F-Secure Oyj

Lausunto

22.06.2017 LCM-2694

Asia: 801/40.02.00/2015

Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi (työryhmän mietintö)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

F-Secure Oyj kiittää mahdollisuudesta lausua sotilastiedustelua koskevasta lakiesityksestä.

F-Secure on seurannut tiedustelulakipaketin valmistelua tiiviisti ja osallistunut vuosina 2015-2017 Elinkeinoelämän keskusliiton johtaman seurantaryhmän toimintaan. Arvostamme mahdollisuutta pysyä informoituna ja tulla kuulluksi jo lakivalmistelun edetessä.

Lakien ja lainvalmistelun julkisuudesta

On tärkeää, että tiedustelusta säädetään julkisella lailla julkisen valmisteluprosessin tuloksena. On jopa niin, että lainvalmisteluprosessin julkisuus on sitä tärkeämpää, mitä salaisempien toimivaltuuksien käytöstä on kyse. Kansalaisten ja oikeushenkilöiden oikeusturvan kannalta on välttämätöntä että viranomaisen toimintaa ja toimivaltaa raamittavat lait ja niiden tulkinnat ovat julkisia. Demokratian kannalta on tärkeää, että päätöksiä tehdessään päättäjät ja heitä tehtäviinsä valitsevat äänestäjät ovat tosiasiallisesti informoituja siitä, miksi ehdotetut lait on kirjoitettu siten kuin ne ovat, miten niitä on tarkoitettu tulkittavaksi ja että lain tarkoitus ei käänny ennakoimattomalla tavalla päälaelleen tulkintatavan muutoksen seurauksena.

F-Secure toivottaa tervetulleeksi valmisteluprosessin aikana lisääntyneen avoimuuden. Erityisen hienoa tämä on jo pelkästään siksi, ettei nyt nähty avoimuus vaikuta pakonomaiselta reaktiolta suomalaisen sotilastiedustelun laimin- tai ylilyönteihin kuten esimerkiksi Yhdysvalloissa, Iso-Britanniassa tai Saksassa on käynyt, vaan terve reaktio demokraattisen prosessin synnyttämään julkisuuspaineeseen. Kannustamme viranomaisia ja päättäjiä vastaisuudessakin osallistumaan

yhteiskunnalliseen keskusteluun kansallisen turvallisuuden tavoitteista, turvallisuusviranomaisten tehtävistä sekä tiedustelun suhteesta kansalaisten perusoikeuksiin kuten yksityisyydensuojaan.

Yleistä F-Securen suhtautumisesta tiedustelulakiehdotuksiin

F-Secure käsittelee sotilas- ja siviilitiedustelua sekä tiedustelutoiminnan valvontaa koskevat lait kokonaisuutena. Ehdotetuilla toimivaltuuksilla on mahdollista murtaa perustuslain muutoin takaaman viestintäsalaisuuden suoja sekä suorittaa toimenpiteitä, jotka normaalisti täyttäisivät rikoslaissa tarkoitetun tietomurron ja luvattoman käytön sekä tietoliikenteen häirinnän tunnusmerkistöt. Käytännössä tiedustelutehtävän osana käytettäisiin teknistä tarkkailua, telepakkokeinoja ja tietoliikennetiedustelua ennalta määriteltyyn kohteeseen. Kansanomaisemmin ilmaistuna kyse olisi tietoturvaloukkauksista. Tämä on F-Securen kannalta merkityksellistä, koska yrityksemme erityisesti ja teollisuudenalamme yleisesti tuottaa ratkaisuja juuri tällaisilta uhilta suojautumiseen.

Tekniseltä tasolta tarkastellen tietoturvaloukkaus näyttää aina tietoturvaloukkaukselta ja viestintäsalaisuuden loukkaus viestintäsalaisuuden loukkaukselta riippumatta siitä, suorittaako toimenpiteen viranomainen vai rikollinen ja millä laillisella oikeutuksella viranomainen toimintaansa kulloinkin perustelee. Koska tekniseltä uhalta suojautumiseen tarkoitetun teknisen työkalun ei ole mahdollista tunnistaa tilannetta, jossa hyökkäykselliset toimenpiteet suorittaakin laillinen taho laillista kohdetta vastaan, jää ainoaksi vastuulliseksi vaihtoehdoksi tarjota suojaa kaikkia tieto- ja kyberturvallisuuden uhkia vastaan riippumatta siitä kuka tai mikä uhan kulloinkin aiheuttaa.

