanteessakaan päästää muuta kuin palvelun toteuttamisen ja ylläpitämisen kannalta tarpeellista liikennettä. Ylimääräinen tulee suodattaa pois.

Suodatustapoja on voitava luoda ja muuttaa tilanteen mukaan niin, että kulloinkin kyseessä olevan hyökkäyksen erityispiirteisiin voidaan tarpeen mukaan reagoida. Suodatuksen periaatteista on syytä sopia oman internetpalveluntarjoajan kanssa jo ennen hyökkäyksiä. Hyökkäyksen jo ollessa käynnissä sallittua liikennettä voi olla hyvin hankala ryhtyä erottelemaan hyökkäysliikenteestä.

Liikenteen analysointi normaalitilanteessa on hyvää harjoitusta hyökkäystilanteen varalle. Analysointia kannatta harjoitella myös mahdollisimman yksinkertaisilla työkaluilla (esimerkiksi tekstimuotoisten lokien prosessointiohjelmilla; UNIX-maailmassa esimerkiksi grep, cut, sort, uniq) siltä varalta, että monimutkaisemmat ohjelmat tukehtuvat hyökkäystilanteessa kasvaneeseen datamäärään.

Vinkkejä DNS-pohjaisten hajautettujen palvelunestohyökkäysten torjuntaan: http://blog.fortinet.com/post/10-simple-ways-to-mitigate-dns-based-ddos-attacks

Älä ole palvelunestohyökkäyksen välikappale

Usein palvelimet, kotitietokoneet, kotireitittimet tai esineiden internetin laitteet voivat osallistua palvelunestohyökkäykseen omistajansa tietämättä. Tähän on kolme pääasiallista syytä: inter-

netiin avoimet palvelut, heikot suojausasetukset tai oletusasetukset ja päivittämättömät ohjelmistot.

Sulje tarpeettomat palvelut

Poista käytöstä ominaisuudet ja palvelut, joita et tarvitse. Tämä koskee niin palvelimia, työasemia kuin verkon aktiivilaitteita niin yrityksessä kuin kotonakin. Esimerkiksi kotireitittimiä ja myös esineiden internetin laitteita murretaan ja liitetään osaksi bottiverkkoa.

Sen lisäksi, että internetiin avoimet palvelut lisäävät hyökkäyspinta-alaa tietomurroille, osaa internetiin avoimista palveluista voi hyödyntää palvelunestohyökkäyksien vahvistimina, jolloin puhutaan vahvistin- tai peilaushyökkäyksistä (amplification attack, reflection attack). Tarkasta ainakin UPnP, SNMP, SSDP, NetBIOS, NTP, multicast DNS (mDNS) ja RIPv1. Peilatuista palvelunestohyökkäyksistä ja niihin liittyvistä protokollista on kerrottu tarkemmin liitteessä 1.

Älä käytä oletussalasanoja ja oletusasetuksia

Oletussalasanat tai heikot salasanat voivat mahdollistaa tietomurron laitteisiin, jolloin laitteisiin voidaan asentaa haittaohjelma, joka liittää ne osaksi palvelunestohyökkäyksiin osallistuvaa bottiverkkoa.

Vaihda siis laitteiden oletussalasanat vahvoihin.

Lisäksi tarkista oletusasetukset, ja poista käytöstä ylimääräiset palvelut ja rajaa tarpeellisten palveluiden käyttö niihin toimintoihin, joita itse tarvitset.

Asenna korjauspäivitykset

Usein ohjelmistojen haavoittuvuuksia voi käyttää palvelunestohyökkäyksiin. Haavoittuvuuksia, jotka voivat liittyä esimerkiksi puutteelliseen syötteentarkistukseen ja virheeseen tilakoneessa, löytyy jatkuvasti palvelimista, verkon aktiivilaitteista — myös kotireitittimistä.

Seuraa ylläpitämiesi laitteiden haavoittuvuustiedotteita suoraan valmistajalta ja Viestintäviraston Kyberturvallisuuskeskuksen tiedotteissa. Päivitä laitteesi aina, kun korjauksia on saatavilla; erityisesti jos laite on suoraan internetissä kiinni.

Valvonta ja reagointikyky

Jatkuva valvonta IDS-järjestelmällä auttaa huomaamaan, mikä on tavanomaista liikennettä ja mikä ei. Hyödyllisiä mittareita ovat esimerkiksi liikenne- tai kyselymäärät, palvelinten ja verkkolaitteiden prosessorikuorma ja muistinkulutus ja sykesignaali (englanniksi heartbeat). Tällöin palvelunestohyökkäystilanne voidaan havaita pian sen alkaessa ja reagoida nopeammin. Tarkkaile palvelusi toimintaa jo hyvän sään aikana, jotta osaat erottaa merkittävät poikkeamat tavanomaisesta käytön vaihtelusta.

