Hallintovaliokunnalle 2018-03-08

HE 198/2017, HE 202/2017, HE 203/2017

F-SECUREN LAUSUNTO TIEDUSTELULAEISTA

F-Secure kiittää mahdollisuudesta lausua historiallisesta lakiuudistuksesta. F-Secure käsittelee sotilas- ja siviilitiedustelua sekä perustuslain 10 §:n muutosta koskevat lait kokonaisuutena.

Yleisellä tasolla F-Secure kannattaa esitettyjä tiedustelulakeja sekä perustuslain muutosta.

Lakien ja lainvalmistelun julkisuudesta

F-Secure on seurannut sotilas- ja siviilitiedustelulakien valmistelua tiiviisti ja osallistunut vuosina 2015-2017 Elinkeinoelämän keskusliiton johtaman seurantaryhmän toimintaan. Olemme arvostaneet mahdollisuutta pysyä informoituna ja käyttäneet mahdollisuutta tulla kuulluksi jo lakivalmistelun edetessä.

On tärkeää, että tiedustelusta säädetään julkisella lailla julkisen valmisteluprosessin tuloksena. On jopa niin, että lainvalmisteluprosessin julkisuus on sitä tärkeämpää, mitä salaisempaa toimivaltuuksien käyttö on. 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.

On tärkeää, että tiedustelusta säädetään lailla julkisen valmisteluprosessin tuloksena. Toivotamme tervetulleeksi prosessin aikana lisääntyneen avoimuuden ja kannustamme viranomaisia ja päättäjiä vastaisuudessakin osallistumaan yhteiskunnalliseen keskusteluun kansallisen turvallisuuden tavoitteista, turvallisuusviranomaisten tehtävistä sekä tiedustelun suhteesta kansalaisten perusoikeuksiin kuten yksityisyydensuojaan.

Muuttuneesta uhkakuvasta

Tietoliikenteen painopisteen siirtyminen radiotaajuuksilta valokuituihin oli nähtävissä jo 1990-luvulla. Kehitykselle kuvaavaa on, että niihin aikoihin kun Euroopan Parlamentti tutki Yhdysvaltain ympäri maailmaa harjoittamaa satelliittiyhteyksien signaalitiedustelua (”ECHELON-järjestelmä”), kyseisen järjestelmän merkitys raakatiedon kerääjänä oli jo laskussa. Tiedustelutoiminnan kannalta on ensiarvoisen tärkeää, että tiedustelu voidaan kohdistaa sinne, missä tiedustelun kohde tai heidän tietonsa ovat. Näin ollen uusien lakien tarve on perustelua jo teknisen kehityksen johdosta.

Tieto- ja viestintäteknologiaan kohdistuvaa tai niitä hyväksikäyttävää häirintää ja opportunistisia kyberhyökkäyksiä on jo nähty Suomessakin, mutta toistaiseksi vaikutuksiltaan rajattuina yksittäistapauksina. Suomella ei kuitenkaan ole mitään immuunitekijää, joka tekisi hyvin resursoidun hyökkääjän toiminnan tyhjäksi, pikemminkin päinvastoin. Yhteiskuntamme on korostetun riippuvainen luotettavasta tieto- ja viestintäteknologiasta ja automaatiosta. Riippuvuus synnyttää haavoittuvuuden. Tekniseen infrastruktuuriin kohdistetun tahallisen häirinnän keinoin voidaan vaikuttaa laajalti koko yhteiskunnan prosesseihin rahaliikenteestä joukkoliikenteen ja tiedonvälityksen kautta energianjakeluun, teolliseen tuotantoon ja jopa vaaleihin. Tapahtuneen jälkeen suoritettava rikostutkinta ei riitä turvaamaan kansallisia tai Suomeen sijoittuneen elinkeinoelämän etuja. On tärkeää että valmisteilla olevista hyökkäyksistä on tiedustelun keinoin saatavissa ennakkotietoa.

Yleistä F-Securen suhtautumisesta tiedustelulakiehdotuksiin

Ehdotetuilla toimivaltuuksilla viranomaiseen on mahdollista murtaa perustuslain 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.

Subjektiivisesti tiedustelun kohteen näkökulmasta kyse olisi luonnollisesti tietoturvaloukkauksista ja viestintäsalaisuuden loukkauksista.

Tekniseltä tasolta tarkastellen tietoturvaloukkaus näyttää aina tietoturvaloukkaukselta ja viestintäsalaisuuden loukkaus viestintäsalaisuuden loukkaukselta riippumatta siitä, suorittaako toimenpiteen viranomainen vai rikollinen ja millä laillisella oikeutuksella tämä toimintaansa perustelee. Tämä on F-Securen kannalta merkityksellistä, koska yrityksemme tuottaa ratkaisuja juuri tällaisilta uhilta suojautumiseen. Koska tekniseltä uhalta suojautumiseen tarkoitetun työkalun ei ole mahdollista tunnistaa tilannetta, jossa hyökkäykselliset toimenpiteet suorittaakin laillinen taho laillista kohdetta vastaan, jää ainoaksi vaihtoehdoksi tarjota suojaa kaikkia tieto- ja kyberturvallisuuden uhkia vastaan.

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 yritykselle on, että yrityksemme pääkonttorin sijoittautumismaan lainsäädäntö ei jatkossakaan velvoita keinotekoisesti heikentämään ohjelmistojemme turvallisuutta esimerkiksi takaporttien muodossa tai vaatimalla meitä ummistamaan silmiämme tietoturvaloukkauksilta. Tämä on ensiarvoisen tärkeää paitsi asiakkaillemme antaman arvolupauksen kannalta, myös laajemminkin kaikkien suomalaisten tietoteknisten ja kyberturvallisuuden alan palvelujen ja tuotteiden uskottavuuden kannalta.

Yksityiskohtaisia huomioita

Haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttaminen yrityksille ja yhteisöille

Siviilitiedustelulakiehdotuksen 16 § ja sotilastiedustelulain 17 ja 71 § mahdollistaisivat, että viranomainen luovuttaa tietoliikennetiedustelun keinoin toteutetun tiedustelutehtävän yhteydessä saamiaan tietoja haittaohjelmista ja tietoturvaloukkausten tekotavoista yrityksille ja yhteisöille. Olemme tyytyväisiä havaitessamme, että siviilitiedustelulakiin kirjattu luovutusoikeus nähdään 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 (esimerkiksi yhteyksien 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.

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 käyty keskustelua 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 viittaa myös Elinkeinoelämän keskusliiton ja Tietoturvaklusteri FISC ry:n lausuntoihin.

Erka Koivunen
Tietoturvallisuusjohtaja
F-Secure Oyj