REKOMENDACIJOS

KOMISIJOS REKOMENDACIJA (ES) 2019/534

2019 m. kovo 26 d.

5G tinklų kibernetinis saugumas

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 292 straipsnį,

kadangi:

(1) Komisija pripažįsta, kad 5-osios kartos (5G) tinklų technologijų diegimas yra vienas pagrindinių veiksnių, sudarančių sąlygas teikti ateities skaitmenines paslaugas, ir vienas iš Bendrosios skaitmeninės rinkos strategijos prioritetų. Siekdama užtikrinti, kad nuo 2020 m. Sąjunga turėtų skaitmeninei transformacijai reikalingą ryšio infrastruktūrą, Komisija priėmė 5G veiksmų planą ([1]);

(2) 5G tinklai bus kuriami remiantis dabartinėmis 4-osios kartos (4G) tinklų technologijomis – jie suteiks galimybę teikti naujas paslaugas ir taps pagrindine didelės Sąjungos ekonomikos dalies infrastruktūra ir veikimo sąlyga. Įdiegti 5G tinklai bus pagrindas įvairioms paslaugoms, būtinoms, kad veiktų vidaus rinka ir kad būtų išlaikomos ir atliekamos visuomenei ir ekonomikai itin svarbios funkcijos (pavyzdžiai – energetikos, transporto, bankų, sveikatos ir pramoninių procesų valdymo sistemos). Skaitmeninė infrastruktūra ir 5G tinklai bus vis daugiau naudojami ir organizuojant demokratinius procesus, pavyzdžiui, rinkimus;

(3) nuo 5G tinklų priklauso daug ypatingos svarbos paslaugų, todėl sisteminis plataus masto jų sutrikdymas turėtų itin rimtų padarinių. Taigi šiuo metu, kai kibernetinių išpuolių daugėja ir kai jie sudėtingesni nei bet kada anksčiau, 5G tinklų kibernetinio saugumo užtikrinimas yra Sąjungai strategiškai svarbus klausimas;

(4) skaitmeninei ekosistemai būtini infrastruktūros objektai yra sujungti tarpusavyje, o jų ir su jais susijusių grėsmių pobūdis – tarpvalstybinis, todėl bet kokios reikšmingos 5G tinklų pažeidžiamumo problemos ir (arba) kibernetinio saugumo incidentai vienoje valstybėje narėje neigiamai paveiktų visą Sąjungą. Todėl turėtų būti numatytos priemonės, padedančios užtikrinti aukštą bendrą 5G tinklų kibernetinio saugumo lygį;

(5) valstybės narės patvirtino, kad reikia imtis Sąjungos lygmens veiksmų. Europos Vadovų Taryba 2019 m. kovo 21 d. susitikimo išvadose nurodė laukianti Komisijos rekomendacijos dėl suderinto požiūrio į 5G tinklų saugumą ([2]);

(6) pagrindinis tikslas turėtų būti užtikrinti Europos suverenitetą, visapusiškai atsižvelgiant į Europos atvirumo ir tolerancijos vertybes ([3]). Užsienio investicijos strateginiuose sektoriuose, ypatingos svarbos turto, technologijų ir infrastruktūros įsigijimas Sąjungoje ir ypatingos svarbos įrangos tiekimas taip pat gali kelti pavojų Sąjungos saugumui;

(7) kaip pripažįstama bendrame komunikate „ES ir Kinija. Strateginė perspektyva“ ([4]), 5G tinklų kibernetinis saugumas yra labai svarbus siekiant užtikrinti Sąjungos strateginį savarankiškumą;

(8) Europos Parlamento rezoliucijoje dėl grėsmių saugumui, susijusių su Kinijos technologijų plitimu Sąjungoje, Komisija ir valstybės narės taip pat raginamos imtis Sąjungos lygmens veiksmų ([5]);

(9) šioje rekomendacijoje 5G tinklų kibernetinio saugumo rizikos klausimas sprendžiamas pateikiant gairių dėl tinkamų nacionalinio lygmens rizikos analizės ir valdymo priemonių, dėl koordinuoto Europos rizikos vertinimo ir dėl proceso, kurio tikslas – parengti bendrą geriausių rizikos valdymo priemonių rinkinį;

(10) Sąjungoje sukurta stipri teisinė sistema, skirta elektroninių ryšių tinklų apsaugai užtikrinti;

([1]) COM(2016) 588 *final*.
([2]) 2019 m. kovo 21–22 d. Europos Vadovų Tarybos išvados.
([3]) Pranešimas apie Sąjungos padėtį 2018 m. „Europos suverenumo valanda“, 2018 m. rugsėjo 12 d.
([4]) JOIN(2019) 5 *final*.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//LT.

(11) Sąjungos elektroninių ryšių srities sistema ([6]) skatinama konkurencija, vidaus rinkos plėtra ir ginami galutinių paslaugų gavėjų interesai, o Europos elektroninių ryšių kodeksu ([7]) siekiama papildomo – junglumo – tikslo, apibūdinamo šiais rezultatais: galimybių visiems Sąjungos piliečiams ir įmonėms plačiai naudotis itin didelio pralaidumo fiksuotuoju ir mobiliuoju ryšiu užtikrinimas ir plėtojimas kartu rūpinantis piliečių interesais. Direktyvoje 2002/21/EB reikalaujama, kad valstybės narės užtikrintų, kad būtų išlaikytas viešųjų ryšių tinklų vientisumas ir saugumas ir kad įmonės, teikiančios viešuosius ryšių tinklus ar viešai prieinamas elektroninių ryšių paslaugas, imtųsi techninių ir organizacinių priemonių, kad būtų tinkamai valdoma tinklų ir paslaugų saugumui kylanti rizika. Joje taip pat numatyta, kad kompetentingos nacionalinės reguliavimo institucijos turi įgaliojimus, be kita ko, įgaliojimą duoti privalomus nurodymus, reikalingus siekiant užtikrinti tokių pareigų vykdymą;

(12) be to, Europos Parlamento ir Tarybos direktyvoje 2002/20/EB ([8]) valstybėms narėms leidžiama taikyti bendrajam leidimui sąlygas, susijusias su viešųjų tinklų apsauga nuo neteisėto prisijungimo, siekiant užtikrinti pranešimų konfidencialumo apsaugą pagal Europos Parlamento ir Tarybos direktyvą 2002/58/EB ([9]);

(13) siekdama padėti vykdyti šias pareigas, Sąjunga sudarė keletą bendradarbiavimo organų. Tinklų ir informacijos apsaugos agentūra (ENISA), Komisija, valstybės narės ir nacionalinės reguliavimo institucijos parengė nacionalinėms reguliavimo institucijoms skirtas technines gaires dėl pranešimo apie incidentus, saugumo priemonių, grėsmių ir turto ([10]). Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 ([11]) įsteigta kompetentingas institucijas vienijanti bendradarbiavimo grupė (toliau – Bendradarbiavimo grupė), kurios tikslas – remti ir lengvinti bendradarbiavimą, visų pirma teikti strategines gaires dėl Reagavimo į kompiuterių saugumo incidentus tarnybų tinklo, kuris techniniu lygmeniu palengvina operatyvinį bendradarbiavimą, veiklos;

(14) būsima Europos kibernetinio saugumo sertifikavimo sistema ([12]) turėtų būti viena iš pagrindinių priemonių, padedančių skatinti užtikrinti vienodą saugumo lygį. Ji turėtų suteikti galimybę rengti kibernetinio saugumo sertifikavimo schemas atsižvelgiant į aparatinės ir programinės įrangos, susijusios su 5G tinklais, naudotojų poreikius. Atsižvelgiant į ypatingą šios infrastruktūros svarbą, atitinkamų Europos kibernetinio saugumo sertifikavimo schemų, skirtų 5G tinkluose naudojamiems informacinių ir ryšių technologijų produktams, paslaugoms ir procesams, rengimas turėtų būti neatidėliotinas prioritetas. Valstybės narės ir rinkos dalyviai turėtų aktyviai dalyvauti rengiant tokias sertifikavimo schemas, be kita ko, padėti nustatyti konkrečius 5G tinklų apsaugos profilius;