Olemme erityisen tyytyväisiä havaitessamme, että kykymme tuottaa tieto- ja kyberturvallisuuden palveluita ei vaarannu ehdotettujen lakien seurauksena. Erityisen tärkeää ohjelmistopohjaista kyberturvallisuutta tuottavalle ja globaalilla markkinalla toimivalle Suomeen sijoittuneelle yritykselle on, että lainsäädäntö ei jatkossakaan velvoita keinotekoisesti heikentämään ohjelmistojen turvallisuutta esimerkiksi takaporttien muodossa tai vaatimalla ummistamaan silmiä tietoturvaloukkauksilta. Tämä on ensiarvoisen tärkeää paitsi asiakkaille annettavan arvolupauksen uskottavuuden kannalta, myös laajemmin kaikkien suomalaisten tietoteknisten ja kyberturvallisuuden alan palvelujen ja tuotteiden uskottavuuden kannalta.

Yksityiskohtaisia huomioita

75 § Haitallista tietokoneohjelmaa koskevien tietojen luovuttaminen yrityksille ja yhteisöille

Lakiehdotuksen 75 § mahdollistaisi, että viranomainen luovuttaa tietoliikennetiedustelun keinoin toteutetun tiedustelutehtävän yhteydessä saamiaan tietoja haitallisista tietokoneohjelmista yrityksille ja yhteisöille. Haluamme korostaa, että lakiin kirjattu luovutusoikeus tulisi nähdä pelkkiä haittaohjelmia laajempana.

Suurin osa käytännön edistyneistä tietoturvaloukkauksista (nk. APT, englanniksi "Advanced Persistent Threat") toteutetaan kokonaan tai ainakin osittain ilman varsinaisia haittaohjelmia hyödyntäen muilla tavoin kohdejärjestelmän suojauksen puutteita ja toimimalla valtuutetun käyttäjän nimissä järjestelmän osana. Englanninkielinen ilmaisu "living off the land" - "maan antimista nauttien" - kuvaa toimintatapaa hyvin. Tällaisen toiminnan havaitsemiseksi on tärkeää, että kohteen suojaamiseksi käytettävälle teknologialle voidaan opettaa kaikki tietoturvaa loukkaavan toiminnan tunnistamiseksi tarpeelliset tiedot, myös sellaiset jotka eivät viittaa haitallisiin tietokoneohjelmiin tai niiden käyttöön. Tunnistamista edesauttavia tietoja ovat riittävällä varmuudella haitallista ja tietoturvaloukkaukseen liittyvää järjestelmän toimintaa yksilöivät tunnisteet, haitallisen toiminnan synnyttämää tietoliikennettä tai liikennevuota (suunnat, määrät, frekvenssit) kuvaavat tiedot, järjestelmien lokitiedoista ilmi käyvät poikkeavuudet, järjestelmiin ilmestyneet käyttäjätunnukset tai käyttövaltuuksien muutokset sekä muistivedoksesta, prosessilistauksesta tai järjestelmän määrittelytiedostosta löytyvät jäljet.

Yllä kuvattuja tunnistetietoja kutsutaan tietoturvaloukkausten käsittelyyn erikoistuneiden ammattilaisten keskuudessa englanninkielisellä nimellä Indicators of Compromise (IoC) ja kyseisenlaisten tunnisteiden vaihtamiseen on syntynyt teollisuuden ja viranomaisten piirissä jo vakiintuneet käytännöt. F-Securen mielestä on kannatettavaa, että suomalaisen tiedusteluviranomaisen mahdollisuus osallistua Suomalaisen yhteiskunnan huoltovarmuuden turvaamiseen ja kansainvälisestikin katsoen tärkeään käytännön tietoturvallisuutta edistävään tiedonvaihtoon mahdollistetaan lainsäädännöllä.

