LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJA

Biudžetinė įstaiga, Totorių g. 25, LT-01121 Vilnius, tel.: (8 5) 273 5501 / 262 4821, faks. (8 5) 264 8517, el. p. kam@kam.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188602751, PVM mokėtojo kodas LT100001016116

Lietuvos Respublikos ryšių reguliavimo tarnybai

2019-04- Nr.

DĖL TEISĖS AKTO PROJEKTO

Lietuvos Respublikos krašto apsaugos ministerija teikia savo pastabas ir pasiūlymus dėl Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymo „Dėl Radijo ryšio plėtros 3400–3800 MHz radijo dažnių juostoje plano patvirtinimo“ projekto, paskelbto Lietuvos Respublikos Seimo kanceliarijos teisės aktų informacinėje sistemoje (TAIS Nr. 19-2836, toliau – projektas).

Atkreipiame dėmesį į tai, kad Europos Komisija 2019 m. kovo 26 d. pateikė rekomendaciją dėl praktinių veiksmų ir priemonių, kuriomis siekiama visoje Europos Sąjungoje užtikrinti aukštą 5G tinklų kibernetinio saugumo lygį, rinkinio (toliau – rekomendacija).

Rekomendacija nustato tokį praktinių veiksmų ir priemonių rinkinį nacionaliniu ir Europos Sąjungos lygiu:

1. Nacionaliniu lygiu:

1.1. Valstybės narės iki 2019 m. birželio 30 d. turi atlikti 5G tinklų infrastruktūros rizikos vertinimą (toliau – rizikos vertinimas), nustatydamos jautriausius elementus, kurių saugumo pažeidimai turėtų didžiausią neigiamą poveikį, ir perduoti jo rezultatus Europos Komisijai ir Europos Sąjungos tinklų ir informacijos apsaugos agentūrai (toliau – ENISA) iki 2019 m. liepos 15 d.

1.2. Valstybės narės iki 2019 m. birželio 30 d. turi peržiūrėti kibernetinio saugumo reikalavimus ir rizikos valdymo metodus, taikomus nacionaliniu lygiu, įvertindamos kibernetinio saugumo grėsmes, kurios gali kilti dėl a) *techninių veiksnių* ir b) *kitų veiksnių* (teisinė bazė ir vykdoma politika).

1.3. Nuo 2019 m. liepos 15 d. valstybės narės, remdamosi atlikto rizikos vertinimo duomenimis ir stebėdamos Europos Sąjungos lygio veiksmus, turi:

1.3.1. atnaujinti kibernetinio saugumo reikalavimus ir rizikos vertinimo metodus, taikomus 5G tinklams;

1.3.2. atnaujinti technines ir organizacines priemones, kurias privalo taikyti viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikėjai, kad suvaldytų elektroninių ryšių tinklų ir jais teikiamų paslaugų rizikas;

1.3.3. dirbti su Europos Komisija, nustatydamos kibernetinio saugumo reikalavimus ir pareigas, kuriuos turi atitikti ir prisiimti įmonės, dalyvaujančios konkursuose dėl radijo dažnių įsigijimo, teikiant 5G ryšį; taip pat nustatydamos kibernetinio saugumo reikalavimus viešųjų pirkimų procesuose, susijusiuose su 5G ryšiu;

1.3.4. naudoti kitas apsaugines priemones, skirtas galimoms kibernetinėms grėsmėms sumažinti.

1.4. Valstybės narės, bendradarbiaudamos su Europos Komisija, turi įvertinti šios rekomendacijos poveikį iki 2020 m. spalio 1 d.

2. Europos Sąjungos lygiu:

2.1. Valstybės narės iki 2019 m. balandžio 30 d. turi pradėti dalyvauti Bendradarbiavimo grupės, įsteigtos pagal Europos Parlamento ir Europos Sąjungos Tarybos 2016 m. liepos 6 d. direktyvą (ES) 2016/1148 „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“ (toliau – NIS direktyva), 5G tinklų temos veikloje.

2.2. Valstybės narės turi dalytis informacija tarpusavyje ir su atitinkamomis Europos Sąjungos institucijomis, siekdamos pakelti bendrą supratingumo apie 5G tinklų keliamas kibernetinio saugumo rizikas lygį.

2.3. Valstybės narės turi perduoti savo atlikto rizikos vertinimo rezultatus Europos Komisijai ir ENISA iki 2019 m. liepos 15 d.

2.4. ENISA turės pabaigti specifinį 5G tinklų grėsmės žemėlapį iki 2019 m. spalio 1 d. ENISA padėti turėtų Bendradarbiavimo grupė ir reagavimo į kompiuterinius saugumo incidentus tarnybos, įsteigtos pagal NIS direktyvą.

2.5. Valstybės narės iki 2019 m. spalio 1 d., padedamos Europos Komisijos ir bendradarbiaudamos su ENISA, turės pabaigti Bendrą saugumo ataskaitą apie 5G tinklų keliamas grėsmes Europos Sąjungos lygiu. Pageidaujama, kad ši ataskaita būtų teikiama kelių valstybių narių, kurios naudotų ir dalintųsi atitinkama technologine ekspertize ir priemonėmis, susijusiomis su 5G tinklais.

2.6. Bendradarbiavimo grupė turi nustatyti gerąsias praktikas, taikomas nacionaliniu lygiu.

2.7. Remdamasi gerosiomis praktikomis, Bendradarbiavimo grupė iki 2019 m. gruodžio 31 d. parengs Įrankių rinkinį, kurį sudarys: *sąrašas saugumo rizikų*, kurios gali daryti įtaką 5G tinklų kibernetiniam saugumui, pvz., tiekimo grandinės rizika, programinės įrangos pažeidžiamumo rizika, priėjimo kontrolės rizika ir pan.; *riziką mažinančios priemonės*, pvz., trečiųjų šalių techninės,

programinės įrangos ar paslaugų sertifikavimas, formalūs techninės ir programinės įrangos testai ar jos tinkamumo patikrinimai ir kt.

2.8. Europos Komisija, remdamasi Įrankių rinkiniu, plėtos minimalius bendruosius reikalavimus, siekdama užtikrinti aukštą 5G tinklų kibernetinio saugumo lygį.

2.9. Įsigaliojus Europos Parlamento ir Tarybos reglamentui dėl Europos Sąjungos kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas), Europos Komisija ir ENISA nustatys sertifikavimo schemas, taikomas Europos Sąjungos lygiu. Valstybės narės kviečiamos bendradarbiauti su ENISA ir Europos Komisija ir kartu siekti nustatyti sertifikavimo schemas, apimančias 5G tinklą ir ją sudarančią įrangą. Kai tai bus padaryta, valstybės narės turėtų šios srities sertifikavimą padaryti privalomą įdiegdamos nacionalinius techninius reikalavimus.

Atsižvelgdami į rekomendaciją ir ypač į tai, kad planuojama ne tik nustatyti papildomus bendruosius kibernetinio saugumo reikalavimus, bet ir sertifikavimo schemas, taikomas 5G tinklui, **siūlome atidėti** projekto tvirtinimą, kol bus nustatyti minimalūs bendrieji kibernetinio saugumo reikalavimai, užtikrinantys 5G tinklų aukštą kibernetinio saugumo lygį, ir numatytos apytikslės sertifikavimo schemų sukūrimo ir įsigaliojimo datos.

Krašto apsaugos viceministras Edvinas Kerza

Jonas Skardinskas, tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt