FISC ry

Lausunto

20.06.2017

Asia: 801/40.02.00/2015

Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi (työryhmän mietintö)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Tietoturvaklusteri FISC ry

Juha Remes

Lausunto

Puolustusministeriö
20.06.2017

www.lausuntopalvelu.fi

Viite: 801/40.02.00/2015

Lausunto: Lausunto sotilastiedustelulainsäädännöstä (työryhmän mietintö)

Yleistä

FISC ry kiittää mahdollisuudesta antaa näkemyksiä ja tulla kuulluksi sotilastiedustelulainsäädäntötyöryhmän mietinnöstä. Haluamme korostaa lain tarpeellisuutta ja kiireellisyyttä. Olemme myös tyytyväisiä lainvalmisteluun liittyvästä yhteistyöstä, jota viranomaiset ovat tehneet kyberturva-alan yritysten sekä koko elinkeinoelämän kanssa tätä lakikokonaisuutta laadittaessa. Suomi on yksi Euroopan merkittävimmistä kyberturvateollisuuden maista ja alan teollisuus kasvaa nopeasti. Suomessa toimii yksi Euroopan suurimmista tietoturvayhtiöistä F-Secure sekä lukuisia muita kilpailukykyisiä alan tuote- ja palveluyrityksiä.

Jatkuvat muutokset maailmalla ovat vaikuttaneet myös merkittävästi Suomen kansallisen kyberturvallisuuden kehittämiseen ja kansainvälisesti luottamuksesta on tullut pääomaa. Luottamus on yksi Suomen tulevaisuuden vientituotteita. Tämä koskee erityisesti kyberturvallisuutta, jossa Suomen on oltava tulevaisuudessa yhä omavaraisempi maa kuin tänä päivänä.

Kyberturvallisuus on edellytys menestyksekkäälle digitalisaation hyödyntämiselle ja sellaisena keskeinen Suomen tulevaisuuden kannalta. Kansallisesti toteutettavissa digiratkaisuissa on kehityttävä hyödyntäen kansallisia kyvykkyyksiä ja innovaatioita. On myös suosittava kansallisesti toteutettuja teknologioita, jotta yritykset saavat niistä arvokkaita referenssejä kansainvälistymiselle. Elinvoimainen, kansainvälisesti kilpailukykyinen ja itsenäinen kyberturvateollisuus vahvistaa kansallista turvallisuutta sekä luo pohjan Public-Private-yhteistyölle sekä perustan tulevaisuuden hyvinvoinnille.

Euroopan Unionin käynnissä olevat huomattavat rakennemuutokset sekä muuttunut poliittinen tilanne Yhdysvalloissa vaikuttavat merkittävästi myös Euroopan sisäiseen turvallisuuteen. EU:n on jatkossa panostettava turvallisuudessa suurempaan omavaraisuuteen sekä vahvistettava kyberturva-alan teollisuuden kasvuedellytyksiä. European Cyber Security Organization (ECSO) on linjannut EU:n investointitarpeeksi kyberturvateollisuuden kehittämiseksi 38 miljardia euroa seitsemän vuoden ajanjaksolle. Tämän lisäksi EU:n puolustusyhteistyön pääpainopiste tullaan suuntaamaan kyberturvallisuuden kehittämiseen ja siihen tullaan investoimaan useita miljardeja euroja vuodessa.

Suomen on oltava mukana tässä kehityksessä ja kyettävä vahvistamaan oman kyberturva-teollisuuden kilpailukykyä sekä toimittava esimerkillisesti jatkuvasti uusia kyberturvainnovaatioita. Tämä vahvistaa Suomen mahdollisuuksia myös toimia yhtenä EU:n kyberturvallisuuden tukipilarina tulevien EU kehityshankkeiden taustalla.

Osana toimivaa kansallista kyberturvallisuutta tarvitaan toimintakykyinen sotilas- ja siviilitiedustelu sekä verkkoliikenneseuranta. Nämä edistävät Suomen turvallisuuspoliittisten intressien toteutumista nopeasti muuttuvassa toimintaympäristössä. FISC ry pitää tärkeänä, että tiedustelua koskeva lainsäädäntö on kokonaisuus, jossa viranomaisten toimivaltuudet, niiden käytön valvonta, yksilöiden perusoikeudet ja elinkeinopoliittiset kysymykset ovat tasapainossa.

FISC ry on korostanut valmistelutyössä hyvää yrityssalaisuuden suojaa, viranomaisten ja elinkeinoelämän yhteistyötä turvallisuusuhkien torjunnassa sekä nopeasti kehittyvän teknologian roolia. Meidän on kiinnitettävä erityisesti huomiota kansallisten kyvykkyyksien kehittämisessä hankkimalla kansallisen kyberturvateollisuuden tarjoamia tuotteita ja palveluita.

