PREPORUKE

PREPORUKA KOMISIJE (EU) 2019/534

od 26. ožujka 2019.

Kibersigurnost 5G mreža

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 292.,

budući da:

(1) Komisija je prepoznala važnost upotrebe mrežnih tehnologija pete generacije (5G) za razvoj budućih digitalnih usluga i strategiju jedinstvenog digitalnog tržišta. Komisija je donijela akcijski plan za 5G tehnologije kako bi Uniji osigurala infrastrukturu za povezivost koja joj je potrebna za digitalnu transformaciju od 2020. ([1])

(2) 5G mreže temeljit će se na postojećoj četvrtoj generaciji (4G) mrežnih tehnologija, omogućiti nove kapacitete usluga i postati središnja infrastruktura i pokretač velikog dijela gospodarstva Unije. Nakon uvođenja 5G mreže činit će okosnicu širokog raspona usluga bitnih za funkcioniranje unutarnjeg tržišta te za održavanje i rad ključnih socijalnih i gospodarskih funkcija, kao što su energija, prijevoz, bankarstvo i zdravstvo, te industrijskih kontrolnih sustava. U organizaciji demokratskih postupaka, kao što su izbori, također će se sve više oslanjati na digitalnu infrastrukturu i 5G mreže.

(3) Budući da ključne usluge ovise o 5G mrežama, sistemski i širi poremećaji mogli bi imati posebno ozbiljne posljedice. Stoga je od strateške važnosti za Uniju osigurati kibersigurnost 5G mreža, u vremenu u kojem se povećava broj kibernapada i njihova složenost.

(4) Zbog povezanosti i transnacionalnosti infrastrukture na kojoj se temelji digitalni ekosustav te prekogranične naravi povezanih prijetnji, sve veće slabosti i/ili kibersigurnosni incidenti povezani s 5G mrežama u jednoj državi članici utjecali bi na Uniju u cjelini. Zato bi trebalo donijeti mjere kojima će se poduprijeti visoka zajednička razina kibersigurnosti 5G mreža.

(5) Države članice potvrdile su da je potrebno djelovati na razini Unije. U zaključcima Europskog vijeća od 21. ožujka 2019. Komisija se poziva da donese preporuku o usklađenom pristupu sigurnosti 5G mreža ([2]).

(6) Jedan od glavnih ciljeva trebalo bi biti osiguranje europskog suvereniteta, uz poštovanje europskih vrijednosti otvorenosti i tolerancije ([3]). Ulaganja stranih subjekata u strateške sektore, njihovo stjecanje ključne imovine, tehnologije i infrastrukture u Uniji i dobava ključne opreme također mogu predstavljati rizik za sigurnost Unije.

(7) Prema Zajedničkoj komunikaciji „EU i Kina – strateški pregled” ([4]) kibersigurnost 5G mreža ključna je za osiguravanje strateške autonomije Unije.

(8) U rezoluciji Europskog parlamenta o sigurnosnim prijetnjama povezanima sa sve većom tehnološkom prisutnošću Kine također se poziva Komisiju i države članice da djeluju na razini Unije ([5]).

(9) U toj se preporuci utvrđuju smjernice za suzbijanje kibersigurnosnih rizika u 5G mrežama putem odgovarajućih analiza rizika i mjera upravljanja rizikom na nacionalnoj razini, izrade usklađene europske procjene rizika te uspostave postupka za izradu zajedničkog skupa najboljih mjera za upravljanje rizikom.

(10) Na snazi je jak zakonodavni okvir Unije o zaštiti elektroničkih komunikacijskih mreža.

