

## **LAUSUNTO EDUSKUNNAN LIIKENNE JA VIESTINTÄVALIOKUNNALLE 13.10.2020**

**Asia:** HE 98/2020 vp Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräksi siihen liittyviksi laeiksi

### **Lausunnon tausta**

Insta antaa lausunnon huoltovarmuuskriittisenä toimijana ja Suomen Puolustusvoimien strategisena kumppanina. Näkökulmana on roolimme kriittisten ympäristöjen tietoturvapalvelujen tuottajana sekä viestintälaitteiden tekijänä ja yhteistyömme verkkovalmistajien ja teleoperaattoreiden kanssa. Lausunnossa tarkastelemme erityisesti teledirektiivin kyber- ja tietoturvallisuuteen liittyviä kohtia.

### **Oleelliset havainnot**

Huoltovarmuuskriittisten toimijoiden osalta 5G-verkkojen laitteiden ja palveluiden on oltava tietoturvallisia ja sertifioituja. Tämä tarkoittaa myös viestintäverkon alustakomponenttien turvallisuuden takaamista.

Tietoturvallisuuden sertifiointitoiminnan rooli tulee kasvamaan. Toimivalla viranomaisella on oltava riittävät kyvykkyydet sekä osaamisen että resurssien osalta. Näkemyksemme ja kokemustemme mukaan sertifiointitoiminnan vaatimat panostukset on hallituksen esityksessä aliarvioitu. Nostamme esille erillisen tietoturvasertifiointiin keskittyneen toiminnon perustamisen.

Verkkojen turvallisuuden ajantasaisen tilannekuvan osalta on huomioitava tiedonvaihto paitsi maiden välillä, niin myös käytännön tasolla huoltovarmuuskriittisille toimijoille ja palveluiden toimittajille.

5G tulee muuttamaan nykyisiä rajoja viestintäverkon sekä ratkaisukerroksen välillä myös kriittisen infrastruktuurin toiminnassa. Täten verkkoturvallisuuden neuvottelukunnan kokoonpanossa toivotaan olevan myös huoltovarmuuskriittisten toimijoiden edustajia.

### **Laajempaa pohdintaa**

Uudet 5G viestintäverkot tulevat paitsi avaamaan uudenlaisia mahdollisuuksia, niin myös vaatimaan muutoksia turvallisuusajatteluun. 5G-verkkojen hyödyntämismahdollisuudet IoT-ratkaisuissa ja teollisuuden hallintajärjestelmissä sekä verkkojen hyödyntäminen myös kriittisillä aloilla, kuten energiahuollossa, liikenteessä, pankkitoiminnassa ja terveydenhuollossa tuovat uusia turvallisuuteen liittyviä haasteita. Myös verkkoarkkitehtuurien monimutkaistuminen sekä lähitulevaisuuden odotettavissa oleva nopea teknologinen kehitys muuttavat merkittävästi turvallisuusnäkökulmia.

5G verkkojen turvallisuuden takaaminen tarkoittaa tiedon aktiivista jakamista kansallisella tasolla turvallisen yhteiskunnan toimijoiden välillä sekä välttämätöntä EU-tason yhteistyötä mukaan lukien sääntelyn rajojen aktiivista uudelleentarkastelua. Jotta uuden teknologian tuomat hyödyt saadaan



käyttöön siten että yhteiskunta kehittyy ja teollisuus pystyy kehittämään ratkaisuja ja nostamaan EU-maiden kilpailukykyä, on toiminnan oltava ketterää ja nopeaa. On kiinnitettävä huomioita viranomaistoimijoiden resurssien riittävyyteen, tehtävä panostuksia tietoturvaosaajien koulutukseen sekä riittävään kansalliseen omavaraisuuteen kyber- ja tietoturvan alueella tukemalla teollisuuden kilpailukykyä. Omavaraisuuden säilyttämisessä on huomioitava myös mahdolliset yritysjärjestelyt.

Tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien kyberturvallisuussertifioinneissa on huomioitava toiminnon kansallinen kyvykkyys. Suomessa on oltava näkemystä pitkäjänteiseen toimintaan ja kyvykkyyttä joustavuuteen, joka vaatii riittäviä resursseja.

Jatkossa kaikki 5G verkkoon liittyvät laitteet ja palvelut on arvioitava tietoturvan osalta. Huoltovarmuuskriittisten toimijoiden osalta 5G-verkkojen palveluiden on oltava sertifioitavissa verkkotason komponenteista lähtien. Ilman valmiita linjauksia hyväksytyistä komponenttitoimittajista ja ratkaisuista hyväksymisprosessit tulevat olemaan erittäin työläitä ja hitaita.

Sertifiointitoiminnan osalta on huomioitava kansallisten toiminnan lisäksi se, että suomalaisten ratkaisujen vientimahdollisuuksien edistäminen vaatii toiminnan liittämistä EU-tason vaatimuksiin sekä standardointitoimintaan.

5G-verkkojen kyberturvallisuus liittyy vahvasti kansalliseen turvallisuuteen, joten toimenpiteiden on oltava riittävissä määrin jäsenvaltioiden toimivallassa. Keinovalikoiman tehokkaaksi täytäntöön panemiseksi, verkkojen kyberturvallisuuden varmistamiseksi, yhteensopivuuden varmistamiseksi ja toimenpiteiden riittävän painoarvon saavuttamiseksi on kuitenkin huolehdittava EU-tason koordinaatiosta ja yhteisestä linjasta.

Tampereella 12.10.2020

Insta DefSec Oy

Marko Hautakangas  
Liiketoimintajohtaja, Kyberturvallisuus