Suomalaisilla viranomaisilla tulee olla selkeä valtuutus käyttää tarpeellisia ja oikeasuhtaisia keinoja digitaalisessa ympäristössä. On myös tärkeää varmistaa, etteivät uudistuvat toimivaltuudet aiheuta elinkeinoelämälle kustannuksia tai heikennä yritysten kilpailukykyä ja toimintamahdollisuuksia tai rajoita yritysten kansainvälistymismahdollisuuksia.

Elinkeinoelämän toimintaedellytyksiä koskevia kysymyksiä on käsitelty runsaasti lainsäädännön valmistelun aikana. Turvallisuusuhkien tunnistamisessa ja torjunnassa yhteistyö julkisen ja yksityisen sektorin välillä on yhä merkittävämmässä roolissa. Erityisesti digitaalisia tuotteita ja palveluita tuottavien tai niitä hyödyntävien yritysten kannalta on tärkeää, että niiden toimintaa koskeva lainsäädäntö on selkeää, tarkkarajaista ja ennustettavaa, eikä horjuta kansalaisten tai yritysten luottamusta digitaaliseen ympäristöön.

Huomioitavaa lain lopullisessa sisällössä ja soveltamisessa

Olemme lainsäädäntötyön valmistelussa painottaneet kyberteollisuuden, FISC ry:n perusarvoja kansallisen kyberturvallisuuden toteuttamissa sekä kehittämisessä. Valmistelutyössä asioiden osalta ei ole ilmennyt erimielisyyksiä, ja valmistelutyö on toteutunut erittäin hyvin yhteistyössä koko elinkeinoelämän kanssa. Huolenamme on kuitenkin lakiaineiston laajuus ja se, että useat keskeisen kohdat on esitetty kattavista perusteluissa mutta varsin niukasti itse lakitekstissä. Näkemyksemme mukaan nyt esitetyssä mietinnössä on lukuisia osa-alueita, joissa tulisi tehdä tarkennuksia siirtämällä kuvauksia ja tarkennuksia perusteluista varsinaiseen lakitekstiin. Lisäksi koemme huolta tuomioistuimien kyvykkyyksistä arvioida tiedusteluviranomaisen pyyntöjä. Päätöksenteko näyttäisi edellyttävän poikkeuksellisen laajaa kokonaisvaltaista ymmärrystä myös teknologiasta. Tuomioistuimille olisi tässä yhteydessä varattava laajemmat valtuudet ja mahdollisuudet hyödyntää ja kuulla eri asiantuntijoita päätöksien tekemisen tueksi.

Korostamme seuraavia periaatteita, jotka ovat huomioitava kaikissa lain tulkinnoissa sekä myös mahdollisissa lakimuutoksissa, joita toteutetaan nyt esitettyjen lausuntojen perusteella.

i. Lainsäädännön toteuttamiseen on varattava riittävästi resursseja. Kyberturvallisuuden uhkakuvat muuttuvat jatkuvasti. Resursoinnissa on varauduttava aiemmin tehtyjä investointeja mitätöivään teknologiseen kehitykseen ja mitoitettava tiedustelun kyvykkyys kulloistakin uhkaa vastaan. Liian pienillä panostuksilla ainoastaan saavutetaan näennäinen turvallisuuden tunne.

ii. Kansallisissa kyberpuolustuksen toteutuksissa on pyrittävä hyödyntämään Suomessa tuotettuja tuotteita ja palveluita. Tämä mahdollistaa pitkäjänteisen kansallisen kyberosaamisen kehittymisen ja tukee kansallista itsenäisyyttä ja riippumattomuutta. Vahva kyberturvateollisuus, joka kykenee kilpailemaan kansainvälisesti ja toimittamaan sekä Eurooppaan että Euroopan ulkopuolisilla markkinoille tuotteita ja palveluita, takaa Suomelle kokonaisvaltaisen kyberturvallisuuden vahvistumisen, osaamisen kehittymisen sekä parantaa samalla kansallista taloudellista hyvinvointia.

iii. Kansallinen kyberturvallisuus ei poista yritysten ja muiden organisaatioiden tarpeita organisaatiokohtaista kyberturvallisuuden huolehtimista. Jokainen organisaatio joutuu itse huolehtimaan oman organisaation kyberturvallisuuden kehittämisestä. Kansallisesti kyberturvallisuutta on kehitettävä niin valtiollisella kuin organisaatiotasolla huolehtien samalla näiden tahojen toimien keskinäisestä koordinoinnista. Näitä toimia on tuettava vahvoilla tutkimus- ja koulutuspanostuksilla.

iv. Tietoturvaa ei saa heikentää millään tavoin. Lainsäädäntöön ei saa sisältyä tietoturvaa heikentävistä tai velvoittavia toimenpiteitä. Tietoturvaa heikentävät ratkaisut eivät tuota toivottua tulosta, mutta altistavat kansalaiset uusille uhille. Jos tuotteisiin ja palveluihin rakennetaan ennakoivasti tietoturva-aukkoja tai haavoittuvuuksia, niiden hyödyntäjiksi päätyvät aina myös ne tahot, jotka toimivat rikollisin tai vihamielisin periaattein.

