

Suurten sivut reikäjuusto

TIETOTEKNIKKA: Jyväskyläläismies löysi krakkerinmentäviä koloja kymmenien yritysten ja virastojen verkkosivuilta.

JYVÄSKYLÄ

Pauliina Kinnunen

Viikonlopuun aikana monien suurten yritysten ja valtion virastojen verkkosivuilta löytyi XSS-haavoittuvuuksia. Tietoturva-asiantuntija Erika Suortti kertoi sunnuntaina, että Viestintäviraston tietoon on tullut useita kymmeniä haavoittuvia sivustoja.

– Viikonlopuun aikana olemme pyrkineet ottamaan yhteyttä kaikkiin niihin tahoihin, joiden sivuilla ongelmia on havaittu. Tietokoneharrastajatkin ovat olleet aktiivisia. Meillä ei kuitenkaan ole tietoa, että tilannetta olisi käytetty hyväksi, Suortti sanoi.

Suuri kiinnostus verkkosivujen turvallisuuteen heräsi Sampo Pankin ongelmien takia. Ongelmat verkkosivuilla näyttävätkin olevan pikemminkin säätö kuin poikkeus. Myös jyväskyläläinen media-alan ammattilainen Mikael Korpela kokosi viikonlopuun aikana listan haavoittuvista verkkosivuista ja toimitti sen Viestintävirastolle.

– Haavoittuvuuksia löytyi miltei kaikilta sivuista, joita keksi kokeilla. Vikojen löytämiseen ei kulunut sivuilla minuutiakaan. Nämä aukot ovat pieniä, mutta kun näistäkään ei ole huolehdittu, saattaa sivulta löytyä pahempiakin ongelmia. Kun esimerkiksi Sampon sivuilla on ollut myös muita ongelmia, mikä estää, ettei muillakin olisi, Korpela huolehti.

"Pankkien aukot vakavimpia"

Mikael Korpelan laitimalla listalla on yli kolmekymmentä suurta toimijaa, muun muassa opetusministeriö, Posti, Patentti- ja rekisterihallitus, Hätäkeskuslaitos, Osuuspankki, Pohjola ja Yle. Korpela löysi haavoittuvuuden myös Keski-suomalaisen-konsernin verkkosivuilta.

Vakavimmaksi löydöksi Korpela nimesi pankin verkkosivujen aukon.

– Pankin edelleenohjaussivulle voi kirjoittaa mitä tahansa koodia, mutta silloinkin sivu näyttää salatulta pankin sivulta, Korpela huomasi.

Krakkeri voi esimerkiksi levittää sähköpostitse tai keskus-telualueella huijauksenlinkkiä tunnettuun verkkokauppaan, josta on löytynyt XSS-haavoittuvuus. Ostaja ohjaillaan sieltä huijattuun verkkopankkiin. Tämä ei vaadi XSS-aukkoja verkkopankissa.

Helsingin kaupungin sivulta löytyi mahdollisuus esittää si-



Mikael Korpela kokeili viikonloppuna yritysten ja virastojen verkkosivujen aukottomuutta. Hän löysi ongelmia yli kahdeltakymmeneltä sivulta. KUVA: JAANA KAUTTO

vuilla kuvitteellisia työpaikkailmoituksia, joiden kautta voisi kerätä henkilötietoja.

Myös Viestintäviraston tietoturva-asiantuntija Suortti pitää pankkien tilannetta huolestuttavimpana.

– Vakuutusyhtiöissä ongelmia ei välttämättä ole kohdistuneet suoja tulille sivuille, tietoturva-asiantuntija kerto.

"Kenties tiedetty, muttei korjattu"

Suojauspuitteet ovat jääneet sivuille koodaajien työn jäljiltä, mutta vastuu on työn tilaajalla.

– Kyse on puhtaasti koodaajien huolimattomuudesta. Ihmisillä otetaan töihin usein niin, ettei koulutuksen tai osaamisen tausta valvota. Esimerkiksi jos pankin sivulta löytyy paljon virheitä, voisiko siitä seurata vaikkapa sakkooja, Korpela kyseli.

Suortin mukaan verkkosivujen XSS-haavoittuvuus ei välittämättä tule yrityksille yllätyksenä.

– Niiden vaaroista on ehkä oltu jopa tietoisia, mutta sivustoa ei olla tarkastettu niitten varalta.

Vaikka tietoja haavoittuvista sivuista on viikonlopuun aikana ryöpynyt, on tilanne tietoturva-asiantuntijan mielestä jo paraneamaan päin.

– On todella ikävää, että jouduttiin mediayläkkään ennen kuin palveluntarjoajat heräävät.

TURVALLISESTI VERKOSSA: OHJEITA

- Sähköpostin mukana tulleita linkkejä ei kannata avata.
- Verkkopankkien ja verkkokauppojen sivuja kannattaa käyttää vain niiden pääsivujen kautta.

Uskon, että loppujen lopuksi jäädään plussan puolelle siinä, että

haavoittuvuudet aletaan ottaa kun haavoista tiedetään ja ne saadaan korjattua.

Krakkerit voivat kerätä pankkitunnusia tai rahaa

JYVÄSKYLÄ

Pauliina Kinnunen

XSS-haavoittuvuus avaa pahimillaan krakkereille keinon kerätä pankkitunnusia tai rahaa. Cross site scripting -hyökkäykseillä (XSS), syötetään www-palvelimelle ohjelmakoodia, joka suoritetaan käyttäjän selaimessa.

Haavoittuvuuden kautta ei voida itse sivustolle, palvelinpäähän, tehdä minkäänlaisia muutoksia. Sen sijaan krakkeri pystyy muokkamaan näkymää ja

lähettämään sen edelleen esimerkiksi sähköpostitse linkin.

Itse sivulle ei siis XSS-haavoittuvuuden kautta voida murtautua. Kalastelusivu näyttää kuitenkin uskottavammalta, kun sisältö saadaan syötettyä tunne-tulle sivulle. Esimerkiksi pankin verkkosivujen XSS-haavoittuvuuden avulla mikä tahansa verkkosivu saadaan tarvittaessa näyttämään pankin salatulta sivulta.

Krakkeriksi kutsutaan henkilöä, joka murtautuu tietojärjestelmään ilman järjestelmästä vastaavan tahan lupaa.

töstä on vuodelta 2005. Silloin Nordean nimissä lähetettiin linkkejä, joilla kerättiin pankkitunnusia ja sitä kautta rahaa.

Viestintävirasto ohjeisti perjantaina verkkosivuillaan, kuinka palvelin voidaan suojaa hyökkäyksiltä. Sivulla annetaan ohjeita myös verkkosivujen käytäjille. Ohjeet löytyvät osoitteesta <http://www.cert.fi>.

Krakkeriksi kutsutaan henkilöä, joka murtautuu tietojärjestelmään ilman järjestelmästä vastaavan tahan lupaa.