IETEIKUMI

KOMISIJAS IETEIKUMS (ES) 2019/534

(2019. gada 26. marts)

5G tīklu kiberdrošība

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 292. pantu,

tā kā:

(1) Komisija ir atzinusi 5. paaudzes (5G) tīkla tehnoloģiju izbūvi par nākotnes digitālo pakalpojumu svarīgu priekšnosacījumu un par prioritāti digitālā vienotā tirgus stratēģijā. Komisija pieņēma 5G rīcības plānu, lai nodrošinātu, ka Savienībai ir savienojamības infrastruktūra, kas nepieciešama tās digitālajai pārveidei, sākot ar 2020. gadu ([1]).

(2) 5G tīkli balstīsies uz pašreizējām 4. paaudzes (4G) tīklu tehnoloģijām, sniedzot jaunas pakalpojumu iespējas un kļūstot par Savienības ekonomikas lielas daļas centrālo infrastruktūru un virzītājspēku. Kad 5G tīkli sāks darboties, tie kļūs par stūrakmeni plašam pakalpojumu lokam, bez kuriem nav iedomājama iekšējā tirgus darbība un tādu svarīgu sabiedrisko un ekonomisko funkciju uzturēšana un darbība kā enerģētika, transports, bankas un veselība, kā arī ražošanas vadības sistēmas. Arī tādu demokrātisku procesu organizēšanā kā vēlēšanas aizvien vairāk tiks izmantota digitālā infrastruktūra un 5G tīkli.

(3) Daudzu izšķiroši svarīgu pakalpojumu atkarība no 5G tīkliem padarītu sistēmisku un plašu traucējumu sekas īpaši nopietnas. Līdz ar to 5G tīklu kiberdrošības nodrošināšana ir Savienībai stratēģiski svarīgs jautājums laikā, kad kiberuzbrukumi kļūst izplatītāki un izsmalcinātāki nekā jebkad agrāk.

(4) Tā kā infrastruktūra, uz kuras balstās digitālā ekosistēma, savstarpēji savieno daudzas valstis un iespējamie apdraudējumi var šķērsot valstu robežas, jebkura nozīmīga ievainojamība un/vai kiberincidents vienā dalībvalstī ietekmētu visu Savienību kopumā. Tāpēc būtu jāveic darbības, kas nodrošinātu augstu vienotu 5G tīklu kiberdrošības līmeni.

(5) Dalībvalstis ir apstiprinājušas nepieciešamību rīkoties ES līmenī. Kā minēts 2019. gada 21. marta Eiropadomes secinājumos, tā sagaida no Komisijas ieteikumus saskaņotai rīcībai 5G tīklu drošības jomā ([2]).

(6) Pilnībā respektējot tādas Eiropas vērtības kā atvērtība un tolerance, Eiropas suverenitātes nodrošināšanai būtu jābūt vienam no galvenajiem mērķiem ([3]). Ārvalstu investīcijas stratēģiskās nozarēs, kritisku aktīvu, tehnoloģiju un infrastruktūras iegāde Savienībā un kritiski svarīgu iekārtu piegāde arī var radīt risku Savienības drošībai.

(7) Kā atzīts kopīgajā paziņojumā "ES un Ķīna – stratēģiskas perspektīvas", 5G tīklu kiberdrošībai ir izšķiroši svarīga nozīme ES stratēģiskās autonomijas nodrošināšanā ([4]).

(8) Arī Eiropas Parlamenta rezolūcija par drošības apdraudējumiem saistībā ar aizvien lielāko Ķīnas tehnoloģiju klātbūtni ES aicina Komisiju un dalībvalstis rīkoties ES līmenī ([5]).

(9) Šis Ieteikums pievēršas kiberdrošības riskiem 5G tīklos, nosakot vadlīnijas par pienācīgu risku analīzi un vadības pasākumiem valstu līmenī, par koordinēta ES līmeņa riska izvērtējuma izstrādi un par procesa izveidi kopīgai labāko riska pārvaldības pasākumu rīku kopuma izstrādei.

