Liikenne- ja viestintävaliokunnalle

F-SECURE OYJ'N LAUSUNTO SÄHKÖISEN VIESTINNÄN TIETOSUOJA-ASETUKSESTA VASTAUKSENA LAUSUNTOPYYNTÖÖN (U 19/2017 vp)

Valiokunta on pyytänyt F-Securea arvioimaan ehdotettua sähköisen viestinnän tietosuoja-asetusta (jäljempänä "asetusluonnos") erityisesti esineiden internetin (IoT) ja sen sääntelyn kannalta. F-Secure Oyj toteaa seuraavaa vastineena annettuun lausuntopyyntöön liittyen seuraavaa.

Asetusluonnos sisältää monia kannatettavia ehdotuksia oikeustilan parantamiseksi etenkin yksityisyyden kannalta liki suojattoman verkkoselailun / sovelluskäytön osalta. Keskitymme kuitenkin tässä sähköisen viestinnän tietosuojasääntelyn ulottamiseen uusiin soveltamisaloihin.

PERUSTELUITA LAAJEMPI SOVELTAMISALAKENTTÄ

Nyt kumottavaksi ehdotettava sähköisen viestinnän tietosuojadirektiivi sääntelee lähinnä yleisissä viestintäverkoissa harjoitettavaa televiestintää, kuten perinteisiä puhelinpalveluja, tekstiviestejä ja sähköposteja. Ehdotetun sähköisen viestinnän tietosuoja-asetuksen myötä vastaavaa sääntelyä laajennettaisiin kaikkiin viestintämuotoihin, mukaan lukien esineiden internetissä tapahtuvaan viestintään. Tämän johdosta myös viestinnän yksityisyyttä koskevan lainsäädännön soveltamisala laajenee aiempaa monimuotoisemmaksi. Valitettavasti tämä ei ole täysin ongelmatonta.

Esimerkkeinä mainittakoon seuraavat:

A) koneiden keskinäisen viestinnän sisällyttäminen ulottaa viestintäsalaisuuden tilanteisiin joihin ei aina sisälly lainkaan viestintäsalaisuuden kaltaista oikeushyvää suojattavakseen;
B) viestinnän tietoturvaperusteisen puuttumisen poikkeama on alimitoitettu, sikäli kun se sulkee ulkopuolelleen päätelaitteiden tietoturvaohjelmistot.

A) Suojattava oikeushyvä

Esineiden internetin toimintaympäristössä korostuu asetusehdotuksen perusoletuksen haasteellisuus siitä, että kaikki viestiliikenne olisi luottamuksellista ja sen tulisi olla viestinnän yksityisyydensuojan (ns. viestintäsalaisuuden piirissä).

F-Secure havainnoi huomattavissa määrin haittaliikennettä (haittaohjelmia, bottiverkkojen ohjaamia palvelunestohyökkäyksiä, roskapostiviestintää) joilla ei ole viestintäsalaisuuden kannalta suojattavaa oikeushyvää. Myös teollisen ympäristön viestinnässä – esim. kerrostalon jätesäiliö ilmoittaa täyttöasteensa jätteenkuljetusyritykselle tai laivan moottorin osat viestivät keskenään – ei aina ole kyse viestintäsalaisuuden kannalta keskeisestä alueesta. Tämän johdosta olisi tarkoin harkittava ko. säännöstön kategorista ulottamista kaikkeen viestintään, sikäli kun soveltamistilanteessa ei ole

kytkentää viestintäsalaisuudella suojeltaviin kommunikaation ja tiedonsaantioikeuden kaltaisiin oikeushyviin. Huolemme on, että mikäli yllämainittu haittaliikennekin tai koneliikenne tulkitaan oletusarvoisesti osaksi luottamuksellista viestintää, hankaloittaa tämä siihen puuttumista. Erityisesti kohdassa B) mainitun tietoturvan suppeamman tietoturvan puuttumisperiaatteen johdosta.