([1]) COM(2016) 588 final.
([2]) Zaključci Europskog vijeća od 21. i 22. ožujka 2019.
([3]) Stanje Unije 2018. – Vrijeme za europski suverenitet, 12. rujna 2018.
([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//EN

(11) Okvirom Unije u području elektroničkih komunikacija ([6]) promiču se tržišno natjecanje, unutarnje tržište i interesi krajnjih korisnika, a Europskim zakonikom elektroničkih komunikacija ([7]) nastoji se ostvariti dodatni cilj povezivosti, izražen u obliku sljedećeg rezultata: opća dostupnost i primjena fiksne i pokretne povezivosti vrlo visokog kapaciteta za sve građane i poduzeća u Uniji, uz zaštitu interesa građana. Direktivom 2002/21/EZ od država članica zahtijeva se da očuvaju integritet i sigurnost javnih komunikacijskih mreža te da osiguraju da poduzeća koja pružaju javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge poduzmu tehničke i organizacijske mjere kako bi na odgovarajući način upravljala rizicima za sigurnost mreža i usluga. Njome je predviđeno i da nadležna državna regulatorna tijela imaju ovlasti za osiguranje usklađenosti s tim obvezama, uključujući ovlast objave obvezujućih uputa.

(12) Osim toga, Direktivom 2002/20/EZ Europskog parlamenta i Vijeća ([8]) državama članicama omogućuje se da općem ovlaštenju dodaju uvjete koji se odnose na zaštitu javnih mreža od neovlaštenog pristupa kako bi se zaštitila povjerljivost komunikacije u skladu s Direktivom 2002/58/EZ Europskog parlamenta i Vijeća ([9]).

(13) Kako bi podržala provedbu tih obveza, Unija je osnovala niz tijela za suradnju. Agencija za mrežnu i informacijsku sigurnost (ENISA), Komisija, države članice i državna regulatorna tijela izradili su za državna regulatorna tijela tehničke smjernice o izvješćivanju o incidentima, sigurnosnim mjerama te prijetnjama i sredstvima ([10]). Skupina za suradnju osnovana Direktivom (EU) 2016/1148 Europskog parlamenta i Vijeća ([11]) („skupina za suradnju") okuplja nadležna tijela kako bi potaknula i olakšala suradnju, posebno pružanjem strateških smjernica za aktivnosti timova za odgovor na računalne sigurnosne incidente, čime se olakšava operativna suradnja na tehničkoj razini.

(14) Budući europski okvir o kibersigurnosnoj certifikaciji ([12]) trebao bi biti ključno pomoćno sredstvo za promicanje dosljednih razina sigurnosti. Taj bi okvir trebao omogućiti uspostavu programa kibersigurnosne certifikacije kojima će se zadovoljiti potrebe korisnika opreme i softvera za 5G. Zbog velike važnosti te infrastrukture, trebalo bi hitno uspostaviti relevantne europske programe kibersigurnosne certifikacije za proizvode, usluge ili procese informacijske i komunikacijske tehnologije koji se upotrebljavaju za 5G mreže. Države članice i sudionici na tržištu trebali bi aktivno sudjelovati u uspostavi takvih programa certifikacije, među ostalim pružanjem potpore u definiranju specifičnih profila zaštite za 5G mreže.

(15) U nedostatku usklađenog zakonodavstva Unije, države članice mogu nacionalnim tehničkim propisima donesenima u skladu s pravom Unije odrediti da bi europski program kibersigurnosne certifikacije trebao biti obvezan. Države članice mogu primijeniti europske programe kibersigurnosne certifikacije i u kontekstu javne nabave i Direktive 2014/24/EU Europskog parlamenta i Vijeća ([13]) te bi mogle pružiti potporu uspostavi pomoćnih mehanizama, npr. centra za pomoć, za javne kupce kibersigurnosnih rješenja.

(16) Visoka razina zaštite podataka i privatnosti važan je element sigurnosti 5G mreža. Na razini Unije također su definirana pravila kojima se osigurava sigurnost obrade osobnih podataka, među ostalim u elektroničkoj komunikaciji. Općom uredbom o zaštiti podataka ([14]) utvrđuje se obveza obrade osobnih podataka na siguran način, među ostalim, sprečavanjem neovlaštenog pristupa ili upotrebe osobnih podataka i opreme koja se

([6]) Direktiva 2002/21/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva) (SL L 108, 24.4.2002., str. 33.) i posebne direktive.

([7]) Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (SL L 321, 17.12.2018., str. 36.).

([8]) Direktiva 2002/20/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o ovlaštenju u području elektroničkih komunikacijskih mreža i usluga (Direktiva o ovlaštenju), SL L 108, 24.4.2002., str. 21.

