Kyberhyökkäykset: uhka kansalliselle turvallisuudelle?

Artikkeli - **Turvallisuus ja puolustus** − 03-11-2010 - 15:08

©BELGA_imagebroker_Simon Belcher

Muistatko vielä hyökkäykset virolaisten tiedotusvälineiden ja julkisten yhteisöjen verkkosivuille vuonna 2007? Erilaiset tietojärjestelmiin tehdyt murrot ovat viime vuosina muuttuneet yksittäisistä hyökkäyksistä järjestelmällisiksi iskuiksi, jotka voivat halvaannuttaa kokonaisen valtion toiminnan. Euroopan komissio esitti ehdotuksensa kyberhyökkäysten torjumiseksi kuulemistilaisuudessa 25. lokakuuta.

Nettirikollisuus ei enää rajoitu pelkästään salasanojen ja pankkitunnusten kalasteluun verkosta. Nykyään verkkohyökkäykset voivat olla sodankäyntiä, joilla tähdätään esimerkiksi poliittisten päämäärien saavuttamiseen. Viime vuosina on saatu jo useita esimerkkejä siitä, mitä järjestelmällisten tietoverkkohyökkäysten avulla voidaan saada aikaan.

Verkkosodasta kokemuksia ympäri maailmaa

"Me tiedämme, mitä tapahtui Virossa ja Georgiassa. Tiedämme, kuinka tärkeästä aiheesta on kyse", totesi turvallisuus- ja puolustuspolitiikan valiokunnan varapuhemies **Krzysztof Lisek** (PL, EPP).

Viro joutui verkkosodan kohteeksi keväällä 2007, kun pronssisoturipatsaan siirrosta syntyi kiista. Kyberhyökkäykset lamaannuttivat muun muassa valtion virastojen, tiedotusvälineiden ja pankkien tietojärjestelmiä. Monta päivää jatkuneiden hyökkäysten jäljet johtivat Venäjälle. Tapahtumista käytetään nimitystä Web War One, ensimmäinen nettisota.

Georgian sodan yhteydessä vuonna 2008 ainakin Georgian presidentin, Georgian keskuspankin ja puolustusministeriön sivuille murtauduttiin. Vastaavasti Georgia esti venäläisten tv-kanavien lähetykset maassa. Lisäksi venäläisen uutistoimiston Ria Novostin sivut kaadettiin.

Viime vuoden maaliskuussa tutkijat löysivät 103 maahan levittäytyneen vakoiluverkon, joka oli varastanut satoja

asiakirjoja hallitusten ja yritysten toimistoista. Vakoiluverkko ulottui myös joidenkin suomalaisten toimistojen tietokoneisiin. Vakoilua hallinnoitiin Kiinasta.

Yli 250 miljardin uhka

Vakavimmissa hyökkäyksissä kaapataan suuri määrä tietokoneita ja käytetään niitä robottiarmeijan tavoin ilman, että oikeat käyttäjät pystyvät vaikuttamaan tapahtumiin. Tällaisilla hyökkäyksillä on myös huomattavat taloudelliset vaikutukset. Pahimmassa skenaariossa koko tietoverkkorakenne, mukaan lukien puhelinlinjat, kuituoptiikka ja tietokone verkot, voidaan halvaannuttaa. Maailman talousfoorumin arvion mukaan hävityksen kustannukset nousisivat yli 250 miljardiin dollariin.

Onneksi kaikki verkkohyökkäykset eivät ole näin tuhoisia. "Eräs hakkeri pääsi kerran Puolan presidentin sivuille ja muutti niiden sisällön aikuisviihteeksi. Jälkeenpäin jotkut toimittajat sanoivat, että nämä sivut olivat kiinnostavammat kuin alkuperäiset", Krzysztof Lisek vitsaili kuulemistilaisuudessa.

Komission ehdotukset tietoturvatyön parantamiseksi

Euroopan unioni perusti kyberhaasteen kanssa kamppailevan Euroopan verkko- ja tietoturvaviraston ENISAn vuonna 20004. Tämä asiantuntijaelin tarjoaa tieteellistä ja teknistä apua kyberhyökkäysten estämiseen sekä osallistuu alaan liittyvän EU-lainsäädännön valmisteluun.

Komissio on tänä syksynä tehnyt uusia ehdotuksia kyberuhan torjumiseksi. Parlamentti tutustui ehdotuksiin kuulemistilaisuudessa 25. lokakuuta.

Komissio ehdottaa

1. Rangaistusten tiukentamista. "Raskauttaviksi asianhaaroiksi luettaisiin esimerkiksi suuren tietokonemäärän kaappaaminen ja sen käyttäminen", sanoi **Radomír Jánský** Euroopan komission sisäasioiden pääosastolta.

2. Jäsenvaltioiden välisen yhteistyön lisäämistä. Vuodesta 2008 EU:n jäsenmailla on ollut 24/7 toimiva verkosto. jonka avulla on tarkoitus vaihtaa ratkaisuehdotuksia yksittäisiin kyberhyökkäyksiin. Komission mukaan verkoston tulisi kuitenkin reagoida hyökkäyksiin nykyistä nopeammin (8 tunnin kuluessa).

3. Järjestelmällisen tiedonkeruun parantamista.

4. ENISAn roolin vahvistamista, jotta jäsenvaltiot ja yksityinen sektori voisivat yhdistää voimansa nykyistä paremmin.

Oikeus- ja sisäasioiden valiokunta aloittaa joulukuussa keskustelun komission tekemistä ehdotuksista. Varsinaisen lainsäädäntöprosessin uskotaan pääsevän käyntiin vuoden 2011 alussa.

Viite : 20101025STO89965
Päivitetty: 14-03-2011 - 20:20

Lisätietoa

Komission päivitetty ehdotus tietojärjestelmähyökkäyksiin liittyvästä lainsäädännöstä
Komission lehdistötiedote (30/09/2010)
ENISA (englanniksi)