Esineiden internetissä esiin noussut suurin tietoturvaongelma ei ole toistaiseksi ollut viestintäsalaisuuden puute. Suurin ongelma on se, että internettiin yhdistetyt laitteet ovat pääsääntöisesti – monesti valmistajien laiminlyöntien takia – erittäin heikosti suojattuja tietomurtoja sekä luvatonta käyttöä vastaan. Tämän takia IoT-laitteet valvontakameroista lypsyautomaatteihin ovat palvelunestohyökkäyksissä usein käytettyjä työkaluja. Tämän kehityksen voidaan olettaa jatkuvan toistaiseksi. Esineiden internetin tuotteiden valmistajat haluavat tuotteidensa kautta analysoida asiakkaiden käyttäytymistä ja jonka johdosta ne varustetaan käyttäytymisanalytiikkaa lähettävillä tietoliikenneyhteyksillä. Tietoturvauhka kohdistuu pääosin kolmansia kohtaan, ja tämän takia esineiden internetin tuotteiden suojaamiseen ei panosteta.

"Appliance makers: stop trying to connect to the Internet, you're no good at it. ®" #miele



Dishwasher has directory traversal bug

Thanks a Miele-on for making everything dangerous, Internet of things security slackers

theregister.co.uk

Esineiden internetissä liikkuvasta sähköisestä viestinnästä voi johtaa merkittävän määrän henkilöiden yksityiselämään juontuvia johtopäätöksiä. Esimerkiksi omakotitalon valaistus- tai sähkönkulutusjärjestelmien viestinnästä. Tämänkaltaisen johdetun tiedon ja profiloinnin suhteen on tosin jo olemassa lainsäädäntökehys; voimaantuloaan odottava yleinen tietosuoja-asetus

B) Tietoturva

Yllämainittu lainsäädännön periaatteiden skaalautuvuusongelma näkyy siinä kuinka asetusehdotus käsittelee tietoturvaa. Asetusluonnos mahdollistaa tietoturvaperusteisen puuttumisen viestin välitystietoihin ja sisältöön vain *sähköisten viestintäverkkojen ja -palvelujen tarjoajille* ja vain *viestintäverkkojen ja -palvelujen turvallisuuden turvaamiseksi*. Toisin sanoen *vain* viestinnän välittäjät arvioivat tietoturvaa ja *vain* viestintäverkkojen ja -palvelujen turvallisuuden kannalta, eivät päätelaitteen turvallisuuden kannalta.

Muiden kuin viestinnän välittäjien ja asetusehdotuksen 5. artiklan periaatteiden (sähköisen viestinnän luottamus) välinen suhde jätetään epäselväksi. Tämän valossa emme ole huolissamme vain loppukäyttäjän tietoturvallisuudesta vaan edustamamme tietoturvateollisuuden kyvystä tuottaa palvelujamme laillisesti.

Esimerkinomaisesti, F-Securen päätelaiteohjelmistot huolehtivat tietoturvasta seuraavasti:

> Asiakkaan viestintäliikenne ohjataan pilvipalveluumme, jonka tarjoamin kootuin resurssein voimme tutkia viestintäliikenteen haittasisältöjen varalta, kehottaa asiakasta pysymään poissa vaarallisiksi profiloiduilta sivustoilta ja karsia käyttäjän yksityisyyttä vaarantavat seurantaevästeet. Varsinaisen tietoturvapalvelun mahdollistamiseksi siirrämme osia päätelaitteen tietoliikenteestä käymään palvelimillamme. Viestinnän välittäminen ei kuitenkaan ole palvelun varsinainen tarkoitus (erotuksena esimerkiksi tietoliikenneyhteyden tarjoamisesta tai pikaviestinsovelluksesta), vaan tietoturvatarkastuksen toteutustavasta johtuva välttämätön paha.

Nykyinen tulkintamme tällaisen toiminnan luonteesta on, että olemme tietoyhteiskuntakaaressa tarkoitettu lisäarvopalvelun tarjoaja. Ja käsittelemme viestiliikennettä tietoyhteiskuntakaaren 138 §'n mukaisin oikeutuksin. Olemme kokeneet tämän ongelmattomana koska toimimme viestinnän välittäjien kanssa yhtäläisin oikeuksien asiakkaidemme suojaamiseksi. Kumpikin taho keskittyy oman osaamisen kannalta keskeisten osioiden suojaamiseen.