(10) Pastāv spēcīgs ES tiesiskais regulējums elektronisko sakaru tīklu aizsardzībai.

([1]) COM(2016) 588 final.
([2]) 2019. gada 21. un 22. marta Eiropadomes secinājumi.
([3]) 2018. gada runa par stāvokli Savienībā – Eiropas suverenitātes stunda, 2018. gada 12. septembris.
([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//LV

(11) ES noteikumi par elektronisko komunikāciju ([6]) veicina konkurenci, stiprina iekšējo tirgu un aizsargā galalietotāju intereses un ar Eiropas Elektronisko sakaru kodeksu ([7]) tiecas sasniegt papildu savienojamības mērķi, kas izteikts rezultātu veidā: ļoti veiktspējīgu tīklu plaša pieejamība un ieviešana visiem Savienības pilsoņiem un uzņēmumiem, vienlaikus aizsargājot pilsoņu intereses. Direktīvā 2002/21/Ek dalībvalstīm prasīts nodrošināt, lai tiktu uzturēta publisko sakaru tīklu integritāte un drošība, uzliekot saistības panākt, ka uzņēmumi, kas nodrošina publisko sakaru tīklus vai publiski pieejamus elektronisko sakaru pakalpojumus, veic tehniskos un organizatoriskos pasākumus, lai pienācīgi pārvaldītu ar tīklu un pakalpojumu drošību saistītos riskus. Tajā arī noteikts, ka kompetentajām valsts regulatīvajām iestādēm ir pilnvaras nodrošināt šādu pienākumu izpildi, tostarp pilnvaras izdot saistošas instrukcijas.

(12) Turklāt Eiropas Parlamenta un Padomes Direktīva 2002/20/EK ([8]) ļauj dalībvalstīm pievienot vispārējai atļaujai nosacījumus attiecībā uz publisko tīklu drošību pret neatļautu piekļuvi nolūkā aizsargāt saziņas konfidencialitāti saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([9]).

(13) Lai atbalstītu šo saistību izpildi, Savienība ir izveidojusi vairākas sadarbības struktūras. Tīklu un informācijas drošības aģentūra (*ENISA*), Komisija, dalībvalstis un valstu regulatīvās iestādes ir izstrādājušas tehniskās pamatnostādnes valsts regulatīvajām iestādēm par ziņošanu par incidentiem, drošības pasākumiem un draudiem un aktīviem ([10]). Sadarbības grupa, kas izveidota ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/1148 ([11]) ("Sadarbības grupa"), apvieno kompetentās iestādes, lai atbalstītu un veicinātu sadarbību, sevišķi sniedzot stratēģiskus norādījumus datordrošības incidentu reaģēšanas vienību tīkla darbībām, kas tehniskā līmenī veicina operatīvo sadarbību.

(14) Iecerētajam ES kiberdrošības sertifikācijas satvaram ([12]) būtu jānodrošina svarīgs atbalsta instruments drošības līmeņu saskaņotības veicināšanai. Tajā būtu jāparedz iespēja izstrādāt kiberdrošības sertifikācijas sistēmas, lai apmierinātu to lietotāju vajadzības, kas lieto 5G iekārtas un programmatūru. Šīs infrastruktūras ārkārtīgi lielās nozīmes dēļ par tūlītēju prioritāti būtu jānosaka attiecīgo Eiropas kiberdrošības sertifikācijas sistēmu izstrāde attiecībā uz informācijas un sakaru tehnoloģiju produktiem, pakalpojumiem vai procesiem, ko izmanto 5G tīklos. Dalībvalstīm un tirgus dalībniekiem būtu aktīvi jāiesaistās šādu sertifikācijas sistēmu izstrādē, tostarp sniedzot atbalstu 5G tīklu īpašo aizsardzības profilu noteikšanai.