(15) nesant suderintų Sąjungos teisės aktų, valstybės narės gali nacionaliniuose techniniuose reglamentuose, priimtuose laikantis Sąjungos teisės, nurodyti, kad tam tikra Europos kibernetinio saugumo sertifikavimo schema turėtų būti privaloma. Reikalavimą dėl Europos kibernetinio saugumo sertifikavimo schemų valstybės narės gali taikyti ir vykdydamos viešuosius pirkimus bei įgyvendindamos Europos Parlamento ir Tarybos direktyvą 2014/24/ES ([13]). Be to, jos galėtų padėti kurti pagalbos mechanizmus, kaip antai pagalbos centrus, skirtus viešiesiems pirkėjams, norintiems pirkti kibernetinio saugumo sprendimus;

(16) aukštas duomenų apsaugos ir privatumo lygis yra svarbus veiksnys siekiant užtikrinti 5G tinklų saugumą. Sąjungos lygmeniu taip pat nustatytos taisyklės, kuriomis užtikrinamas asmens duomenų tvarkymo, be kita ko elektroninių ryšių srityje, saugumas. Bendrajame duomenų apsaugos reglamente ([14]) nustatytas įpareigojimas asmens duomenis tvarkyti taip, kad būtų užtikrintas jų saugumas, be kita ko, būtų užkirstas kelias neteisėtai prieigai prie asmens duomenų ir jiems tvarkyti naudojamos įrangos ar neteisėtam jų naudojimui. Direktyvoje dėl

([6]) 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų Direktyva) (OL L 108, 2002 4 24, p. 33) ir specialiosios direktyvos.

([7]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (OL L 321, 2018 12 17, p. 36).

([8]) 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo (Leidimų direktyva) (OL L 108, 2002 4 24, p. 21).

([9]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

([12]) Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (COM(2017) 477 final, 2017/0225 (COD)).

([13]) 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

([14]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

privatumo ir elektroninių ryšių nustatomos konkrečios taisyklės dėl pranešimų konfidencialumo apsaugos ir galutinių naudotojų galinių įrenginių apsaugos. Joje taip pat nustatomi įpareigojimai paslaugų teikėjams imtis tinkamų techninių ir organizacinių priemonių savo paslaugų saugumui užtikrinti;

(17) Sąjunga taip pat priėmė priemonę, kuri padės apsaugoti ypatingos svarbos, pavyzdžiui, ryšių srities, infrastruktūrą ir technologijas – ja valstybėms narėms leidžiama tikrinti tiesioginės užsienio investicijas saugumo ar viešosios tvarkos sumetimais ir sukuriamas bendradarbiavimo mechanizmas, sudarysiantis valstybėms narėms ir Komisijai sąlygas keistis informacija ir išreikšti susirūpinimą dėl konkrečių investicijų ([15]);

(18) valstybės narės ir operatoriai šiuo metu atlieka svarbius parengiamuosius veiksmus, kurių tikslas – sudaryti sąlygas plačiu mastu diegti 5G tinklus. Kelios valstybės narės išreiškė susirūpinimą dėl galimos su 5G tinklais susijusios saugumo rizikos, kylančios atliekant teisių naudotis 5G tinklams skirtomis radijo spektro juostomis suteikimo procedūras ([16]), ir nagrinėja, kokiomis priemonėmis būtų galima mažinti šią riziką;

(19) mažinant su 5G tinklais susijusią kibernetinio saugumo riziką, turėtų būti atsižvelgiama ir į techninius, ir į kitus veiksnius. Techniniai veiksniai gali apimti kibernetinio saugumo spragas, kuriomis gali būti pasinaudota siekiant neteisėtai gauti informaciją (kibernetinis šnipinėjimas dėl ekonominių ar politinių priežasčių) arba kitais piktavališkais tikslais (kibernetiniai išpuoliai, kuriais siekiama sugadinti arba sunaikinti sistemas ir duomenis). Svarbūs aspektai, į kuriuos reikėtų atsižvelgti, yra būtinybė užtikrinti, kad tinklai būtų apsaugoti visą jų gyvavimo ciklą, ir būtinybė aprėpti visą susijusią įrangą, be kita ko, įrangą, naudojamą 5G tinklų projektavimo, plėtojimo, viešojo pirkimo, diegimo, eksploatavimo ir techninės priežiūros etapais;

