26.06.2014 Dnro 8/41/14

Oikeusministeriö
Lainvalmisteluosasto
PL 25
00023 VALTIONEUVOSTO

Lausunto tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin (2013/40/EU) kansallisista täytäntöönpanotoimista (ns. tietoverkkorikosdirektiivi)

Oikeusministeriö on 7.5.2014 (OM 15/41/2013) pyytänyt Helsingin syyttäjänvirastolta lausuntoa otsikon aiheesta. Pyydettynä lausuntona Helsingin syyttäjänvirasto haluaa kiinnittää huomiota muun muassa seuraaviin syyttäjän työn kannalta merkityksellisiin muutosehdotuksiin:

Rikoslaki 38 luku 8 §; tietomurto sekä rikoslaki 38 luku 3 §; viestintäsalaisuuden loukkaus

Rikoslain 38 luvun 8 §:n 2 momentin 2) -kohdassa ehdotetaan lavennettavaksi "murtautumisen" määritelmää tietomurron tunnusmerkistöihin, mikä on erittäin kannatettavaa. Ehdotuksessa olevan lisäyksen mukaan "tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmästä olevasta tiedosta tai datasta". Kyseessä on usein juuri tietojärjestelmän haavoittuvuuden hyväksi käyttäminen eikä suora murtautuminen tietojärjestelmään, esimerkkinä esityksessäkin mainittu SQL-injektiotekniikka.

Viestintäsalaisuuden loukkaamisen tunnusmerkistössä ei kuitenkaan ole samanlaista haavoittuvuuden hyväksi käyttämistä, vaan pykälän 1) -kohdan mukaan teko edellyttää suojauksen murtamista. Harkittavaksi voisi kuitenkin tulla, pitäisikö tietomurtoa vastaava lavennus, joka on kirjattu RL 38 luvun 2 momenttiin, lisätä myös viestintäsalaisuuden loukkaamisen tunnusmerkistöön. Esimerkiksi tietojärjestelmän haavoittuvuutta hyväksi käyttäen saatu tieto sähköisesti tallennetusta viestistä täyttäisi todennäköisesti vain tietomurron tunnusmerkistön, mikä on syytä pitää mielessä, mikäli lainsäätäjä haluaa varmistaa ni-

Postiosoite	Käyntiosoite	Puhelin	Telefax	Sähköposti
PL 318	Porkkalankatu 13, 6. krs	029 56 22100	029 56 22203	helsinki.sy@oikeus.fi
00181 Helsinki	00180 Helsinki			

menomaan viestintäsalaisuutta koskevan oikeushyvän suojaamisen. Kun viestintäsalaisuuden loukkauksen rangaistavuuden edellytyksenä on, että viesti on sähköisesti tai muulla vastaavalla teknisellä keinolla suojattu ulkopuolisilta, olisi loogista, että ei oltaisi rajattu pelkästään suojauksen murtamisen kriteeriin.

Rikoslaki 38 luku 9 b §; identiteettivarkaus

Pykälässä ehdotetaan uutta kriminalisointia koskien identiteettivarkautta, joka olisi sakolla rangaistavaa.

Ongelmalliseksi kuitenkin käytännössä muodostunee se, että jutun tutkinta nykyisillä pakkokeinosäännöksillä ei olisi riittävää. Todennäköisesti tyypillisin identiteettivarkaus tällä hetkellä on valeprofiili sosiaalisessa mediassa ja oletettavaa on, että juttujen tutkiminen vaati usein aikaa vieviä ja niiden vakavuuteen nähden raskaita tutkintakeinoja. Mikäli tutkinnassa voitaisiin edetä riittävän tehokkaasti, tulisi pakkokeinolaissa mahdollistaa televalvonnan käyttö myös identiteettivarkauksissa.