Ehdotuksemme on, että pykälä kirjoitetaan uudestaan seuraavaan muotoon:

- -

75 §

Tietoturvaloukkauksen paljastamisen kannalta tarpeellisten tunnisteiden luovuttaminen yrityksille ja yhteisöille

Sotilastiedusteluviranomainen saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankittuja tietoturvaloukkauksen paljastamista edesauttavia tietoja

yritykselle, yhteisölle tai viranomaiselle, jos tietojen luovuttaminen on tarpeen maanpuolustuksen turvaamiseksi, kansallisen turvallisuuden suojaamiseksi tai yrityksen tai yhteisön etujen turvaamiseksi.

- -

Ehdotetun muokkauksen jälkeen pykälä olisi hengeltään vastaavanlainen 113 §:ään kirjatun luovutusoikeuden kanssa, mahdollistaen käytännön suojautumisen todellisilta tietoturvaloukkauksilta. Vastaavanlainen kirjaus löytyy tietoliikennetiedustelusta siviilitiedustelussa annetusta lakiehdotuksesta (lakiesityksen 16 §). Myös tämä kirjaus tulisi muokata vastaavalla tavalla.

100 § Tietojen saanti yksityiseltä yhteisöltä tai henkilöltä

F-Secure katsoo, että EK:n lausunnossa on ansiokkaasti kiinnitetty huomiota ongelmiin, joita saattaa syntyä kun viranomaisen tiedonsaantioikeus kohdistetaan organisaation jäsenenä työskentelevään henkilöön. Tietovaltaisella alalla toimivana ja osaavan henkilökunnan työpanoksesta ja lojaaliudesta keskeisellä tavalla riippuvaisena yhtiönä yhdymme täysin EK:n näkemykseen, jonka mukaan toimivaltuuden kohdentaminen "henkilöön" tulisi poistaa kokonaan.

Avustamisvelvoitteet

Lakiluonnoksessa osalle yrityksistä ja yhteisöistä asetettaisiin avustamisvelvoite. Siltä osin kuin tällaisia velvoitteita yrityksille tulee, on tärkeää, että yritykset pystyvät ennakoimaan, milloin näihin kohdistuu velvoitteita ja miten tähän tulisi omassa toiminnassa varautua. Esimerkiksi Ison-Britanniassa vasta tiedustelulain säätämisen jälkeen on toden teolla käynnistynyt keskustelu siitä, mihin yrityksiin avustamisvelvoite kohdennettaisiin.

Velvoitteista aiheutuvat seuraukset tulee olla ennakoitavissa, niistä aiheutuneet kustannukset ja vaikutukset operatiiviseen toimintaan tulee olla hallittavissa ja yrityksille mahdollisesti aiheutuva haitta on oltava kompensoitu oikeudenmukaisella tavalla.

On myös tärkeää, että avustamisvelvollisten yritysten tukeen turvaudutaan viimesijaisena keinona eikä esimerkiksi tavalla, jossa viranomaisen omien resurssien rajallisuudesta johtuvia rajoitteita kierretään "ulkoistamalla" työllistäviä tai hankaliksi koettuja tehtäviä elinkeinoelämän kannettavaksi. Avustamisvelvoitteesta muodostuvia käytäntöjä ja velvoitteesta elinkeinoelämälle mahdollisesti

aiheutuvia haittoja tulisi jatkotyössä seurata tarkasti. F-Secure yhtyy tältäkin osin EK:n lausunnossa ja sen liitteessä esitettyihin huomioihin.

Muilta osin F-Secure viittaa Elinkeinoelämän keskusliiton ja Tietoturvaklusteri FISC ry:n lausuntoihin sekä kehottaa perehtymään myös siviilitiedustelusta ja tiedustelutoiminnan valvonnasta ehdotettuihin lakeihin antamiimme lausuntoihin.

Koivunen Erka
F-Secure Oyj - CISO Office