

Palvelunestohyökkäykseltä voi suojautua

15.6. 09:58 (päivitetty 11:01) — Antti Kirves

Palvelunesto- eli DoS-hyökkäyksissä (Denial of Service) kohdejärjestelmän tai -palvelun resursseja kuormitetaan niin paljon, että se lakkaa vastaamasta.

Ongelmia aiheuttavat enemmän hajautetut palvelunestohyökkäykset (DDoS, Distributed Denial of Service), jotka voivat tulla miljoonista osoitteista.

- Ilmiö ei ole uusi, mutta se kehittyy ja muuttuu. Siksikin torjunta on välillä vaikeaa. Kaiken ratkaisevaa hopealuotia on harvoin tarjolla, sanoo Fujitsun tietoturvapäällikkö **Tuomas Kaijanen**.

Monenlaisia hyökkäyksiä

Palvelunestohyökkäys voi kohdistua verkkoliikenteeseen, jolloin puhutaan tulvahyökkäyksestä. Esimerkiksi web-palvelinta voidaan kuormittaa erityyppisillä hyökkäyksillä niin, että järjestelmän kapasiteetti loppuu. Hyökkääjä voi myös käyttää hyväkseen erilaisia haavoittuvuuksia kohdejärjestelmässä.

Voimakkaalla hyökkäyksellä pyritään kaatamaan palvelu hetkellisesti.

Jotkin haittaohjelmat taas hyökkäävät automaattisesti ja jatkuvasti aina kun pystyvät. Ne voivat levitä aina vain uusiin koneisiin, mikä vaikeuttaa torjuntaa.

Haittaohjelmien avulla voidaan myös rakentaa haltuun otetuista koneista muodostettuja bottiverkkoja hyökkäyksiä varten.

Iskun voi torjua

Perussuojaus DDoS-hyökkäyksiä vastaan saataisiin jo ylimitoittamalla palvelun kapasiteetti. Moni yritys välttää tätä, koska se ei välttämättä ole kovin edullista.

Yritykset käyttävät DDoS-hyökkäysten torjuntaan palomureja, hyökkäyksen estojärjestelmiä (Intrusion Prevention System, IPS) ja kuormantasauslaitteita. Järjestelmien ja laitteiden hinnat vaihtelevat muutamasta tuhannesta kymmeneen

tuhansiin euroihin.

Ips torjuu parhaiten haavoittuvuus pohjaisia hyökkäyksiä suodattamalla hyökkäysliikenteen ennen kuin se ehtii kohdejärjestelmään. Paljon voi nykyisin tehdä jo palomuurillakin.

- Parhaiten tehoa suojaus, jossa palvelunestohyökkäys pysäytetään lähellä sen lähdettä. Tällä tavoin pyritään pysäyttämään vain hyökkäysliikenne. Jos hyökkäys pysäytetään lähellä kohdetta, pysäytetään usein samalla myös laillista liikennettä, sanoo tuotemerkkinointipäällikkö **Klaus Majewski** Stonesoftista.

Apua operaattorilta

Usein yrityksen internetyhteydestä tulee pullonkaula, joka tukkeutuu hyökkäysliikenteestä. Silloin yrityksen omista torjuntalaitteista ei ole apua. Laillinen liikenne ei pääse koskaan yritykseen asti.

- Akuuteissa tilanteissa on voitu sulkea tiettyjä osoiteavaruuksia pois. Se on kriisinhallintaa ja ratkaisuna väliaikainen, sanoo Kaijanen.

Verkkoyhteyden tukkivia palvelunestohyökkäyksiä voivat pysäyttää internetoperaattorit. Yrityksen omat toimet eivät yleensä tehoa, koska ne harvoin itse hallitsevat omia nettiyhteyksiään.

Jos liikenteen pullonkaula on yrityksen internetyhteydessä, ip-osoitteiden sulkeminen yrityksen omissa puolustusmekanismeissa ei auta. Internetoperaattorin puolella se taas saattaa auttaa.

- Jos hyökkäykseen ei osallistu tuhansia koneita, vaan esimerkiksi 10-200, ip-osoitteiden sulkeminen on aika tehokaskin torjuntatapa, Majewski sanoo.

<http://www.digitoday.fi/tietoturva/2007/06/15/palvelunestohyokkaykselta-voi-suojautua/200714925/66>