(20) kiti veiksniai gali apimti reguliavimo ar kitus reikalavimus, taikomus informacinių ir ryšių technologijų įrangos tiekėjams. Vertinant tokių veiksnių svarbą reikėtų atsižvelgti į, be kita ko, bendrą trečiosios valstybės įtakos riziką, visų pirma į tai, koks jos valdymo modelis, ir į tai, ar Sąjunga su atitinkama trečiąja valstybe yra sudariusi bendradarbiavimo saugumo srityje susitarimų arba dėl jos priėmusi panašių su duomenų apsauga susijusių priemonių, pavyzdžiui, sprendimų dėl tinkamumo, arba ar ta valstybė yra pasirašiusi daugiašalių, tarptautinių arba dvišalių susitarimų dėl kibernetinio saugumo, kovos su kibernetiniais nusikaltimais arba duomenų apsaugos;

(21) vienas iš svarbių veiksmų, kurie turėtų būti atlikti formuojant Sąjungos požiūrį į 5G tinklų kibernetinį saugumą, yra nacionalinio lygmens rizikos vertinimas. Šio vertinimo rezultatai padėtų valstybėms narėms atitinkamai pritaikyti nacionalines saugumo reikalavimų ir rizikos valdymo priemones;

(22) siekiant užtikrinti, kad priemonės, kuriomis siekiama šalinti šias grėsmes kibernetiniam saugumui, taip pat priemonės, būtinos siekiant užtikrinti sklandų vidaus rinkos veikimą ir asmens duomenų bei privatumo apsaugą, būtų veiksmingos, veiksmai turėtų būti koordinuojami;

(23) remiantis nacionaliniais rizikos vertinimais, turėtų būti atliktas koordinuotas Sąjungos rizikos vertinimas – valstybės narės, padedamos Komisijos, kartu su Europos kibernetinio saugumo agentūra (ENISA) turėtų nustatyti aktualias grėsmes ir atlikti bendrą peržiūrą;

(24) atsižvelgdama į nacionalinius ir Sąjungos rizikos vertinimus, Bendradarbiavimo grupė turėtų parengti priemonių rinkinį, kuriame būtų nustatytos kibernetinio saugumo rizikos rūšys ir galimos priemonės rizikai tokiose srityse kaip sertifikavimas, bandymai ir prieigos kontrolė mažinti. Jame taip pat turėtų būti nurodytos galimos konkrečios priemonės, kuriomis galėtų būtų mažinama vienos arba kelių valstybių narių nustatyta rizika. Bendradarbiavimo grupė turėtų naudotis Europos kibernetinio saugumo agentūros (ENISA), Europolo, Europos elektroninių ryšių reguliuotojų institucijos (BEREC) ir ES žvalgybos ir situacijų centro pagalba. Šis priemonių rinkinys turėtų padėti Komisijai nustatyti būtinuosius bendrus reikalavimus siekiant papildomai užtikrinti aukšto lygio 5G tinklų kibernetinį saugumą visoje Sąjungoje;

(25) imantis priemonių kibernetinio saugumo rizikai mažinti, turėtų būti apsvarstyta galimybė skatinti įvairius tiekėjus diegiant bet kokį tinklą užtikrinti kibernetinį saugumą;

([15]) 2019 m. kovo 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/452, kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema (OL L 79I, 2019 3 21, p. 1).

([16]) Surengti aukcionus dėl bent vienos spektro juostos 2019 m. planuojama vienuolikoje valstybių narių: Airijoje, Austrijoje, Belgijoje, Čekijoje, Graikijoje, Lietuvoje, Nyderlanduose, Portugalijoje, Prancūzijoje, Vengrijoje, Vokietijoje. Dar šeši aukcionai numatyti surengti 2020 m. šiose šalyse: Ispanijoje, Jungtinėje Karalystėje, Lenkijoje, Lietuvoje (dėl kitų dažnių), Maltoje, Slovakijoje. Šaltinis: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) šia rekomendacija neturėtų būti daromas poveikis valstybių narių kompetencijai, susijusiai su viešojo saugumo, gynybos ir nacionalinio saugumo sričių veikla, ir valstybių veiklai baudžiamosios teisės srityse, visų pirma valstybių narių teisei pašalinti tiekėjus arba paslaugų teikėjus iš savo rinkų nacionalinio saugumo sumetimais,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