Mikäli kyse on pelkästään identiteettivarkaudesta, eikä esimerkiksi myös samalla teolla täytetystä petoksesta, kansalaisen näkökulmasta voi olla liian paljon odotuksia siitä, että viranomaiset alkaisivat tutkia juttuja herkästi. Tämä saattaa myös olla hieman ristiriidassa siihen nähden, että lakiehdotuksen kanssa samaan aikaan esimerkiksi kunnianloukkauksen ja yksityiselämää koskevan tiedon levittämisen rangaistusasteikkoja on lievennetty. Yleisestävyyden kannalta olisikin välttämätöntä antaa mahdollisille tekijöille viesti siitä, että kiinnijäämisriski on todellinen ja että käytettävissä olevat tutkintakeinot ovat riittävän tehokkaat.

Mikäli identiteettivarkauden tutkintaa ei tosiasiassa pystytä hoitamaan menestyksekkäästi, vaarana on, että kynnys lopettaa juttujen tutkinta jo esitutkinnan aikana saattaa muodostua matalaksi.

Järjestäytyneen rikollisryhmän määritelmästä tietoverkkorikoksissa

Ehdotuksessa esitetään lisättäväksi rikoslain 35 luvun 3 b § (törkeä datavahingonteko), rikoslain 38 luvun 6 § (törkeä tietoliikenteen häirintä) ja rikoslain 38 luvun 7 b § (törkeä tietojärjestelmän häirintä), joissa yhtenä kvalifiointiperusteena olisi se, että rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa. Voimassa olevaan törkeään vahingontekoon ja törkeään tietomurtoon vastaava kvalifiointiperuste on jo lisätty.

Helsingin syyttäjänviraston puolesta halutaan tuoda esille, että rikollisryhmät tietoverkossa ovat varsin usein löyhiä yhteenliittymiä, joissa

järjestäytyminen on varsin erilaista verrattuna ns. perinteiseen rikollisuuteen. Jo nyt on oikeuskäytännössä käynyt selväksi, että kynnys tuomita henkilöitä järjestäytyneen rikollisryhmän osana on varsin korkea tavanomaisissakin rikoksissa, joten odotettavissa on, että etenkin tietoverkkorikoksissa näyttötaakka voi osoittautua erittäin vaikeaksi täyttää.

Tietoverkkorikokseen epäillyt henkilöt ovat toki usein verkostoituneita, mutta myös jälkien ja sitä myötä näytön peittäminen on rikostyypeille ominaista. Tällä on suora vaikutus siihen, kuinka hyvin kvalifiointiperuste menestyy tuomioistuimessa. Lisäksi esimerkiksi haittaohjelmarikoksissa tekijät toimivat usein alihankinta- ja värväysperusteella. Prosessin eri vaiheissa toimivat eri henkilöt omissa rooleissaan (koodaaja, injektoija, komentopalvelimen hallitsija, rahamuulien rekrytoija, itse rahamuuli jne.) eivätkä välttämättä tiedä, kuinka suuresta "organisaatiosta" on kyse ja sen vuoksi perinteiset rikollisryhmän määritelmät eivät toimi oikein hyvin. Helsingin syyttäjänvirasto ei varsinaisesti esitä suoranaisia ratkaisuehdotuksia, mutta pitää soveltamisongelmaa potentiaalisena, joka olisi syytä huomioida jatkossa.

Elintärkeästä infrastruktuurista kvalifiointiperusteena

Ehdotuksen mukaan törkeän datavahingonteon, törkeän tietoliikenteen häirinnän ja törkeän tietojärjestelmän häirinnän yhtenä kvalifiointiperusteena on se, että teko kohdistuu laitteeseen /tietojärjestelmään/ viestintään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon.

Vaikka muu "näihin rinnastettava yhteiskunnan tärkeä toiminto" voinee tulkita laajasti, harkittavaksi voisi kuitenkin tulla, tulisiko listauksessa erikseen vielä mainita esimerkiksi elintarvikehuolto ja finanssipalvelut. Viimeksi mainitulla tarkoitamme erityisesti pankkipalveluja verkossa, joihin kohdistuneet teot voivat vakavasti vaarantaa järjestelmää ilman, että sille olisi jo aiheutunut erityisen tuntuvaa haittaa tai taloudellista vahinkoa.

Johtavan kihlakunnansyyttäjän sijainen — Eija Velitski

Kihlakunnansyyttäjä — Tuomas Soosalu