Teknologia teollisuus

LAUSUNTO

13.5.2014

Teknologiateollisuus ry ja FISC ry – Lausunto 13.5.2014

Lainsäädäntöhanke:

Kansallisen lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kyberympäristön uhkista.

HARE PLM004:00/2013 FI.PLM.2013-5807 /909/40.02.00/2013

Suomen tietoturvaklusteri, Finnish Information Security Cluster, FISC ry ja Teknologiateollisuus ry kiittävät lausuntopyynnöstä. Suomen tietoturvaklusteriin kuuluu merkittävä osa suomalaisista tietoturvatuotteita ja -palveluita tarjoavista yrityksistä. Suurin osa yrityksistä on myös Teknologiateollisuus ry:n jäsenyrityksiä. Tässä dokumentissa esitetään Suomen Tietoturvaklusterin ja Teknologiateollisuuden yhteinen lausunto kansallisen turvaviranomaisten tiedonhankintakyvyn parantamislainsäädäntöön.

Näkemyksemme mukaan Suomen kansallisen kyberturvallisuuden kehittäminen on erittäin tärkeää, ja yhtenä tukipilarina tälle on sovelias lainsäädäntö.

Kansainvälisesti Suomi tunnetaan puolueettomana, turvallisena sekä luotettavana maana. Suomessa on erittäin vahvaa osaamista kyberturvateollisuuden eri osa-alueilta. Vuoden 2013 aikana lukuisten tiedonurkintapaljastusten luoma epävarmuus on jo muuttanut koko maailman suhtautumista varautuneemmaksi digitalisoitumiseen ja kansainväliseen yhteistyöhön. Epäluulo kohdistuu pääosin amerikkalaisiin tai niitä lähellä oleviin yrityksiin ja niiden tarjoamiin palveluihin, jotka ovat olleet todistetusti tai epäillysti osana laajassa tiedonhankinnassa NSA:lle. Yhdysvalloissa paljastuneiden vakoiluskandaalien on arvioitu aiheuttaneen jo tähän mennessä noin 40 miljardin dollarin välittömät menetykset maan ICT-teollisuudelle.

Suomi on aiemmin toiminut rauhanturvaamisen suurvaltana. Digitaalisessa maailmassa maamme voi toimia kyberturvallisuuden luottamuksen takaajana. Tärkeä kansallinen visio on erottautua tulevaisuuden dataliikenteen solmukohtana, jossa kansainvälistä tietoliikennettä käsitellään suurella luottamuksella ja jonne voidaan turvallisesti taltioida tietoa. Suomessa on paljon teknologiaa, jonka hyödyntäminen tämän päivän vision toteuttaminen on mahdollista. maailman luottamispula nykyisiin toimijoihin on avannut markkinatyhjiön, jossa Suomella on rajattomasti kasvumahdollisuuksia. Tätä tukevat myös suunnitellut merikaapelihankkeet, joiden keskeinen tarkoitus on mahdollistaa tietointensiivisen teollisuuden sijoittuminen Suomeen.

Talous- ja turvallisuusvaikutukset arvioitava etukäteen huolellisesti

Maailman viimeaikojen tapahtumat ovat käynnistäneet laajoja kyberkeskushankkeita eri maissa kuten Intiassa, Isossa-Britanniassa, Ranskassa ja Saksassa. Tiedustelu sekä tiedon kerääminen kansallisen turvallisuuden takaamiseksi on mielletty hyvin eri tavoin maailmalla. Tiedon kerääminen

ja hyödyntäminen vaativat huomattavia investointeja. esimerkiksi NSA:n toiminta vaatii vuosittain yli 10 miljardin dollarin toimintabudjetin.

Jos Suomessa halutaan kehittää toimintakykyä viranomaistoimilla, se vaatii kansallisesti yli 100 miljoonan euron vuosibudjetin, jotta tiedustelu olisi edes kohtuullisella tasolla. Kun uutta lainsäädäntöä valmistellaan, se vaatii rinnalleen arvion kokonaisvaltaisesta taloudellisesta panostuksesta sekä arvion suorista ja välillisistä vaikutuksista, muutoin lakimuutokset saavat kansantalouden tasolla aikaan enemmän vahinkoa kuin hyötyä.

Ennen kuin lainsäädäntötyössä voidaan edetä, tulisi kaikki vaikutukset arvioida niin kansallisen turvallisuuden, vaadittavien investointien kuin mahdollisten taloudellisten hyötyjen ja menetysten osalta. Jos lain valmistelu tapahtuu hätäisesti ja ristiriitaisessa ilmapiirissä, sillä vahingoitetaan eri toimijoiden taloudellisia ponnistuksia ja pahimmillaan koko luottamukseen perustuvan Suomen maabrändiä.