I. **TIKSLAI**

1) Siekiant padėti suformuoti Sąjungos požiūrį į 5G tinklų kibernetinio saugumo užtikrinimą, šioje rekomendacijoje nustatomi veiksmai, kurių turėtų būti imtasi, kad:

a) valstybės narės galėtų atlikti nacionalinio lygmens 5G tinklams kylančios kibernetinio saugumo rizikos vertinimą ir imtis būtinų saugumo priemonių;

b) valstybės narės ir atitinkamos Sąjungos institucijos, agentūros ir kitos įstaigos galėtų bendrai atlikti koordinuotą Sąjungos rizikos vertinimą, pagrįstą nacionaliniais rizikos vertinimais;

c) pagal Direktyvą (ES) 2016/1148 įsteigta bendradarbiavimo grupė (Bendradarbiavimo grupė) galėtų nustatyti galimas bendras priemones, kurių reikia imtis siekiant mažinti kibernetinio saugumo riziką, susijusią su skaitmeninei ekosistemai būtinais infrastruktūros objektais, visų pirma 5G tinklais.

II. **APIBRĖŽTYS**

2) Šioje rekomendacijoje vartojamų terminų apibrėžtys:

a) 5G tinklai – visuma su mobiliojo ir belaidžio ryšio technologija susijusių tinklo infrastruktūros elementų, naudojamų ryšio ir pridėtinės vertės paslaugoms teikti ir pasižyminčių pažangiomis veikimo savybėmis, kaip antai labai didele duomenų perdavimo sparta ir pajėgumu, nedidelės delsos ryšiu, itin dideliu patikimumu arba galimybe veikti prijungus daug įrenginių. Šie tinklai gali apimti senesnius tinklo elementus, pagrįstus ankstesnių kartų, pavyzdžiui, 4G arba 3G, mobiliojo ir belaidžio ryšio technologija. 5G tinklas apima visas susijusias tinklo dalis;

b) skaitmeninei ekosistemai būtini infrastruktūros objektai – infrastruktūros objektai, sudarantys įvairių ekonomikai ir visuomenei itin svarbių sričių skaitmeninimo sąlygas.

III. **NACIONALINIO LYGMENS VEIKSMAI**

3) Valstybės narės iki 2019 m. birželio 30 d. turėtų atlikti su 5G tinklo infrastruktūra susijusios rizikos vertinimą, be kita ko, nustatyti jautriausius elementus, kurių saugumo pažeidimai darytų didelį neigiamą poveikį. Iki tos pačios datos valstybės narės turėtų peržiūrėti nacionaliniu lygmeniu taikomus saugumo reikalavimus ir rizikos valdymo metodus, kad būtų atsižvelgta į grėsmes kibernetiniam saugumui, galinčias kilti dėl: i) techninių veiksnių, tokių kaip konkrečios techninės 5G tinklų charakteristikos, ir ii) kitų veiksnių, tokių kaip teisinė ir politikos sistema, kuri gali būti taikoma informacinių ir ryšių technologijų įrangos tiekėjams trečiosiose valstybėse.

4) Remdamosi šiuo nacionaliniu rizikos vertinimu bei peržiūra ir atsižvelgdamos į vykdomus koordinuotus Sąjungos lygmens veiksmus, valstybės narės turėtų:

a) atnaujinti taikomus su 5G tinklais susijusius saugumo reikalavimus ir rizikos valdymo metodus;

b) atnaujinti atitinkamus reikalavimus, kurie pagal Direktyvos 2002/21/EB 13a ir 13b straipsnius taikomi įmonėms, teikiančioms viešuosius ryšių tinklus ar viešai prieinamas elektroninių ryšių paslaugas;

c) taikyti bendrajam leidimui sąlygas, susijusias su viešųjų tinklų apsauga nuo neteisėto prisijungimo, ir visose būsimose teisių naudotis 5G tinklams skirtų juostų radijo dažniais suteikimo procedūrose dalyvaujančių įmonių prašyti prisiimti įsipareigojimus, susijusius su tinklų saugumo reikalavimų laikymusi pagal Direktyvą 2002/20/EB;

d) taikyti kitas prevencines priemones, kuriomis siekiama mažinti galimą kibernetinio saugumo riziką.