(15) Ja nav saskaņotu Savienības tiesību aktu, dalībvalstis ar valsts tehniskajiem noteikumiem, kas pieņemti saskaņā ar ES tiesību aktiem, var noteikt, ka Eiropas kiberdrošības sertifikācijas sistēmai jābūt obligātai. Dalībvalstis var izmantot Eiropas kiberdrošības sertifikācijas sistēmas arī saistībā ar publisko iepirkumu un Eiropas Parlamenta un Padomes Direktīvu 2014/24/ES ([13]) un varētu atbalstīt palīdzības mehānismu, piemēram, palīdzības punktu, izveidi, lai publiskā sektora pircēji varētu iegādāties kiberdrošības risinājumus.

(16) Augsts datu aizsardzības un privātuma līmenis ir svarīgs elements 5G tīklu drošības nodrošināšanā. Savienības līmenī ir definēti arī noteikumi, kas nodrošina personas datu apstrādes drošību, tostarp elektronisko sakaru jomā. Vispārīgā datu aizsardzības regula ([14]) nosaka pienākumu apstrādāt personas datus tādā veidā, kas garantē to drošību, tostarp novērst nesankcionētu piekļuvi personas datiem un iekārtām, ko izmanto datu apstrādei, un to nesankcionētu izmantošanu. Direktīvā par privātumu un elektronisko komunikāciju paredzēti īpaši noteikumi par

([6]) Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīva 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva) (OV L 108, 24.4.2002., 33. lpp.) un īpašās direktīvas.

([7]) Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīva (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi (OV L 321, 17.12.2018., 36. lpp.).

([8]) Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīva 2002/20/EK par elektronisko komunikāciju tīklu un pakalpojumu atļaušanu (atļauju izsniegšanas direktīva) (OV L 108, 24.4.2002., 21. lpp.).

([9]) Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

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

([11]) Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

([12]) Priekšlikums Eiropas Parlamenta un Padomes regulai par ENISA – ES Kiberdrošības aģentūru – un Regulas (ES) Nr. 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts", COM(2017) 477 final – 2017/0225 (COD)).

([13]) Eiropas Parlamenta un Padomes 2014. gada 26. februāra Direktīva 2014/24/ES par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

([14]) Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

sakaru un galalietotāju galiekārtu konfidencialitātes aizsardzību. Tā arī uzliek pienākumu pakalpojumu sniedzējiem veikt atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu savu pakalpojumu drošību.

(17) Savienība ir pieņēmusi arī instrumentu, kas aizsargās kritisko infrastruktūru un tehnoloģijas, piemēram, tās, kas tiek izmantotas saziņā, ļaujot dalībvalstīm pārbaudīt ārvalstu tiešos ieguldījumus, pamatojoties uz drošības vai sabiedriskās kārtības apsvērumiem, un izveidojot sadarbības mehānismu, kura ietvaros dalībvalstis un Komisija varēs apmainīties ar informāciju un paust bažas par konkrētiem ieguldījumiem ([15]).

(18) Dalībvalstis un operatori pašlaik veic svarīgus sagatavošanās pasākumus, lai veicinātu plaša mēroga 5G tīklu ieviešanu. Vairākas dalībvalstis ir paudušas bažas par iespējamiem drošības riskiem saistībā ar 5G tīkliem attiecībā uz tiem paredzēto radiofrekvenču spektra joslu izmantošanas tiesību piešķiršanas procedūrām ([16]) un ir apsvērušas iespējamos pasākumus šo risku novēršanai.

(19) Nodrošinoties pret kiberdrošības riskiem 5G tīklos, būtu jāņem vērā gan tehniskie, gan citi faktori. Tehniskie faktori var ietvert neaizsargātību kiberdrošības jomā, ko var izmantot, lai iegūtu neatļautu piekļuvi informācijai (kiberspiegošana – ekonomisku vai politisku iemeslu dēļ) vai citā ļaunprātīgā nolūkā (kiberuzbrukumi, kuru mērķis ir traucēt sistēmu un datu pareizu darbību vai tos iznīcināt). Aspektiem, kas jāņem vērā, vajadzētu būt šādiem: nepieciešamība aizsargāt tīklus visā to aprites ciklā un nepieciešamība aptvert visu attiecīgo aprīkojumu, tostarp 5G tīklu projektēšanas, izstrādes, iepirkuma, uzstādīšanas, ekspluatācijas un apkopes posmus.

(20) Citi faktori var ietvert regulatīvas vai citas prasības, ko piemēro informācijas un sakaru tehnoloģiju iekārtu piegādātājiem. Šo faktoru nozīmes novērtējumā cita starpā būtu jāņem vērā trešās valsts kopējās ietekmes risks, jo īpaši attiecībā uz tās pārvaldības modeli, sadarbības nolīgumu par drošību vai līdzīgu pasākumu attiecībā uz datu aizsardzību, piemēram, lēmumu par aizsardzības līmeņa pietiekamību, neesamība starp Savienību un attiecīgo trešo valsti, kā arī tas, vai šī valsts ir noslēgusi daudzpusējus, starptautiskus vai divpusējus nolīgumus par kiberdrošību, cīņu pret kibernoziedzību vai datu aizsardzību.

(21) Lai izstrādātu Savienības pieeju 5G tīklu kiberdrošībai, valstu līmenī būtu svarīgi veikt un pabeigt riska novērtējumu. Tas palīdzētu dalībvalstīm pielāgot valsts pasākumus attiecībā uz drošības prasībām un riska pārvaldību, ņemot vērā šo novērtējumu.

(22) Būtu jāattīsta koordinācija, lai nodrošinātu to pasākumu efektivitāti, kuru mērķis ir novērst šos kiberdrošības apdraudējumus un kas ir būtiski iekšējā tirgus netraucētai darbībai un personas datu un privātās dzīves aizsardzībai.

(23) Valstu riska novērtējumiem vajadzētu kļūt par pamatu saskaņotam Savienības riska novērtējumam, ko veidotu drošības apdraudējumu apraksts un kopīga pārskatīšana, kas dalībvalstīm jāveic ar Komisijas atbalstu un kopīgi ar Eiropas Kiberdrošības aģentūru (*ENISA*).

(24) Ņemot vērā valstu un Savienības riska novērtējumus, Sadarbības grupai būtu jāizveido instrumentu kopums, kas noteiktu kiberdrošības riska veidus un iespējamos pasākumus risku mazināšanai tādās jomās kā sertifikācija, testēšana un piekļuves kontrole. Tajā būtu arī jānosaka iespējamie konkrētie pasākumi, ko var veikt, lai novērstu vienas vai vairāku dalībvalstu identificētos riskus. Sadarbības grupai būtu jāvēršas pēc atbalsta pie Eiropas Kiberdrošības aģentūras (*ENISA*), Eiropola, Eiropas Elektronisko komunikāciju regulatoru iestādes (*BEREC*) un ES Izlūkošanas un situāciju centra. Šim instrumentu kopumam būtu jāpalīdz Komisijai izstrādāt obligātās vispārējās prasības, lai nodrošinātu vēl augstāku 5G tīklu kiberdrošības līmeni visā Savienībā.

(25) Lai novērstu kiberdrošības riskus, veidojot katru atsevišķo tīklu, būtu jāapsver kiberdrošības veicināšana, izmantojot dažādus piegādātājus.

([15]) Eiropas Parlamenta un Padomes 2019. gada 19. marta Regula (ES) 2019/452, ar ko izveido regulējumu ārvalstu tiešo ieguldījumu Savienībā izvērtēšanai (OV L 79I, 21.3.2019., 1. lpp.).

([16]) 2019. gadā ir paredzēta izsoles procedūra vismaz vienā spektra joslā 11 dalībvalstīs: Austrijā, Beļģijā, Čehijas Republikā, Francijā, Grieķijā, Īrijā, Nīderlandē, Lietuvā, Portugālē, Ungārijā, Vācijā. Vēl sešas izsoles ir paredzētas 2020. gadā: Apvienotajā Karalistē, Lietuvā (dažādas frekvences), Maltā, Slovākijā, Spānijā, Polijā. Avots: http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) Šim Ieteikumam nebūtu jāskar dalībvalstu kompetence attiecībā uz darbībām, kas saistītas ar sabiedrības drošību, aizsardzību, valsts drošību un valsts darbībām krimināltiesību jomā, tostarp dalībvalstu tiesības valsts drošības apsvērumu dēļ neielaist pakalpojumu sniedzējus vai piegādātājus savos tirgos,

IR PIEŅĒMUSI ŠO IETEIKUMU.

I. **MĒRĶI**

1. Lai atbalstītu Eiropas Savienības mēroga pieejas izstrādi 5G tīklu kiberdrošības nodrošināšanai, šajā ieteikumā ir noteikti pasākumi, kas jāveic, lai:

   a) dalībvalstis varētu novērtēt kiberdrošības riskus, kas ietekmē 5G tīklus valsts līmenī, un veikt nepieciešamos drošības pasākumus;

   b) dalībvalstis un attiecīgās Savienības iestādes, aģentūras un citas struktūras varētu kopīgi izstrādāt koordinētu Savienības riska novērtējumu, kura pamatā ir valstu riska novērtējums;

   c) Sadarbības grupa, kas izveidota saskaņā ar Direktīvu (ES) 2016/1148 (Sadarbības grupa), varētu noteikt kopīgu pasākumu kopumu, kas jāveic, lai mazinātu kiberdrošības riskus saistībā ar infrastruktūru, kura ir digitālās ekosistēmas pamatā, it īpaši 5G tīkliem.

II. **DEFINĪCIJAS**

2. Šajā ieteikumā:

   a) "5G tīkli" nozīmē visu attiecīgo tīkla infrastruktūras elementu kopumu mobilo un bezvadu sakaru tehnoloģijai, ko izmanto savienojamības un pievienotās vērtības pakalpojumiem, ar uzlabotiem veiktspējas parametriem, piemēram, ļoti lielu datu pārraides ātrumu un jaudu, zema latentuma sakariem, ārkārtīgi augstu uzticamību vai atbalstu lielam skaitam savienotu ierīču. Tie var ietvert vēsturiskos tīkla elementus, kuru pamatā ir iepriekšējās paaudzes mobilo un bezvadu sakaru tehnoloģija, piemēram, 4G vai 3G. Ar 5G tīkliem būtu jāsaprot visas atbilstošās tīkla daļas;

   b) "Digitālās ekosistēmas pamatā esošās infrastruktūra" ir infrastruktūra, ko izmanto, lai digitalizētu plašu kritiski svarīgu lietojumu klāstu ekonomikā un sabiedrībā.

III. **RĪCĪBA VALSTU LĪMENĪ**

3. Līdz 2019. gada 30. jūnijam dalībvalstīm būtu jāveic 5G tīkla infrastruktūras riska novērtējums, tostarp identificējot sensitīvākos elementus, kuru drošības pārkāpumiem būtu ievērojama negatīva ietekme. Tādā pašā termiņā dalībvalstīm būtu arī jāpārskata valsts līmenī piemērotās drošības prasības un riska pārvaldības metodes, tā lai tiktu ņemti vērā kiberdrošības apdraudējumi, kas var izrietēt no i) tehniskajiem faktoriem, piemēram, 5G tīklu specifiskajām tehniskajām īpašībām, un ii) citiem faktoriem, piemēram, tiesiskā un politiskā satvara, kas var attiekties uz informācijas un sakaru tehnoloģiju aprīkojuma piegādātājiem trešās valstīs.

4. Pamatojoties uz šo valsts riska novērtējumu un pārskatīšanu un ņemot vērā pašreizējo koordinēto rīcību Savienības līmenī, dalībvalstīm vajadzētu:

   a) atjaunināt 5G tīkliem piemērojamās drošības prasības un riska pārvaldības metodes;

   b) papildināt attiecīgos pienākumus uzņēmumiem, kuri nodrošina publisko komunikāciju tīklus vai sniedz publiski pieejamus elektronisko komunikāciju pakalpojumus saskaņā ar Direktīvas 2002/21/EK 13.a un 13.b pantu;

   c) pievienot vispārējai atļaujai nosacījumus attiecībā uz publisko tīklu drošību pret neatļautu piekļuvi un pieprasīt no uzņēmumiem, kas piedalās turpmākajās iepirkuma procedūrās radiofrekvenču izmantošanas tiesību piešķiršanai 5G joslās, uzņemties saistības attiecībā uz tīklu drošības prasību ievērošanu saskaņā ar Direktīvu 2002/20/EK;

   d) piemērot citus preventīvus pasākumus, kuru mērķis ir mazināt iespējamos kiberdrošības riskus.