([9]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

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

([11]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

([12]) Prijedlog uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) br. 526/2013 te o sigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti") (COM(2017) 477 final – 2017/0225(COD)).

([13]) Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

([14]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

upotrebljava za obradu. Direktivom o privatnosti u elektroničkoj komunikaciji utvrđuju se posebna pravila o zaštiti povjerljivosti komunikacije i terminalne opreme krajnjih korisnika. Na temelju te direktive pružatelji usluga dužni su poduzeti odgovarajuće tehničke i organizacijske mjere za zaštitu sigurnosti svojih usluga.

(17) Unija je donijela i instrument kojim će se zaštititi ključna infrastruktura i tehnologije, npr. one koje se upotrebljavaju za komunikaciju, tako što će državama članicama omogućiti da provjeravaju izravna strana ulaganja radi sigurnosti ili održavanja javnog reda te da uspostave mehanizam suradnje u okviru kojeg će države članice i Komisija moći razmjenjivati informacije i izražavati dvojbe u pogledu određenih ulaganja ([15]).

(18) Države članice i subjekti trenutačno poduzimaju važne pripremne korake kako bi se omogućilo opsežno uvođenje 5G mreža. Više je država članica izrazilo zabrinutost u pogledu potencijalnih sigurnosnih rizika povezanih s 5G mrežama u kontekstu provođenja postupaka za dodjelu prava na korištenje radiofrekvencijskih spektara namijenjenih za 5G mreže ([16]) i razmatraju mjere kojima bi te rizike uklonile.

(19) Pri uklanjaju kibersigurnosnih rizika u 5G mrežama trebalo bi uzimati u obzir tehničke i druge čimbenike. Tehnički čimbenici mogu uključivati kibersigurnosne slabosti koje se mogu iskoristiti za dobivanje neovlaštenog pristupa informacijama (kiberšpijunaža, iz ekonomskih ili političkih razloga) ili za drugu zlonamjernu svrhu (kibernapadi u cilju ometanja ili uništavanja sustava i podataka). Važno je razmotriti aspekte kao što su potreba za zaštitom mreža tijekom cijelog životnog ciklusa te potreba za obuhvaćanjem sve relevantne opreme, uključujući onu koja se koristi u fazi dizajna, izrade, nabave, upotrebe, rada i održavanja 5G mreža.

(20) Drugi čimbenici mogu uključivati regulatorne ili druge zahtjeve za dobavljače opreme za informacijske i komunikacijske tehnologije. Pri procjeni važnosti takvih čimbenika trebalo bi među ostalim uzeti u obzir ukupan rizik utjecaja treće zemlje, posebno kad je riječ o njezinu modelu upravljanja, postoji li sporazum o suradnji ili sličan dogovor, kao što su odluke o primjerenosti, u području zaštite podataka između Unije i dotične treće zemlje ili je li ta zemlja stranka multilateralnih, međunarodnih ili bilateralnih sporazuma o kibersigurnosti, borbi protiv kiberkriminaliteta ili zaštiti podataka.

(21) Kao važan korak u razvoju Unijina pristupa kibersigurnosti 5G mreža, trebalo bi provesti i dovršiti procjenu rizika na nacionalnoj razini. Time bi se državama članicama pomoglo da s obzirom na tu procjenu prilagode nacionalne mjere o sigurnosnim zahtjevima i upravljanju rizicima.

(22) Trebalo bi provesti usklađivanje kako bi se osigurala učinkovitost mjera usmjerenih na uklanjanje prijetnji kibersigurnosti jer su te mjere ključne za neometano funkcioniranje unutarnjeg tržišta i zaštitu osobnih podataka i privatnosti.

(23) Procjene rizika na nacionalnoj razini trebale bi biti osnova za usklađenu procjenu rizika na razini Unije koja će obuhvaćati pregled prijetnji i zajedničko preispitivanje koje uz potporu Komisije i zajedno s Europskom agencijom za kibersigurnost (ENISA) trebaju provesti države članice.