5) 4 punkte nurodytos priemonės turėtų apimti griežtesnius tiekėjams ir operatoriams nustatytus įpareigojimus užtikrinti jautrių tinklo dalių saugumą, taip pat atitinkamais atvejais tokius įpareigojimus, kaip įpareigojimas teikti kompetentingoms nacionalinėms institucijoms atitinkamą informaciją apie planuojamus elektroninių ryšių tinklų pakeitimus, ir reikalavimus nacionalinėse audito ir (arba) sertifikavimo laboratorijose iš anksto atlikti tam tikrų informacinių technologijų sudedamųjų dalių ir sistemų saugumo ir vientisumo bandymus.

6) Tais atvejais, kai, pavyzdžiui, ta pati įmonė eksploatuoja arba diegia tinklo infrastruktūrą daugiau nei vienoje valstybėje narėje arba kai esama esminių tinklų konfigūracijos panašumų, dvi ar daugiau valstybių narių turėtų atlikti bendras saugumo peržiūras naudodamosi ir dalydamosi atitinkama techninе kompetencija ir įranga, susijusiomis su skaitmeninei ekosistemai būtinais infrastruktūros objektais ir 5G tinklais. Europos kibernetinio saugumo agentūra (ENISA), Europolas ir Europos elektroninių ryšių reguliuotojų institucija (BEREC) turėtų teikti pirmenybę su šia sritimi susijusiems valstybių narių paramos prašymams. Šių peržiūrų rezultatai turėtų būti perduoti Bendradarbiavimo grupei ir Reagavimo į kompiuterių saugumo incidentus tarnybų tinklui.

IV. **KOORDINUOTI SĄJUNGOS LYGMENS VEIKSMAI**

7) Kad būtų suformuotas bendras požiūris į kibernetinio saugumo rizikos, susijusios su 5G tinklais, mažinimą, valstybės narės turėtų iki 2019 m. balandžio 30 d. imtis su tuo susijusio darbo Bendradarbiavimo grupėje. Valstybės narės prireikus turėtų kviesti atitinkamas institucijas dalyvauti Bendradarbiavimo grupės darbe.

Koordinuotas Europos rizikos vertinimas

8) Siekiant užtikrinti bendrą esamos ir galimos su 5G tinklais susijusios kibernetinio saugumo rizikos supratimą, valstybės narės turėtų keistis informacija tarpusavyje ir su atitinkamomis Sąjungos įstaigomis.

9) Valstybės narės turėtų iki 2019 m. liepos 15 d. perduoti nacionalinius rizikos vertinimus Komisijai ir Europos kibernetinio saugumo agentūrai (ENISA).

10) Europos kibernetinio saugumo agentūra (ENISA) turėtų nustatyti konkrečias su 5G tinklais susijusias aktualias grėsmes. Šį procesą turėtų remti Bendradarbiavimo grupė ir Reagavimo į kompiuterių saugumo incidentus tarnybų tinklas, įsteigti pagal Direktyvą (ES) 2016/1148.

11) Atsižvelgdamos į visus šiuos elementus, valstybės narės, padedamos Komisijos, kartu su Europos kibernetinio saugumo agentūra (ENISA) turėtų iki 2019 m. spalio 1 d. atlikti visai Sąjungai kylančios su skaitmeninei ekosistemai būtinais infrastruktūros objektais, visų pirma 5G tinklais, susijusios rizikos bendrą peržiūrą.

12) Atliekant šią bendrą peržiūrą pirmenybė turėtų būti teikiama rizikos, susijusios su itin jautriais ar pažeidžiamais elementais, įtrauktais į 5G tinklų pagrindinius elementus, taip pat su eksploatavimo ir techninės priežiūros centru ir pramonės reikmėms naudojamais 5G prieigos tinklo elementais, analizei.