5. 4. punktā minētajos pasākumos būtu jākļauj stingrākas prasības piegādātājiem un operatoriem nodrošināt tīklu sensitīvo daļu drošību, kā arī vajadzības gadījumā saistības, piemēram, sniegt kompetentajām valsts iestādēm attiecīgu informāciju par plānotajām izmaiņām elektronisko sakaru tīklos, un prasība, ka konkrēti informācijas tehnoloģiju komponenti un sistēmas drošības un integritātes vārdā iepriekš ir jāpārbauda valsts audita/sertifikācijas laboratorijās.

6. Divām vai vairāk dalībvalstīm, izmantojot un apmainoties ar attiecīgajām tehniskām zināšanām un iekārtām, būtu jāveic kopīgas drošības pārbaudes attiecībā uz infrastruktūru, kura ir digitālo ekosistēmu un 5G tīklu pamatā, piemēram, ja viens un tas pats uzņēmums darbojas vai veido tīkla infrastruktūru vairāk nekā vienā dalībvalstī, vai ja tīkla konfigurācijas ir ļoti līdzīgas. Eiropas Kiberdrošības aģentūrai (*ENISA*), Eiropolam un Eiropas Elektronisko komunikāciju regulatoru iestādei (*BEREC*) būtu jāpiešķir prioritāte dalībvalstu atbalsta pieprasījumiem šajā jomā. Šo pārskatu rezultāti būtu jānosūta Sadarbības grupai un Datordrošības incidentu reaģēšanas vienības tīklam.

IV. **KOORDINĒTA RĪCĪBA SAVIENĪBAS LĪMENĪ**

7. Lai izstrādātu kopēju pieeju kiberdrošības risku novēršanai attiecībā uz 5G tīkliem, dalībvalstīm līdz 2019. gada 30. aprīlim būtu jāsāk darboties īpašā darba plūsmā Sadarbības grupā. Dalībvalstīm būtu jāuzaicina attiecīgās iestādes vajadzības gadījumā piedalīties Sadarbības grupas darbā.

Koordinēts Eiropas riska novērtējums

8. Dalībvalstīm būtu jāapmainās ar informāciju savā starpā un ar attiecīgām Savienības struktūrām, lai veidotu kopīgu izpratni par esošajiem un potenciālajiem kiberdrošības riskiem, kas saistīti ar 5G tīkliem.

9. Dalībvalstīm savi riska novērtējumi būtu jānosūta Komisijai un Eiropas Kiberdrošības aģentūrai (*ENISA*) līdz 2019. gada 15. jūlijam.

10. Eiropas Kiberdrošības aģentūrai (*ENISA*) būtu jāizstrādā īpašs 5G tīklu drošības apdraudējumu apraksts. Šis process būtu jāatbalsta Sadarbības grupai un Datordrošības incidentu reaģēšanas vienību tīklam, kas izveidots saskaņā ar Direktīvu (ES) 2016/1148.

11. Ņemot vērā visus šos elementus, dalībvalstīm ar Komisijas atbalstu un kopā ar Eiropas Kiberdrošības aģentūru (*ENISA*) līdz 2019. gada 1. oktobrim būtu jāsagatavo kopīgs pārskats par Savienības mēroga pakļautību riskiem, kas saistīti ar infrastruktūru, kura ir digitālās ekosistēmas pamatā, sevišķi 5G tīkliem.

12. Šajā kopīgajā pārskatā par prioritāti būtu jānosaka riska analīze attiecībā uz īpaši sensitīviem vai neaizsargātiem elementiem, kuri iekļauti 5G tīklu pamatelementos, uz operatīvo un tehniskās apkopes centru, kā arī attiecībā uz 5G piekļuves tīkla elementiem, ko izmanto rūpnieciskiem mērķiem.

