Ericssonin vastine: 5G kyberturvallisuuteen liittyvä pykäläluonnos

Päivämäärä: 26.2.2020

Vastaanottaja: Kirjaamo / Liikenne- ja viestintäministeriö

Lähetys sähköpostitse: Kyllä

Lähettäjä: Mikko Karikytö Head of Ericsson Network Security on behalf of Ericsson Finland.

Ericsson kiittää mahdollisuudesta kommentoida 5G-teknologiaan liittyvää lakimuutosehdotusta sekä sen perustelumuistiota. Muutosehdotus koskee lakia 7.11.2014/917 Laki sähköisen viestinnän palveluista pykälää 244 a Viestintäverkon kriittisissä osissa käytettävät laitteet.

Ericsson on perehtynyt lakimuutosehdotukseen ja sen tavoitteisiin. Ericsson ei kommentoi lakimuutosehdotuksen yksityiskohtia, mutta haluaisi korostaa keskeisiä nostoja EU:n yhteisestä riskiaviosta ja sitä koskevasta keinovalikoimasta.

Tämä dokumentti on yhteenvetävä suomennos Ericssonin virallisesta lausunnosta (liitteenä samassa sähköpostissa, jolla tämä toimitetaan), eikä näitä dokumentteja tule käsitellä erillisesti.

1. Yksittäisiä laitevalmistajia koskevat riskiarvot

Ericsson on yhteydessä asianomaisiin päätöksentekijöihin ja viranomaisiin seuraavien periaatteiden mukaisesti, kun asiat liittyvät toimitusketjuihin sekä laitevalmistajia koskeviin riskiarvioihin, mukaan lukien ei-tekniset näkökulmat:

- Ericsson ei ota kantaa kilpailijoidensa turvallisuustilanteeseen.
- Ericsson ei ota kantaa valtioiden kansallisen turvallisuuden politiikkaan, päämääriin tai päätöksiin.

- Ericsson haluaa tuoda esiin, että kaikki tähän mennessä 5G-lakipykälät implementoineet maat ovat arvioineet Ericssonin turvalliseksi laitevalmistajaksi. Ericssonin on arvioitu täyttävän sekä tekniset että ei-tekniset kriteeristöt.
- Minkä tahansa valtion kansallista turvallisuutta koskevat päätökset tulee tehdä itsenäisesti, eikä Ericssonilla ei ole kantaa päätöksentekoon muuten, kuin jos ne liittyvät johonkin seuraavista:
    - Ericsson tekee yhteistyötä päätöksentekijöiden kanssa rajoittamattoman markkinoille pääsyn turvaamiseksi kansallisille 5G-markkinoille. Tarkoituksena on edistää liiketoiminnan edellytyksiä ja samalla varmistaa, että lakisääteisiä vaatimuksia noudatetaan. EU: n kannalta tämä sisältää sen, että varmistetaan, että yksittäisten toimittajien ei-teknistä arviointia, sellaisena kuin se on määriteltynä kaikissa jäsenvaltioissa hyväksytyssä EU: n yhteisessä 5G-työkalupakissa, sovelletaan objektiivisesti EU:n määrittelemien perusteiden perusteella. Tällä pyritään varmistamaan ennustettava sääntely-ympäristö EU: n rajojen yli.
    - Tähän sisältyy myös sen varmistaminen, että yksittäisten toimittajien ei-teknistä arviointia EU: n yhteisen 5G-työkalupakin mukaisesti sovelletaan 5G-verkon komponentteihin EU: n työkalupakin mukaisesti kriittisiksi tai arkaluontoisiksi määritellyille tärkeille verkko-osuuksille, jotta varmistetaan yhdenmukainen lähestymistapa koko EU:ssa.
- Laitevalmistajien arvioinnin tavoitteena tulisi olla:
    - De-politisoitu: toimivaltaisen ja riippumattoman viranomaisen olisi voitava tehdä tosiasioihin perustuva tietoinen päätös tavoitteista ja suhteellisuudesta.
    - Tavoitteellista: toimivaltaisen kansallisen viraston tai viranomaisen suorittama arviointi perustuu määriteltyihin kriteereihin, EU:n kontekstissa yhteiseen työkalupakkiin.
    - Suhteellista: kohdistettu määriteltyihin kriittisiin sektoreihin ja niihin järjestelmiin / komponentteihin, jotka ovat haavoittuvimpia käyttötapausten kriittisyyden, verkkojen käyttöönoton ja tekniseen turvallisuuteen liittyvien tosiseikkojen perusteella, kuten määritelty EU:n työkalupakissa.
    - Tehokasta: toimenpiteiden toteuttamisen tulisi olla kokonaisvaltaista kattaen kaikentyyppiset liiketoimet, esimerkiksi laitteiden myynti, operointipalvelut sekä järjestelmien tarjoamisen palveluna.
    - Ennakoitavissa: täytäntöönpano oikeudellisesti sitovalla päätöksellä tai lainsäädännöllä, minimoimalla markkinoiden epävarmuus.
- Arvioinnin ei pitäisi olla mielivaltaista eikä peiteltyä kaupan protektionismia. Esimerkiksi sen olisi oltava yhteensopiva WTO:n ja EU:n kauppalain kanssa, mukaan lukien kansallista turvallisuutta koskevat poikkeukset.