Nopea reagointi edellyttää, että hälytyksiä on helppo valvoa. Tarvittaessa ne voi välittää ATK-tuen päivystäjälle esimerkiksi tekstiviestillä. Lisäksi hälytysten kynnysarvot pitää säätää sellaiseksi, että vääriä hälytyksiä ei tule liikaa.

Toiminta palvelunestohyökkäystilanteessa

Tässä luvussa on yleisiä ohjeita päällä oleviin hyökkäystilanteisiin. Tiivis muistilista on tämän ohjeen liitteessä 2; katso Lisätietoja-luku.

Suodata ja väistä

Tarkista suodatus- ja väistötoimenpiteet ja tee niitä tarvittaessa lisää. Muokkaa suodatustoimia liikenteen mukaan. Hyökkäyksen aikana mahdollisia suodatus- ja väistötoimia voivat olla muiden muassa:

- "Ylimääräisten" protokollien suodatus yhdessä operaattorin kanssa. HTTP-palvelimelle ei tarvitse mennä esimerkiksi DNS-liikennettä.
- Protokollan vastaisen liikenteen suodatus yhdessä operaattorin kanssa. Hyökkäyspaketeissa voi olla ylimääräisiä tai puuttuvia kenttiä, jotka poikkeavat normaalista.
- IP-osoitteiden perusteella suodattaminen. Tämä ei yleensä kuitenkaan ole tehokasta hajautettujen hyökkäysten tapauksessa.
- Jos hyökkäys tehdään tietyntyyppisillä kyselyillä, jotka kuormittavat palvelinta, näiden kyselyiden määrää voi rajoittaa ajanjaksolla per IP-osoite (englanniksi rate limit).
- Ohjaa verkkosivu erityiselle ruuhkasivulle, joka on eri osoitteessa kuin varsinainen, hyökkäyksen alle joutunut palvelu.

Osaa etukäteistoimenpiteiden kohdalla mainituista voi soveltaa myös hyökkäystilanteen aikana, jos niitä ei ole otettu käyttöön aiemmin. Tällaisia ovat muiden muassa:

- Palvelimen hyväksymien yhteysmäärien ja timeout-arvojen muutokset
- Ylimääräisten avonaisten palveluiden sulkeminen

Aina palvelunestohyökkäykselle ei kuitenkaan voi tehdä mitään, varsinkin jos hyökkäys vie kaiken tietoliikennekaistan.

Yhteistyö operaattorin ja Viestintäviraston kanssa

Ota yhteyttä operaattoriin, joka voi suodattaa liikennettä tai tehdä reititysmuutoksia. Operaattorit toimivat yhteistyössä keskenään ja kansainvälisten operaattorien kanssa. He voivat tarvittaessa suodattamalla tai reititysmuutoksilla torjua palvelunestoliikennettä ennen kuin se pääsee kohteen verkkoon. **Toiminnasta ja mahdollisesta automaattisesta suodattamisesta kannattaa sopia jo etukäteen.**

Tee rikosilmoitus

Kyberrikosten tutkimista pidetään monesti vaikeana, sillä rikosten tekijöiden on mahdollista väärentää ja hävittää monia tekojensa jälkiä. Tekijöiden saaminen vastuuseen ei kuitenkaan ole mahdotonta, sillä taitavakin rikollinen tekee virheitä. Rikosilmoitus on silti välttämätön edellytys rikoksen tutkimiselle.

Vaikka kaikkia rikoksia ei saada heti ratkaistua, rikosilmoituksen tekeminen tuoreeltaan kannattaa. Useissa suomalaisissa palvelunestohyökkäystapauksissa poliisi ja Viestintäviraston Kyberturvallisuuskeskus löysivät todisteita muista samojen henkilöiden tekemiksi epäillyistä kyberrikoksista. Kun rikoksista on ilmoitettu heti niiden tapahduttua, saa poliisi kerättyä luotettavampaa todis-

tusaineistoa ja voi myös torjua uusia rikoksia.

Lue lisää:

- Tietoturva nyt! Kyberrikoksista jää kiinni — rikoksista kannattaa ilmoittaa https://www.viestintavirasto.fi//2015/12/ttn201512071630

- Tietoturva nyt! Poliisi otti kiinni palvelunestohyökkäysten tekijöiksi epäillyt https://www.viestintavirasto.fi/2016/03/ttn201603291639

Lisätietoja

Liite 1 Palvelunestohyökkäysten tekniikkaa puolustajille https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje32016palvelunestohyokkaystenehkaisyjatorjunta.html

Liite 2 Toimintaohjeet palvelunestohyökkäyksen kohteeksi joutuneelle

DDoS Overview and Incident Response Guide. CERT-EU, July 2014 http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_09_DDoS_final.pdf

DDoS Quick Guide. US-CERT, 29.1.2014 https://www.us-cert.gov/security-publications/DDoS-Quick-Guide

Guide to DDoS protection. Protonmail blog 15.12.2015 https://protonmail.com/blog/ddos-protection-guide/