Suomi on perustanut kyberturvakeskuksen, joka on kevyt mikroluokan toteutus siitä, mitä se voisi todellisuudessa olla. Kyberkeskuksen resursseja ja toiminta-aluetta voisi laajentaa aktiivisen suojauksen ja laajemman havainnoinnin suuntaan. Keskuksen tulisi tehdä voimallisempaa yhteistyötä alan teollisuuden kanssa, jotta saamme aikaan uusia innovaatioita ja keinoja haitallisten toimijoiden toiminnan estämiseksi. Erityisesti maassamme tulisi kehittää eteenpäin Havaro-järjestelmän kaltaisia, jo tehtyjä investointeja siten, että investoinnit kattavat Suomessa toimivat yksityiset yritykset ja julkisen sektorin paremmin. Lisäksi havainnointi tulisi ulottaa Suomen rajojen ulkopuolelle, sillä digitaalisessa maailmassa ei ole maarajoja.

Internet, kyberrikollisuus ja tiedustelu muuttuvat nopeasti. Tämän vuoksi akateemisen maailman ja teollisuuden tulee yhdessä etsiä keinoja, joilla pysymme mukana kehityksessä. Tässä työssä tulisi keskittyä siihen, kuinka internetin hallintoon mahdollisesti liittyvät muutokset tai kerrostuminen ja ns. Deep Webin - tyyppiset järjestäytyneen rikollisuuden käyttämät mallit vaikuttavat maamme kokonaisturvallisuuteen. On todennäköistä, että massatiedonkeruumenetelmien kehittäminen ei paranna kokonaisturvallisuutta, koska uhkakuvat muuttuvat dynaamisesti.

Nykylainsäädännössä kyseessä olevan liikenteen haravointi ei ole mahdollista, vaan kaikkia tapauksia käsitellään yksittäisinä. Esimerkiksi verkkorikollisten ja valtiollisten toimijoiden käyttämien haittaohjelmien ja muiden tekniikoiden käyttäytyminen perustuu usein aktiivisiin tietoliikenneyhteyksiin maan rajojen ulkopuolelle. Kyseiseen toimintaan liittyvä verkkoliikenne olisi teknisesti mahdollista havaita ja kohdentaa ilman, että itse liikenteen sisältöä tai koko Suomen sisäistä verkkoliikennettä on tarvetta seurata.

Tarvetta olisi myös parantaa viranomaisten välillä tapahtuvaa tietoturvaloukkauksiin liittyvää tiedonvaihtoa. Lisäksi viranomaisten tulisi pystyä kertomaan yrityksille ja yksityishenkilöille, millaisia hyökkäyksiä on käynnissä, jotta niiltä voidaan suojautua. Samalla pitäisi tapausten vakavuuden mukaan velvoittaa hyökkäysten uhreja raportoimaan heihin kohdistuneista hyökkäyksistä ja niiden tekniikoista, jotta muut voivat niiltä suojautua.

Lisäksi tulisi harkita tunnistettujen bottiverkkojen komentoliikenteen blokkaamisen sallimista operaattoritasolla sekä kyseisen liikenteen lähettäjien ip-osoitteiden selvittämistä, jotta bottiverkkoon liitettyjen päätelaitteiden omistajia voitaisiin operaattorin toimesta varoittaa. Lisäksi verkkoliikenteen seuraamista tarvitaan teknisistä syistä, mikä on sallittava myös jatkossa.

EU-tuomioistuimen päätökset huomioitava lainsäädäntöhankkeessa

EU-tuomioistuin korosti vahvasti tietosuojan asemaa kaikkia jäsenvaltioita sitovana kansalaisten perusoikeutena 8.4.2014 Digital Rights Ireland -tapaukseen antamassaan tuomiossa, jossa se julisti EU:n teletunnistetietojen säilyttämistä koskevan direktiivin (2006/24/EY) pätemättömäksi ja linjasi samalla, ettei kaikkia ihmisiä koskevaa tiedonkeruuta tule EU:n alueella harjoittaa ilman selkeää epäilyä rikollisuudesta.

Kaikki ihmisiä koskeva tiedonkeruu rikkoo EU:n kansalaisten perusoikeuksia. EU-tuomioistuimen tekemä päätös 2006/24/EY vahvistaa jo aiemmin Teknologiateollisuus ry:n ja FISC ry:n 5.2.2014 lausunnossaan tekemiä linjauksia.

Juha Remes
FISC Finnish Information Security Cluster ry
hallitus
juha.remes@cyberlab.fi

Jukka Viitasaari
johtaja
Teknologiateollisuus ry
jukka.viitasaari@teknologiateollisuus.fi