



22.5.2007



YLIMÄÄRÄINEN TIETOTURVAKATSAUS 1B/2007

Viime aikojen näkyvimpiä tapahtumia ovat olleet erilaiset palvelunestohyökkäykset. Monenlaisia hyökkäyksiä havaittiin jo vuoden alkupuolella, ja toukokuussa ne nousivat otsikoihin Viron valtionhallinnon ja Yleisradion palveluihin tehtyjen hyökkäysten johdosta. Tutkittujen hyökkäysten toteuttamistavat poikkeavat toisistaan, eikä CERT-FI:n käytettävissä olevien tietojen perusteella tapausten välillä voida osoittaa suoraa yhteyttä.

Palvelunestohyökkäyksessä pyritään ylikuormittamaan kohteena olevaa palvelua niin, ettei sen normaali käyttö ole mahdollista. Hyökkäykset toteutetaan useimmiten joko itsestään leviävien ja toimivien haittaohjelmien tai botnet-verkkojen avulla. Yleisradiota vastaan tehdyssä hyökkäyksessä käytettiin hyväksi p2p-tiedostonjako-ohjelmia.

Virossa hyökättiin valtionhallinnon ja pankkien järjestelmiä vastaan

Virossa on pyritty lamauttamaan valtionhallinnon verkkosivustoja ja lisäksi hyökätty pankkien sivustoja vastaan. Hyökkäykset alkoivat Tallinnan ns. patsaskiistan puhjettua ja jatkuvat edelleen voimakkuudeltaan vaihtelevina. Hyökkäyksiä torjuttiin aluksi sulkemalla pääsy kohteena oleville palvelimille Viron ulkopuolelta, jolloin suurin osa kuormittavasta liikenteestä estyi. Myöhemmin on liikennettä suodatettu sekä IP-osoitteiden että yhteyksien sisällön perusteella.

Palvelunestohyökkäys Yleisradion web-palvelimia vastaan

Yleisradion www-palvelimia vastaan hyökättiin maanantaina 14.5. iltapäivällä, ja hyökkäykset jatkuivat myöhään samana iltana. Niiden vaikutukset olivat havaittavissa vielä seuraavan aamupäivän aikana. Tällöin www.yle.fi -sivusto toimi hitaasti tai ei ajoittain vastannut lainkaan. Hyökkäystä torjuttiin aluksi samalla keinolla kuin Virossakin, eli estämällä pääsy palveluun ulkomailta. Myöhemmin häirintäliikennettä alettiin erottaa normaaliien käyttäjien yhteyksistä analysoimalla sisään tulevien pakettien sisältöä. Yleisradiota vastaan tehdyssä hyökkäyksessä ohjattiin vertaisverkkoperiaatteella toimivan tiedostonjako-ohjelman yhteyspyyntöjä yli sadasta tuhannesta eri IP-osoitteesta kuormittamaan palvelinta.

Hyökkäys Eniron palveluja vastaan

Maanantaina 14.5. ilmoitettiin myös Eniron suomi24.fi -sivuihin kohdistuneesta hyökkäyksestä, joka näkyi palvelun ajoittaisina katkoksina ja hidastumisena. CERT-FI:n tietojen mukaan hyökkäys toteutettiin Yleisradion hyökkäyksestä poikkeavalla tavalla. Kohteena olleet palvelimet sijaitsevat Ruotsissa. Hyökkäys toistui maanantaina 21.5.

Hyökkäysten julkisuus toi myös turhia ilmoituksia

Uutiset palvelunestohyökkäyksistä ovat johtaneet hätäisiin johtopäätöksiin eri verkkopalveluiden käyttökatkosten syistä. Toisaalta palvelujen toimivuutta on myös seurattu tarkasti. CERT-FI:n tietoon ei ole tullut muita palvelunestohyökkäyksiksi luokiteltavia tapahtumia.

Onnistuneet hyökkäykset voivat innostaa uusiin yrityksiin

Monet sähköiset asiointipalvelut ovat osoittautuneet helpoiksi kohteiksi, ja niihin kohdistettuja hyökkäyksiä tehtäneen jatkossakin. Palvelujen tarjoajien tulisi varautua vihamielisten hyökkäysten mahdollisuuteen, ja varmistaa tarpeellinen reagoitukyky poikkeustilanteissa.