Tietoturva nyt! Verkkorikollisuus ja pimeä verkko — verkkorikollisille suunnatuilla palveluilla omat markkinansa https://www.viestintavirasto.fi/2016/03/ttn201603021442

Tietoturva nyt! Heikosti ylläpidetyt kotireitittimet ovat verkkorikollisten kohteena — osa 1 https://www.viestintavirasto.fi/2015/10/ttn201510121051

Tietoturva nyt! Heikosti ylläpidetyt kotireitittimet ovat verkkorikollisten kohteena — osa 2 https://www.viestintavirasto.fi/2015/10/ttn201510201051

Tietoturva nyt! Peilatut palvelunestohyökkäykset edelleen internetin riesana https://www.viestintavirasto.fi/2014/02/ttn201402101546

Ohje 2/2016 Verkkosivujesi pimeä puoli — Ohjeita sisällönhallintajärjestelmien kyberuhkien torjumiseksi https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje22016verkkosivujesipimeapuoli-ohjeitasisallonhallintajarjestelmienkyberuhkientorjumiseksi.html

Tietoturva nyt! Verkon käyttäjiä tahtomattaan palvelunestohyökkäyksissä https://www.viestintavirasto.fi/2012/01/ttn201201271148

Tietoturva nyt! [Teema] Tietoverkkorikollisuus — rikoksia verkossa tai verkon avulla https://www.viestintavirasto.fi/2015/05/ttn201506031327

Layer seven DDoS attacks. Infosec institute, 24.10.2013 http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

Lizard Squad now selling DDoS attacks as a service for as little as $6 a month. Techspot, 2.1.2015 http://www.techspot.com/news/59274-lizard-squad-now-selling-ddos-attacks-service-little.html

$38 an hour is the cost of destructive DDoS Attacks. Security affairs, 15.6.2015 http://securityaffairs.co/wordpress/37819/cyber-crime/cost-of-ddos-attacks.html

Application Denial of Service. Is it Really That Easy? OWASP/Hacktics, May 2007 https://www.owasp.org/images/d/da/OWASP_IL_7_Application_DOS.pdf

Sanasto

amplification: katso *vahvistus*.

botti: hyökkääjän ohjauksessa oleva sivullisen tahon tietokone tai sivullisen tietokoneessa toimiva etäohjattava haittaohjelma (englanniksi bot).

cache: katso välimuisti.

CDN: verkkosisältöjen hajautettu jakelujärjestelmä (englanniksi content delivery network). Hajautetuilla jakelujärjestelmillä voidaan parantaa verkkopalvelun kapasiteettia ja häiriösietoisuutta.

CMS: verkkosivujen sisällönhallintajärjestelmä (englanniksi content management system). Esimerkiksi WordPress ja Joomla ovat suosittuja sisällönhallintajärjestelmiä.

DoS: palvelunestohyökkäys (englanniksi denial of service); mikä tahansa keino, jolla estetään tietojenkäsittelypalvelun käyttö siihen oikeutetuilta henkilöiltä.

DDoS: hajautettu palvelunestohyökkäys (distributed denial of service); useasta lähteestä tulevaa verkkoliikennettä, joka aiheuttaa palvelunestotilan.

DNS: internetin nimipalvelu (englanniksi domain name service tai system); muuntaa ihmisen luettavat verkkonimet IP-osoitteiksi.

heijastus: väärennetyn liikenteen lähettäminen jollekin hajautetun palvelunestohyökkäyksen välikappaleena toimivalle palvelulle niin, että välikappale lähettää vastausliikenteen hyökkäyksen kohteelle eikä alkuperäiselle lähettäjälle (englanniksi reflection).

reflection: katso *heijastus*.

reverse proxy: palvelun kapasiteetti parantava toiminto, jossa palvelun muuttuvasta sisällöstä koostettua tulosta pidetään hetken aikaa työmuistissa sen sijaan, että sisältö koottaisiin jokaiseen pyyntöön erikseen. Katso myös *välimuisti*.

TCP: internetin yhteyskäytäntö, jossa tietokoneet varmistavat keskinäisen yhteytensä ennen varsinaista tiedonsiirtoa (transmission control protocol).

UDP: internetin yhteyskäytäntö, jossa tiedonsiirto alkaa ilman alkukättelyä (user datagram protocol); hyökkääjä voi lähettää dataa väärennetyllä lähdeosoitteella.

vahvistus: liikennemäärän lisääminen jonkin palvelunestohyökkäyksen välikappaleena toimivan palvelun kautta. Katso myös heijastus.

välimuisti: yksittäisen palvelimen toiminto, jossa palvelimen muuttuvasta sisällöstä koostettua tulosta pidetään hetken aikaa työmuistissa sen sijaan, että sisältö koottaisiin jokaiseen pyyntöön erikseen (englanniksi cache). Katso myös *reverse proxy*.

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi