

Kotimaa 25.8.2014 klo 18:00 | päivitetty 25.8.2014 klo 18:05

Verkkohyökkäys vaaransi VR:n työntekijöiden henkilötiedot

Suomalaisyrittäjien palvelimelle tehty hyökkäys paljastui ulkomailta tulleen vinkin ansiosta. Vaarassa olivat kahdeksan suomalaisen yrityksen työntekijöiden henkilötiedot.



Kuva: Yle

Suomalaisen Arc Technology -yrityksen palvelin joutui verkkohyökkäyksen kohteeksi kuluvan vuoden alussa. Isku osui arkaan kohtaan, sillä palvelimen kautta kirjaututtiin kahdeksan suomalaisen yrityksen tai yhteisön henkilöstötietojärjestelmiin.

Tietomurron tutkinnassa on käynyt ilmi, että hyökkääjät saivat sisäänkirjautumispalvelimen hallintaansa ja käyttivät sitä apuna roskapostituksessa tai muussa laittomassa toiminnassa.

– Tietoturva-arvioinnin mukaan sieltä on voinut lähteä porttiskannausta, roskapostia tai jotain tällaista. Hyökkäys näyttää tulleen Venezuelasta ja kohdistuneen Suomesta Brasiliaan, kertoo henkilöstötietojärjestelmiä toimittavan Arc Technologyn hallituksen puheenjohtaja Kimmo Koivu.

Murretun palvelimen kautta kirjaututtiin VR:n, Oriolan, Verohallinnon ja viiden muun yrityksen tai yhteisön henkilötietojärjestelmiin.

VR:n tietohallintojohtaja Jukka-Pekka Suonikko pitää tapausta vakavana. Jo palvelimen

kaappaaminen verkkohyökkäyksen työkaluksi on harmillinen tapaus, mutta vakavinta on työntekijöiden henkilötietojen vaarantuminen.

Tietojen varastaminen mahdollista

Pelkästään VR:n henkilöstötietojärjestelmässä on noin 10 000 ihmisen nimet, sosiaaliturvatunnukset ja tietoja palkkauksesta. Halutessaan hyökkääjät olisivat voineet päästä käsiksi tietokantoihin ja varastaa tietoja.

”

Tiedetään, että taitava hakkeri olisi pystynyt menemään myös henkilöstöjärjestelmään ja hakemaan sieltä jotain.

– *Jukka-Pekka Suonikko, VR:n tietohallintojohtaja*

– Tämäntyyppisissä tapauksissa emme voi koskaan olla täysin varmoja, mitä järjestelmässä on tapahtunut. Tiedetään, että taitava hakkeri olisi pystynyt menemään myös henkilöstöjärjestelmään ja hakemaan sieltä jotain, sanoo Suonikko ja muistuttaa, että toistaiseksi varkaudesta ei ole näyttöä.

Hyökkäykseen havahduttiin, kun Brasilian tietoturvaviranomainen kiinnitti huomiota Suomessa olevalta palvelimelta tulevaan asiattomaan tietoliikenteeseen ja ilmoitti asiasta Suomeen. Ensimmäisenä Arc Technologyn väki veti palvelimen sähköt irti. Saman tien myös yritysten henkilöstötietojärjestelmät kaatuivat.

Käyttökätkön jälkeen VR ja Arc Technology palkkasivat ulkopuolisen tietoturvakonsultin tutkimaan tapausta. Keväällä tehdyissä tutkimuksissa ei löytynyt merkkejä siitä, että tietokannoista olisi varastettu tietoja, mutta varkauden mahdollisuutta ei voida myöskään sulkea pois.

– Tutkijoiden mukaan ei voida todentaa, että varkautta ei olisi tapahtunut. Toisaalta ei ole tullut merkkejä siitä että tietoja olisi varastettu tai niitä olisi käytetty muussa tarkoituksessa, sanoo Kimmo Koivu.

Koivun mukaan hyökkäyksen mahdollisesti vanhentunut komponentti, jonka toimittaneen yrityksen kanssa Arc Technology käy keskustelua.

– Me olemme toki vastuussa siitä, että kaikki palvelumme osapuolet täyttävät tietoturva vaatimukset, hän sanoo.

Koivu korostaa, että Arc Technology on parantanut murren jälkeen järjestelmiensä tietoturvaa ja ulkopuolinen asiantuntija tarkastaa järjestelmät ennen niiden käyttöönottoa.

Verohallinnon tietohallintojohtaja Markku Heikura kertoo A-Studiolle, että se pitää Arc Technologyn toimintaa ja tiedotusta murren jälkeen asianmukaisena ja että Verohallinto jatkaa yrityksen asiakkaana. Sen sijaan VR on katkaissut yhteistyönsä Arc Technologyn kanssa murto tapauksen vuoksi.

– Meidän on pystyttävä luottamaan siihen, että tietojamme käsittelevät yritykset toimivat vastuullisesti niiden kanssa ja nyt näin ei ole käynyt. Kyllä tämä tarkoittaa sitä, että tietoturvaan liittyvät asiat katsotaan meillä jatkossa entistä tarkemmin, Jukka-Pekka Suonikko sanoo.

Suonikko korostaa, että hyökkäys kohdistui henkilöstötietojärjestelmän kirjautumispalvelimeen, josta ei ollut yhteyttä esimerkiksi asiakasrekistereihin, lipunmyyntiin tai junien turvallisuuteen liittyviin järjestelmiin.



Tuomas Kerkkänen
Yle Uutiset