13. Šā kopīgā pārskata otrajā posmā būtu jāiekļauj arī citi digitālās vērtības ķēdes stratēģiskie elementi.

Kopīgs Savienības instrumentu kopums risku novēršanai

14. Sadarbības grupai būtu jānosaka 4. punktā paredzēto pasākumu paraugprakse valsts līmenī. Pamatojoties uz šo valstu paraugpraksi, līdz 2019. gada 31. decembrim būtu jāvienojas par piemērotu, efektīvu un samērīgu iespējamo riska pārvaldības instrumentu kopumu identificēto kiberdrošības risku mazināšanai valstu un Savienības līmenī, lai iesniegtu Komisijai kopējas obligātās prasības ar mērķi turpmāk nodrošināt 5G tīklu augstu kiberdrošības līmeni visā Savienībā.

15. Šajā instrumentu kopumā būtu jāiekļauj:

   a) to drošības risku veidu uzskaitījums, kas var ietekmēt 5G tīklu kiberdrošību (piemēram, piegādes ķēdes risks, programmatūras ievainojamības risks, piekļuves kontroles risks, riski, kas izriet no tiesiskās un politikas sistēmas, kurai ir pakļauti informācijas un sakaru tehnoloģiju aprīkojuma piegādātāji trešās valstīs); kā arī

   b) iespējamo ietekmes mazināšanas pasākumu kopums (piemēram, trešās personas veikta aparatūras, programmatūras vai pakalpojumu sertifikācija, oficiāli aparatūras un programmatūras testi vai atbilstības pārbaudes, procesi, kas ļauj pārliecināties, ka piekļuves kontrole ir ieviesta un darbojas, identificējot produktus, pakalpojumus vai piegādātājus, kas potenciāli uzskatāmi par nedrošiem, utt.). Šie pasākumi būtu jāpiemēro katram drošības riska veidam, kas konstatēts vienā vai vairākās dalībvalstīs pēc riska novērtējuma.

16. Kad Eiropas kiberdrošības sertifikācijas sistēmas, kas attiecas uz 5G tīkliem, būs izstrādātas, dalībvalstīm saskaņā ar Savienības tiesību aktiem būtu jāpieņem valsts tehniskie noteikumi, kas paredz obligātu sertifikāciju informācijas un sakaru tehnoloģiju produktiem, pakalpojumiem vai sistēmām, uz kurām attiecas šādas sistēmas.

17. Dalībvalstīm kopā ar Komisiju būtu jāidentificē nosacījumi attiecībā uz publisko tīklu drošību pret neatļautu piekļuvi, kuri jāpievieno vispārējai atļaujai, un jāpieprasa no uzņēmumiem, kas piedalās turpmākajās iepirkuma procedūrās radiofrekvenču izmantošanas tiesību piešķiršanai 5G joslās, uzņemties saistības attiecībā uz tīklu drošības prasību ievērošanu saskaņā ar Direktīvu 2002/20/EK. Tās būtu iespēju robežās jāatspoguļo 4. punkta c) apakšpunktā minētajos pasākumos.

18. Dalībvalstīm būtu jāsadarbojas ar Komisiju, lai izstrādātu konkrētas drošības prasības, ko piemērot publisko iepirkumu procesā saistībā ar 5G tīkliem. Tām būtu jāietver obligātas prasības par kiberdrošības sertifikācijas sistēmu ieviešanu publiskajā iepirkumā, ciktāl šādas sistēmas vēl nav saistošas visiem piegādātājiem un operatoriem.

V. **PĀRSKATĪŠANA**

19. Dalībvalstīm būtu jāsadarbojas ar Komisiju, lai novērtētu šā Ieteikuma ietekmi līdz 2020. gada 1. oktobrim ar mērķi noteikt piemērotus turpmākos pasākumus. Šajā novērtējumā būtu jāņem vērā koordinētā Savienības riska novērtējuma un Savienības instrumentu kopuma rezultāti.

Strasbūrā, 2019. gada 26. martā

Komisijas vārdā –
Komisijas loceklis
Julian KING