13) Antruoju etapu ši bendra peržiūra turėtų apimti ir kitus strateginius skaitmeninės vertės grandinės elementus.

Bendras Sąjungos rizikos mažinimo priemonių rinkinys

14) Bendradarbiavimo grupė turėtų nustatyti geriausia praktika laikytinas nacionaliniu lygmeniu taikomas 4 punkte nurodyto pobūdžio priemones. Remiantis šia geriausia nacionaline praktika, iki 2019 m. gruodžio 31 d. turėtų būti sutarta dėl tinkamų, veiksmingų ir proporcingų galimų rizikos valdymo priemonių, kuriomis siekiama nacionaliniu ir Sąjungos lygmenimis mažinti nustatytą kibernetinio saugumo riziką, rinkinio, kuris Komisijai padėtų nustatyti būtinuosius bendrus reikalavimus siekiant papildomai užtikrinti aukšto lygio 5G tinklų kibernetinį saugumą visoje Sąjungoje.

15) Ši priemonių rinkinį turėtų sudaryti:

a) 5G tinklų kibernetinio saugumo rizikos rūšių sąrašas (pavyzdžiui, tiekimo grandinės rizika, programinės įrangos pažeidžiamumo rizika, prieigos kontrolės rizika, rizika, kylanti dėl teisinės ir politikos sistemos, kuri gali būti taikoma informacinių ir ryšių technologijų įrangos tiekėjams trečiosiose valstybėse);

b) galimų rizikos mažinimo priemonių sąrašas (pavyzdžiui: trečiųjų šalių atliekamas aparatinės ir programinės įrangos ar paslaugų sertifikavimas; oficialūs aparatinės ir programinės įrangos bandymai ar atitikties patikros; procesai, kuriais siekiama užtikrinti, kad būtų nustatytos ir taikomos prieigos kontrolės priemonės; produktų, paslaugų ar tiekėjų, kurie gali būti nesaugūs, nustatymas ir kt.). Šiomis priemonėmis turėtų būti mažinama visų rūšių saugumo rizika, kuri atlikus rizikos vertinimą buvo nustatyta vienoje ar daugiau valstybių narių.

16) Kai bus parengtos su 5G tinklais susijusios Europos kibernetinio saugumo sertifikavimo schemos, valstybės narės turėtų, laikydamosi Sąjungos teisės, priimti nacionalinius techninius reglamentus, kuriose būtų numatytas privalomas informacinių ir ryšių technologijų produktų, paslaugų arba sistemų, kurioms taikomos tos schemos, sertifikavimas.

17) Valstybės narės kartu su Komisija turėtų nustatyti bendrajam leidimui taikytinas sąlygas, susijusias su viešųjų tinklų apsauga nuo neteisėto prisijungimo, ir tinklų saugumo reikalavimus, kurių laikytis pagal Direktyvą 2002/20/EB būtų prašomos įsipareigoti įmonės, dalyvaujančios teisių naudotis 5G tinklams skirtų juostų spektru suteikimo procedūrose. Jei įmanoma, jie turėtų būti įtraukti į priemones, kurių imtasi pagal 4 punkto c papunktį.

18) Bendradarbiaudamos su Komisija valstybės narės turėtų nustatyti konkrečius saugumo reikalavimus, kurie galėtų būti taikomi vykdant su 5G tinklais susijusius viešuosius pirkimus. Jie turėtų apimti privalomus reikalavimus vykdant viešuosius pirkimus taikyti reikalavimą dėl kibernetinio saugumo sertifikavimo schemų, jei jos dar nėra privalomos visiems tiekėjams ir operatoriams.

V. **PERŽIŪRA**

19) Bendradarbiaudamos su Komisija valstybės narės turėtų iki 2020 m. spalio 1 d. įvertinti šios rekomendacijos poveikį, kad būtų galima nustatyti tolesnius tinkamus veiksmus. Atliekant šį vertinimą turėtų būti atsižvelgiama į koordinuoto Sąjungos rizikos vertinimo ir Sąjungos priemonių rinkinio taikymo rezultatus.

Priimta Strasbūre 2019 m. kovo 26 d.

Komisijos vardu

Julian KING

Komisijos narys