2. 5G-verkot osana kriittistä infrastruktuuria

Euroopan komission linjausten mukaisesti EU-jäsenvaltioiden tulisi huomioida seuraavat asiat 5G:n liittyen:

- 5G mahdollistaa teollisen muutoksen tulevaisuudessa, ja turvallisuus on keskeinen osa 5G:n standardointia ja arkkitehtuuria.
- 5G-verkko muodostaa kriittisen infrastruktuurin
- 5G verrattuna 4G:n tarjoaa turvallisuuden näkökulmasta tärkeitä parannuksia, ja näin parempaa turvallisuutta loppukäyttäjille.
- Teknologian kehittyminen kuten ohjelmistopohjaiset verkot, verkon toimintojen virtualisointi sekä reunalaskenta, eli verkon toimintojen siirtäminen lähelle loppukäyttäjää johtavat verkon kriittisten ja tiedoiltaan arvokkaiden toimintojen leviämiseen core-verkosta radioverkkoon ja jopa loppukäyttäjälaitteeseen.

3. Ei-tekniset haavoittuvuudet

Teknisen haavoittuvuushallinnan rajallisuus ei-tekniset haavoittuvuuksien hallinnassa

- Testilaboratoriossa tapahtuvat tekniset testit antavat tietoa verkosta tietyssä ajassa ja tarkoin määritellyssä testikonfiguraatiossa.
- Laboratoriossa tehtävät testit sekä ohjelmistoille että laitteistolle eivät osoita tai paljasta operatiivisten verkkojen konfiguraatioissa olevia haavoittuvuuksia.
- Modernit viestintäverkot kehittyvät jatkuvasti. Myös niiden ohjelmistoja kehitetään ja päivitetään kokoajan, jotta esimerkiksi uusilta ja kehittyviltä uhkilta voitaisiin suojautua. Tästä syystä kuitenkin testilaboratoriossa tehtävät kokeet eivät peilaa realistista tilannetta käytössä olevassa verkossa sen jälkeen, kun ohjelmistopäivitykset on tehty.
- Lähdekoodin tarkastelua ei ole tarkoitettu turvatakuuksi niiden järjestelmien osalta, joita päivitetään jatkuvasti. Tällaisiin järjestelmiin luetaan muun muassa viestintäverkot. Viestintäverkoissa käytettävien lähdekoodien tarkastelu ei tuo lisäarvoa haavoittuvuuksien tarkastelussa ja arvioinnissa.
- Lähdekoodia sellaisenaan ei ajeta tietokoneessa (kuten 5G-verkkolaitteessa), vaan lähdekoodista käännetty konekielinen suoritettava ohjelma, eli binääri. Binäärimuotoinen ohjelma on koneluettavassa muodossa. Lähdekoodin tarkastelu haavoittuvuuksien löytämiseksi voidaan kiertää uhkatoimijan toimesta lisäämällä haitallinen koodi kääntäjän kautta joka lähdekoodista luo binäärin.

DOKUMENTIN LOPPU