

Internetin nimipalveluiden turvastandardi sai vauhtia Kaminsky-reiästä

5.3.2009 16:49 — Jarmo Lahti

Viime kesäinen internetin nimipalvelinjärjestelmän haavoittuvuuden paljastuminen on vauhdittanut 10-vuotiaan DNSSEC-standardin käyttöönottoa maailmalla.

Suomalainen dns-ohjelmistotalo Nixu Software on valmis, .fi-domainia hallinnoiva Viestintävirasto ei kuitenkaan pidä kiirettä.

Tietoturvatutkija **Dan Kaminskyn** viime kesänä paljastama dns-järjestelmän haavoittuvuus nosti internetin nimipalveluun liittyvät tietoturvariskit julkiseen keskusteluun.

Vaikka Kaminsky-haavoittuvuutta vastaan nimipalvelinvalmistajat ovatkin julkaisseet ohjelmistopäivityksiä ja niitä on otettu myös käyttöön, niin täydellinen suojaus edellyttää Nixu Software Oy:n toimitusjohtaja **Juha Holkkolan** mukaan julkisen avaimen menetelmää käyttävän 10-vuotiaan DNSSEC (DNS security extensions) -standardin maailmanlaajuisesta käyttöönottoa.

- Meidän näkövinkkelistämme katsellen esimerkiksi helmikuisesta Helsingin Sanomien ["Kuinka internet pelastettiin" -jutusta](#) jäi kuva, että nimipalvelun turvallisuuteen liittyvät ongelmat olisi tällä erää siirretty pois päiväjärjestyksestä. Näinhän asia ei kuitenkaan ole; kyseessä oli vain riskitason lasku, ei riskien eliminointi, Juha Holkkola sanoo.

Puolen vuoden aikanamerkittävää liikehdintää Viimeisen puolen vuoden aikana maailmalla on hänen mukaansa kuitenkin ollut nähtävissä merkittävää liikehdintää asiassa.

- Miltei kaikki merkittävät tld:t (top level domain, esimerkiksi .com, .net, .maalyhenne jne.) aikovat allekirjoittaa omat ylätasen domaininsa vuosien 2009 ja 2010 kuluessa. Ylätasen verkkotunnuksista suurin .com aiotaan myös allekirjoittaa vuoden 2010 loppuun mennessä, Holkkola kertoo.

- Kun yhtälöön vielä lisätään presidentti **Obaman** hallituksen

antama määräys kaikkien .gov-ylätason alla olevien domainien allekirjoittamisesta vuoden 2009 loppuun mennessä, niin seuraavien 10 kuukauden kuluessa täytyy tapahtua paljon, hän jatkaa.

Nixu Softwaren nimipalvelinten hallintaohjelmisto Name Surferin asiakkaista muun muassa yhdysvaltalaiset palveluntarjoajat ES.net ja One Communications allekirjoittavat hostaamansa .gov-alidomainit vuoden loppuun mennessä.

- Lisäksi Ruotsissa on jo useampiakin yritysasiakkaita, jotka aikovat allekirjoittaa omat .se -tld:n alle kuuluvat domaininsa.

Myös kotimaisen .fi -verkkotunnuksen allekirjoittamiseen alkaa Holkkolan mukaan olla jo jopa jonkinlaiset poliittiset paineet olemassa. Myös muun muassa operaattoripuolella ollaan kiinnostuneita DNSSECistä.

Tällä hetkellä asia on kuitenkin Holkkolan mukaan muna-kana -tilanteessa.

- Ennen kuin Viestintävirasto allekirjoittaa .fi-tld:n, eivät siihen kuuluvien verkkotunnusten omistajat pysty etenemään asiassa, Holkkola toteaa.

Viestintävirastossaollaan varovaisia Viestintäviraston verkkotunnusyksikön päällikkö **Juhani Juselius** vastaa .fi-domainin allekirjoittamisen tilannetta koskevaan kysymykseen It-viikolle ICANNin (Internet Corporation for Assigned Names and Numbers) [kokouksesta Meksikosta](#).

Viestintävirastossa on Juseliuksen mukaan tutkittu DNSSECiä ensimmäisen kerran jo pari vuotta sitten ja seurattu sen jälkeen tilanteen kehittymistä aktiivisesti.

Ennen Kaminsky-haavoittuvuutta standardin haittapuolet voittivat hänen mukaansa fi-juuren osalta hyödyt selvästi.

- Haavoittuvuuden julkaisu kuitenkin käänsi vaa'an toiseen asentoon.

Käyttöönoton suurin este liittyy Juseliuksen mukaan tekniikan kriittisyyteen koko .fi-juuren toiminnan kannalta.

- Pienikin tekninen häiriö tai inhimillinen virhe voi aiheuttaa koko fi-juuren putoamisen internetistä, jolloin vuorokaudessa lähes 200 miljoonaa .fi -päätteisen sähköpostin lähetystä ja www-sivun latautumista epäonnistuisi. Siksi DNSSECiin täytyy suhtautua erittäin suurella vakavuudella ja varata ylläpitoon riittävästi henkilöresursseja, Juselius sanoo.

Vaikka DNSSECistä on käyty keskustelua liikenne- ja viestintäministeriön kanssa, Juselius ei tunnusta havainneensa poliittista painetta.

- Maailmalla tld-rekisterien ja ICANNin piirissä käydään paljon keskustelua DNSSECistä. Yleinen julkinen mielipide on ehkä aavistuksen verran DNSSECin kannalla, mutta esimerkiksi juuri täällä Meksikossa ICANNin kokouksessa kahvipöytäkeskusteluissa esiintyy myös paljon voimakkaita ja perusteltuja mielipiteitä DNSSECiä vastaan, Juselius kertoo.

Nixu Software valmiina kuin lukkari sotaan Nixu Software on [helmikuussa julkistanut](#) Name Surfer -hallintaohjelmistostaan version, jolla yrityksen mukaan onnistuu myös DNSSECin käyttöönotto isoissakin nimipalvelinympäristöissä. Perustuki ilman varsinaista hallintoa Name Surferiin tuli jo kaksi vuotta sitten.

Juha Holkkolan mukaan yrityksen noin 3 000 Name Surfer -asiakkaasta (muun muassa Fortune 500 -yrityksiä ja noin 30 prosenttia maailman 2,5G- (gprs)- ja 3G-palveluntarjoajia sekä Suomessa puolet Talouselämä 20 -listan yrityksistä) päivityksiä uuteen versioon on tehty kymmenistä parin viime viikon aikoina.

Maailman noin 12 miljoonasta nimipalvelimesta valtaosaa hallinnoidaan [Holkkolan mukaan](#) erilaisilla enemmän ja vähemmän avoimen koodin ratkaisuilla. Kymmenesosan luokkaa hoidetaan Microsoftin AD-palvelimilla, joiden mukana tulee DNS-palvelin.

DNS-palvelinten hallintaan erikoistuneita Nixu Softwaren kilpailijoita ovat Infoblox, Nominum ja Bluecat Networks. Niiden myytyjen palvelinten määrät ovat 12 miljoonan kokonaiskakuun suhteutettuna pieniä, muutamia tuhansia tai kymmeniä tuhansia.

Holkkolan mukaan Infoblox ja Nominum eivät tarjoa vielä DNSSECin avaintenluontiin ja zone-tietueiden allekirjoittamiseen mitään, Bluecat on julkaissut oman perustuksensa DNSSECille vasta helmikuussa.

<http://www.digitoday.fi/tietoturva/2009/03/05/internetin-nimipalveluiden-turvastandardi-sai-vauhtia-kaminsky-reiasta/20096086/66>