(24) Na temelju procjena rizika na razini Unije i na nacionalnoj razini skupina za suradnju trebala bi izraditi skup alata za utvrđivanje vrsta rizika u području kibersigurnosti i mogućih mjera za smanjenje rizika u područjima kao što su certifikacija, testiranje i kontrola pristupa. Trebala bi utvrditi i moguće posebne mjere prikladne za uklanjanje rizika koje utvrdi jedna ili više država članica. Skupina za suradnju trebala bi se oslanjati na potporu Europske agencije za kibersigurnost (ENISA), Europola, Tijela europskih regulatora za elektroničke komunikacije (BEREC) te Obavještajnog i situacijskog centra EU-a. Komisija bi s pomoću tog skupa alata trebala utvrditi minimalne zajedničke zahtjeve za daljnje osiguravanje visoke razine kibersigurnosti 5G mreža u cijeloj Uniji.

(25) Pri poduzimanju mjera za uklanjanje kibersigurnosnih rizika trebalo bi uzeti u obzir da se kibersigurnost može promicati tako da se za izgradnju svake jedinstvene mreže osigura raznolik izbor dobavljača.

([15]) Uredba (EU) 2019/452 Europskog parlamenta i Vijeća od 19. ožujka 2019. o uspostavi okvira za provjeru izravnih stranih ulaganja u Uniji (SL L 79I, 21.3.2019., str. 1.).

([16]) U 2019. se planira provesti postupak aukcije za najmanje jedan pojas u 11 država članica: Austriji, Belgiji, Češkoj, Francuskoj, Njemačkoj, Grčkoj, Mađarskoj, Irskoj, Nizozemskoj, Litvi i Portugalu. Još šest aukcija predviđeno je za 2020.: u Španjolskoj, Malti, Litvi (različite frekvencije), Slovačkoj, Poljskoj i Ujedinjenoj Kraljevini. *Izvor*: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Ovom se Preporukom ne bi trebale dovoditi u pitanje nadležnosti država članica za aktivnosti koje se odnose na javnu sigurnost, obranu, nacionalnu sigurnost i djelovanje države u području kaznenog prava, uključujući pravo država članica da iz razloga nacionalne sigurnosti isključe pružatelje ili dobavljače sa svojih tržišta,

DONIJELA JE OVU PREPORUKU:

I. **CILJEVI**

1. U cilju podržavanja razvoja Unijina pristupa kibersigurnosti 5G mreža, ovom se Preporukom utvrđuju relevantne mjere koje bi trebalo poduzeti kako bi:

   (a) države članice mogle na nacionalnoj razini procjenjivati kibersigurnosne rizike koji utječu na 5G mreže i poduzimati potrebne sigurnosne mjere;

   (b) na temelju nacionalne procjene rizika države članice i relevantne institucije, agencije i druga tijela Unije zajednički mogli provesti usklađenu procjenu rizika na razini Unije;

   (c) skupina za suradnju osnovana na temelju Direktive (EU) 2016/1148 („skupina za suradnju”) mogla utvrditi zajednički skup mjera koje treba poduzeti radi smanjenja kibersigurnosnih rizika povezanih s infrastrukturom na kojoj se temelji digitalni ekosustav, posebno 5G mreže.

II. **DEFINICIJE**

2. Za potrebe ove Preporuke:

   (a) „5G mreže” znači skup svih relevantnih elemenata mrežne infrastrukture za mobilne i bežične komunikacijske tehnologije koji se upotrebljavaju za povezivanje i usluge s dodanom vrijednošću s naprednim karakteristikama, primjerice velike brzine prijenosa podataka i veliki podatkovni kapaciteti, komunikacije niske latencije, iznimno visoka pouzdanost ili mogućnost povezivanja velikog broja uređaja. Oni mogu uključivati postojeće mrežne elemente koji se temelje na prethodnim generacijama mobilnih i bežičnih komunikacijskih tehnologija, kao što su 4G ili 3G. Trebalo bi smatrati da 5G mreže uključuju sve relevantne dijelove mreže;

   (b) „infrastruktura na kojoj se temelji digitalni ekosustav” znači infrastruktura koja se upotrebljava za digitalizaciju u širokom rasponu ključnih primjena u gospodarstvu i društvu.