Kaltaisemme tietoturvapalvelutarjoajat (ns. päätelaitteiden anti-virus ohjelmistot ja IoT-tietoturvaa tarjoavat palvelut) olisivat"toimijaneutraalin" asetusehdotuksen jälkeen heikommassa asemassa kuin vastaavaa palvelua toimittavat viestinnän välittäjät. Eli asetusehdotus paradoksaalisesti jopa tältä osin heikentää tietoturvaa.

Tämä johtuu siitä, että asetusehdotuksen myötä meidän kaltaisiemme toimijoiden viestintään puuttumisen oikeuttamisperuste joko katoaisi(?) tai meitä kehotettaisiin – asetusluonnoksen mukaisesti – tiedustelemaan jatkuvasti asiakkaalta kuuden kuukauden välein tämän halusta saada tietoturvaa (asetusehdotuksen 9.3). Nämä pakottaisivat suunnittelemaan palvelun toteutuksen sellaiseksi, että emme pystyisi enää takaamaan käyttäjillemme näiden toivomaa tietoturvan ja tietosuojan tasoa.

Nykyään eri toimijat ovat tietoyhteiskuntakaaren alla yhtenevässä tilassa. Mikäli tämä tilanne ylläpitää asetusehdotuksen alaisessa maailmassa, tulisi joko kaikki käyttäjän tietoturvapalvelut saattaa

asetusehdotuksen 6.1.b) alaisiksi, tai viestintätietoja lisäarvopalveluntarjoajana (/ tietoyhteiskunnan palveluna) käsittelevät tahot voisivat jatkaa toimintaansa.

YLEISET LISÄKOMMENTIT

Suostumuksesta

Asetusehdotuksessa nostetaan päätelaitteen käyttäjän suostumus monessa kohtaan keskiöön. Varoitamme tämän johtamisesta jo nykyisissä evästeilmoituksissa ja käyttöliittymissä havaittavaan ”suostumusväsymykseen”. Ihmisen kyvykkyys hallinnoida suostumuksia häviää aina suostumuksia toistuvasti pyytävälle automaatiolle. Kehotamme lainsäätäjää pitämään suostumuksen perusteena vain sellaisessa viestintään / päätelaiteen sisältöön puuttumisessa, joka ei ole ehdottoman välttämätöntä tietoyhteiskunnan palvelun toimittamiselle. Vastaavaa kritiikkiä esitettiin lainsäädäntövaiheessa yleistä henkilötietoasetusta kohtaan. Tämä kritiikki johti ’oikeutetun edun’ laajempaan käyttöön käsittelyperusteena ja uskoaksemme parempaan tosiasialliseen tietosuojaan.

Suostumuksen nostaminen asetusehdotuksessa keskeiseen asemaan johtaa myös tilanteeseen, jossa esimerkiksi asiakkaalle viestintäliikennettä valvovan tietoturvapalvelun oikeutukseksi tulee yleisen henkilötietoasetuksen suostumusperuste? Vaikka ko. käsittelyperusteena toimisi luonnollisemmin yleisen henkilötietoasetuksen logiikan mukaisesti esimerkiksi ’palvelun toimittaminen’ tai ’oikeutettu etu’. Eli asetusehdotus ei tällaisenaan selkeytä oikeustilaa.

Lainsäädännön aikataulusta

F-Secure ei näe kannatettavana lainsäädäntötyötä, missä tätä asetusluonnosta pyritään – mahdollisesti laadun kustannuksella – kiirehtimään eteenpäin lainsäädäntöprosessissa, vaikka sen keskeiset määritelmät ovat riippuvaisia eurooppalaisen sähköisen viestinnän säännöstön vielä keskeneräisestä sääntelytyöstä.

Ehdotamme asian ratkaisemista esimerkiksi niin, että asetusluonnokseen otetaan omat määritelmänsä tai asetusluonnosta ei viedä lainsäädäntöprosessissa seuraaviin vaiheisiin kunnes telemarkkinapaketin määritelmistä on pysyvästi sovittu.

Helsingissä 27.3.2017

F-Secure Oyj

Hannes Saarinen

tietosuojavastaava, lakimies