Vastaavalla tavalla myös eräiden tiedustelunmenetelmien (laitteet, ohjelmat) kohdistaminen viestintäverkkoon (muutoin kuin erikseen valikoituihin tietoliikenneoperaattorin osittamiin rajanylityskytkentäpisteisiin) tai Internet-palveluihin tai näiden tuotantotiloihin heikentäisi tietoturvaa merkittävästi.

Emme alan teollisuutena voi hyväksy takaporttien vaatimista Suomessa tuotettuihin tuotteisiin tai ratkaisuihin, emmekä voi hyväksya salausyleisavaimien tai salausalgoritmien luovuttamisvaatimuksia.

v. Yrityksille ei saa aiheutua suoria eikä välillisiä kustannuksia. Kyberturvallisuus on hyvin dynaaminen kokonaisuus. Tiedustelun ja verkkoliikenneseurannan toteuttamisessa voivat yhteistyömuodot julkisen sektori ja yksityisen sektorin osalta vaihdella. Yhteistyö ei saa aiheuttaa yrityksille ylimääräisiä kustannuksia ja mikäli kustannuksia syntyy, on ne korvattava kustannukset kärsineelle osapuolelle kokonaisuudessaan.

vi. Lakimuutokset sekä niiden toimeenpano ei saa asettaa ristiriitaisia velvollisuuksia yrityksille. Yrityksille ei saa aiheutua eturistiriitaa yrityksen oman liiketoiminnan ja viranomaisille tuotettavien palveluiden välillä.

Korostamme, ettei viranomaisten tule turvautua esimerkiksi reserviläisten laajamuotoiseen hyödyntämiseen pikaratkaisuina vaan viranomaisten tulee panostaa pitkäaikaiseen public-private-yhteistyöhön, yritysten kanssa.

Suomessa on kyberturva-alan yrityksiä, joilla on paljon tarjottavaa viranomaisille ja niiden palveluita tulee viranomaisten hyödyntää. Näitä yrityksiä on merkittävästi FISC ry:n jäsenkunnassa. Tässä on kuitenkin oltava kyse kaupallisesta liiketoiminnasta, ei velvoittavasta viranomaisen avustamisvelvollisuudesta.

vii. Viranomaistiedonvaihto on suuri kansanvälinen haaste, johon on suhtauduttava erityisellä huolella. Kansainvälinen viranomaisyhteistyö on laajaa. Usein kansainvälinen rikollistorjunta edellyttää tiedonvaihtoa. Tiedosta on muodostunut tiedusteluviranomaisille, sekä poliisille globaalisti jopa kauppatavaraa, jossa pätee vaihdannan lait. Tiedonvaihto voi olla välttämätöntä.

Tähän liittyy kuitenkin huomattava riski. Useat valtiot toimivat tiedustelussa laajemmin tarkoitusperin kuin Suomi. Näissä valtioissa kyberturvallisuuteen liittyy tiiviisti myös kansallisen hyvinvoinnin kehittäminen. Tiedonvaihdolla nämä maat voivat haalia merkittäviä yrityssalaisuuksia haltuunsa. Suomalaiset viranomaiset ja heidän tarkoitusperät ovat tässä asiassa selkeät, mutta tiedonvaihdossa tulee olemaan näitä uudenlaisia riskejä. Vaikka esitetyssä lainsäädännössä pyritään suojelemaan kansallisesti merkittäviä yrityksiä ja niiden yrityssalaisuuksia, on niiden tunnistaminen todellisuudessa yhä vaikeampaa.

Suomalainen keskimääräinen yrityskoko on vajonnut alle 20 työntekijään ja uudet innovaatiot syntyvät usein näissä pienissä ja keskisuurissa kasvuyrityksissä. PK-yrityksissä on tänä päivänä kansallisesti merkittäviä yrityssalaisuuksia ja niiden tunnistaminen voi olla viranomaisten toimesta vaikeaa jopa mahdotonta.

Suosittelemme viranomaisia käyttämään tässä riittävästi ulkopuolista asiantuntemusta sekä varamaan riittävästi resursseja näiden arkaluontoisten ja kauaskantoisten asioiden varmistamiseen.

Eritysesti, emme hyväksy ”raakadatan” eli tiedon, jonka sisältöä viranomainen ei tunne tai ei tunne riittävästi, luovutettavaksi muiden maiden tiedusteluvianomaisille.

Edellä kuvatun lisäksi sitoudumme Elinkeinoelän Keskusliiton (EK) antamiin yksityiskohtaisin lakimuutosehdotuksiin, joiden laatimisessa, FISC ry on ollut tiivisti osallisena.

_____

Juha Remes

Toiminnanjohtaja,

FISC Finnish Information Security Cluster ry

juha.remes@cyberlab.fi

Remes Juha
FISC ry