III. **DJELOVANJE NA NACIONALNOJ RAZINI**

3. Države članice trebale bi do 30. lipnja 2019. provesti procjenu rizika infrastrukture 5G mreža, među ostalim utvrditi najosjetljivije elemente u kojima bi povrede sigurnosti imale znatan negativan učinak. Do tog bi datuma države članice trebale preispitati i sigurnosne zahtjeve i metode upravljanja rizicima primjenjive na nacionalnoj razini, kako bi uzele u obzir prijetnje kibersigurnosti koje mogu proizaći iz i. tehničkih čimbenika, primjerice posebnih tehničkih karakteristika 5G mreža i ii. drugih čimbenika, primjerice pravnog i političkog okvira koji se može primjenjivati u trećim zemljama na dobavljače opreme za informacijske i komunikacijske tehnologije.

4. Na temelju te procjene rizika i preispitivanja na nacionalnoj razini te uzimajući u obzir trajni postupak usklađivanja na razini Unije, države članice trebale bi:

   (a) ažurirati sigurnosne zahtjeve i metode upravljanja rizicima koji se primjenjuju na 5G mreže;

   (b) ažurirati relevantne obveze za poduzeća koja pružaju javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge u skladu s člancima 13.a i 13.b Direktive 2002/21/EZ;

   (c) općem ovlaštenju dodati uvjete koji se odnose na zaštitu javnih mreža od neovlaštenog pristupa i od poduzeća koja sudjeluju u novim postupcima za dodjelu prava na korištenje radijskih frekvencija u 5G pojasevima zatražiti da preuzmu obvezu usklađivanja sa sigurnosnim zahtjevima za mreže u skladu s Direktivom 2002/20/EZ.

   (d) provesti druge preventivne mjere usmjerene na smanjenje potencijalnih kibersigurnosnih rizika;

5. Mjere iz točke 4. trebale bi obuhvaćati pojačane obveze za dobavljače i operatere kako bi se zajamčila sigurnost osjetljivih dijelova mreža i, prema potrebi, obveze kao što je dostavljanje relevantnih informacija nadležnim nacionalnim tijelima o planiranim promjenama u elektroničkim komunikacijskim mrežama te zahtjeve da nacionalni laboratoriji za reviziju/certifikaciju unaprijed testiraju sigurnost i integritet posebnih komponenti i sustava informacijske tehnologije.

6. Zajednička preispitivanja sigurnosti trebale bi provesti dvije države članice ili više njih, uz upotrebu i razmjenu odgovarajućeg tehničkog znanja i objekata koji se odnose na infrastrukturu na kojoj se temelji digitalni ekosustav i 5G mreže, primjerice, ako isto poduzeće gradi mrežnu infrastrukturu ili upravlja njome u više država članica ili ako postoje velike sličnosti u konfiguracijama mreže. Europska agencija za kibersigurnost (ENISA), Europol i Tijelo europskih regulatora za elektroničke komunikacije (BEREC) trebali bi dati prednost zahtjevima za potporu država članica u tom području. Rezultate tih preispitivanja trebalo bi proslijediti skupini za suradnju i mreži timova za odgovor na računalne sigurnosne incidente.

IV. **USKLAĐENO DJELOVANJE NA RAZINI UNIJE**

7. Države članice trebale bi do 30. travnja 2019. početi primjenjivati poseban radni postupak u okviru skupine za suradnju kako bi se osmislio zajednički pristup uklanjanju kibersigurnosnih rizika za 5G mreže. Države članice trebale bi, prema potrebi, pozvati nadležna tijela na sudjelovanje u skupini za suradnju.

Usklađena procjena rizika na europskoj razini

8. Države članice trebale bi razmjenjivati informacije međusobno i s nadležnim tijelima Unije radi jačanja zajedničke svijesti o postojećim i potencijalnim kibersigurnosnim rizicima povezanima s 5G mrežama.

9. Države članice trebale bi Komisiji i Europskoj agenciji za kibersigurnost (ENISA) dostaviti nacionalne procjene rizika do 15. srpnja 2019.

10. Europska agencija za kibersigurnost (ENISA) trebala bi dovršiti poseban pregled prijetnji za 5G mreže. Taj bi postupak trebale poduprijeti skupina za suradnju i mreža timova za odgovor na računalne sigurnosne incidente osnovane Direktivom (EU) 2016/1148.

11. Uzimajući u obzir sve navedene elemente, države članice trebale bi u suradnji s Europskom agencijom za kibersigurnost (ENISA) te uz potporu Komisije do 1. listopada 2019. zajednički preispitati izloženost Unije rizicima koji se odnose na infrastrukturu na kojoj se temelji digitalni ekosustav, posebno 5G mreže.

12. U tom zajedničkom preispitivanju prioritet bi trebala biti analiza rizika koji se odnose na posebno osjetljive dijelove ključnih elemenata 5G mreža, na operacije i centar za održavanje te na elemente za pristup 5G mreži za industrijske primjene.

13. U drugoj bi fazi to zajedničko preispitivanje trebalo proširiti na ostale strateške dijelove digitalnog vrijednosnog lanca.

Zajednički skup mjera Unije za uklanjanje rizika

14. Skupina za suradnju trebala bi utvrditi mjere najbolje prakse na nacionalnoj razini u skladu s točkom 4. Na temelju utvrđenih najboljih nacionalnih praksi trebalo bi do 31. prosinca 2019. dogovoriti skup mogućih odgovarajućih, učinkovitih i razmjernih mjera za smanjenje rizika kibersigurnosti utvrđenih na nacionalnoj razini i razini Unije, s pomoću kojeg će Komisija izraditi minimalne zajedničke zahtjeve za daljnje osiguravanje visoke razine kibersigurnosti 5G mreža u cijeloj Uniji.

15. Taj bi skup mjera trebao uključivati:

(a) popis vrsta sigurnosnih rizika koji mogu utjecati na kibersigurnost 5G mreža (npr. rizici povezani s lancima opskrbe, osjetljivošću softvera, kontrolom pristupa, rizici koji proizlaze iz pravnog i političkog okvira koji se može primjenjivati u trećim zemljama na dobavljače opreme za informacijske i komunikacijske tehnologije); i

(b) skup mogućih mjera za smanjenje rizika (npr. certifikacija hardvera, softvera ili usluga koje provodi treća strana, službena testiranja hardvera i softvera ili provjere sukladnosti, postupci za provjeru postojanja i provedbe kontrola pristupa, identificiranje potencijalno nesigurnih proizvoda, usluga ili dobavljača itd.). Te bi mjere trebale služiti za uklanjanje svih vrsta sigurnosnih rizika utvrđenih procjenom rizika u jednoj državi članici ili više njih.

16. Nakon uspostave europskih programa kibersigurnosne certifikacije za 5G mreže države članice trebale bi donijeti, u skladu s pravom Unije, nacionalne tehničke propise za obveznu certifikaciju proizvoda, usluga te sustava informacijske i komunikacijske tehnologije koji su obuhvaćeni takvim programima.

17. Države članice trebale bi u suradnji s Komisijom utvrditi uvjete za zaštitu javnih mreža od neovlaštenog pristupa koje je potrebno dodati općem ovlaštenju i sigurnosne zahtjeve za mreže na temelju kojih će se zatražiti preuzimanje obveza od poduzeća koja sudjeluju u postupcima za dodjelu prava na korištenje spektra u 5G pojasevima u skladu s Direktivom 2002/20/EZ. Ako je moguće, to bi trebalo uzeti u obzir u mjerama iz točke 4.c.

18. Države članice trebale bi surađivati s Komisijom na izradi posebnih sigurnosnih zahtjeva koji bi se mogli primjenjivati u kontekstu javne nabave povezane s 5G mrežama. To bi trebalo uključivati obvezne zahtjeve za provedbu programa kibersigurnosne certifikacije u području javne nabave ako takvi programi još nisu obvezujući za sve dobavljače i operatere.

V. **PREISPITIVANJE**

19. Države članice trebale bi do 1. listopada 2020. u suradnji s Komisijom procijeniti učinke ove Preporuke kako bi se utvrdili odgovarajući daljnji koraci. U toj bi procjeni trebalo uzeti u obzir rezultate usklađene procjene rizika i skupa mjera na razini Unije.

Sastavljeno u Strasbourgu 26. ožujka 2019.

Za Komisiju
Julian KING
Član Komisije