PRIPOROČILA

PRIPOROČILO KOMISIJE (EU) 2019/534

z dne 26. marca 2019

Kibernetska varnost omrežij 5G

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 292 Pogodbe,

ob upoštevanju naslednjega:

(1) Komisija je uvedbo omrežnih tehnologij pete generacije (5G) prepoznala kot enega najpomembnejših dejavnikov, ki omogoča prihodnje digitalne storitve, in eno od prednostnih nalog strategije za enotni digitalni trg. Komisija je sprejela akcijski načrt za 5G, da bi zagotovila ustrezno infrastrukturo Unije za povezljivost, potrebno za njeno digitalno preobrazbo po letu 2020 ([1]).

(2) Omrežja 5G bodo temeljila na sedanjih omrežnih tehnologijah četrte generacije (4G), in sicer bodo zagotavljala nove storitvene zmogljivosti ter postala osrednja infrastruktura in gonilo za obsežne dele gospodarstva Unije. Omrežja 5G bodo po uvedbi postala hrbtenica širokega nabora storitev, ki so bistvenega pomena za delovanje notranjega trga ter za vzdrževanje in delovanje ključnih družbenih in ekonomskih funkcij, kot so energija, promet, bančništvo in zdravstvo, pa tudi industrijskih kontrolnih sistemov. Organizacija demokratičnih procesov, kot so volitve, bo vedno bolj odvisna od digitalne infrastrukture in omrežij 5G.

(3) Ker so številne kritične storitve odvisne od omrežij 5G, bi bile posledice sistemske in močno razširjene motnje še posebej resne. Zato je zagotavljanje kibernetske varnosti omrežij 5G vprašanje strateškega pomena za Unijo v času, ko se kibernetski napadi krepijo in so bolj prefinjeni kot kdaj koli prej.

(4) Medsebojna povezanost in nadnacionalni značaj infrastruktur, ki podpirajo digitalni ekosistem, ter čezmejna narava s tem povezanih groženj pomenijo, da bi morebitne pomembne šibke točke in/ali kibernetski incidenti v zvezi z omrežji 5G v eni državi članici vplivali na Unijo kot celoto. Zato bi bilo treba uvesti ukrepe za podporo visoki skupni ravni kibernetske varnosti omrežij 5G.

(5) Države članice so potrdile potrebo po ukrepanju na ravni Unije. Evropski svet v svojih sklepih z dne 21. marca 2019 navedel, da z zanimanjem pričakuje priporočilo Komisije za usklajen pristop k varnosti omrežij 5G ([2]).

(6) Zagotavljanje evropske suverenosti bi moralo biti eden glavnih ciljev, pri tem pa bi bilo treba v celoti spoštovati evropski vrednoti odprtosti in strpnosti ([3]). Tveganje za varnost Unije lahko predstavljajo tudi tuje naložbe v strateške sektorje, pridobitev kritičnih sredstev, tehnologij in infrastrukture v Uniji ter dobava kritične opreme.

(7) Kibernetska varnost omrežij 5G je ključna za zagotavljanje strateške avtonomije Unije, kar je priznano tudi v skupnem sporočilu „EU-Kitajska: strateška vizija“ ([4]).

(8) Resolucija Evropskega parlamenta o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU prav tako poziva Komisijo in države članice, naj ukrepajo na ravni Unije ([5]).

(9) To priporočilo obravnava tveganja za kibernetsko varnost v omrežjih 5G, in sicer z določitvijo smernic o ustreznih ukrepih za analizo in obvladovanje tveganja na nacionalni ravni, razvoju usklajene evropske ocene tveganja in vzpostavitvi postopka za razvoj skupnega nabora orodij, ki bi zajemal najboljše ukrepe za obvladovanje tveganja.

(10) Za zaščito elektronskih komunikacijskih omrežij je vzpostavljen trden zakonodajni okvir Unije.

([1]) COM(2016) 588 final.
([2]) Sklepi Evropskega sveta z dne 21. in 22. marca 2019.
([3]) Stanje v Uniji 2018 – Čas za evropsko suverenost, 12. september 2018.
([4]) JOIN(2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//SL.

(11) Okvir Unije na področju elektronskih komunikacij ([6]) spodbuja konkurenco, notranji trg in interese končnih uporabnikov ter si skupaj z Evropskim zakonikom o elektronskih komunikacijah ([7]) prizadeva za dodaten cilj glede povezljivosti, izražen glede na rezultate: širok dostop do in uporaba zelo visokozmogljive fiksne in mobilne povezljivosti za vse državljane in podjetja Unije ob zaščiti interesov državljanov. Direktiva 2002/21/ES zahteva, da države članice zagotovijo ohranjanje integritete in varnosti javnih komunikacijskih omrežij, hkrati pa podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve obvezuje, da sprejmejo tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganj za varnost omrežij in storitev. Določa tudi, da imajo pristojni nacionalni regulativni organi pooblastila za zagotovitev izpolnjevanja teh obveznosti, vključno s pooblastilom za izdajanje zavezujočih navodil.

(12) Poleg tega Direktiva 2002/20/ES Evropskega parlamenta in Sveta ([8]) državam članicam omogoča, da za zaščito zaupnosti komunikacij v skladu z Direktivo 2002/58/ES Evropskega parlamenta in Sveta ([9]) dodajo pogoje v zvezi z varnostjo javnih omrežij pred nepooblaščenim dostopom do splošne odobritve.

(13) Unija je v podporo izvajanju teh obveznosti vzpostavila številne organe za sodelovanje. Agencija za varnost omrežij in informacij (ENISA), Komisija, države članice in nacionalni regulativni organi so razvili tehnične smernice za nacionalne regulativne organe glede poročanja o incidentih, varnostnih ukrepov ter groženj in sredstev ([10]). Skupina za sodelovanje, ustanovljena z Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta ([11]) (v nadaljnjem besedilu: skupina za sodelovanje), združuje pristojne organe, da bi podprla in olajšala sodelovanje, zlasti z zagotavljanjem strateških smernic za dejavnosti mreže skupin za odzivanje na incidente na področju računalniške varnosti, ki na tehnični ravni omogoča operativno sodelovanje.

(14) Prihodnji evropski certifikacijski okvir za kibernetsko varnost ([12]) bi moral zagotoviti bistveno podporno orodje za spodbujanje enako visokih ravni varnosti. Omogočiti bi moral razvoj certifikacijskih shem za kibernetsko varnost, da bi se odzvali na potrebe uporabnikov strojne in programske opreme, povezane s 5G. Zaradi kritičnega pomena teh infrastruktur bi bilo treba čim prej in prednostno razviti ustrezne evropske certifikacijske sheme za kibernetsko varnost za izdelke, storitve ali postopke informacijskih in komunikacijskih tehnologij, ki se uporabljajo za omrežja 5G. Države članice in udeleženci na trgu bi morali dejavno sodelovati pri razvoju takih shem certificiranja, vključno z zagotavljanjem podpore za opredelitev posebnih profilov zaščite omrežij 5G.

(15) Če ni usklajenega prava Unije, lahko države članice z nacionalnimi tehničnimi predpisi, sprejetimi v skladu s pravom Unije, določijo, da mora biti evropska certifikacijska shema za kibernetsko varnost obvezna. Države članice lahko evropske certifikacijske sheme za kibernetsko varnost uporabljajo tudi v okviru javnih naročil in Direktive 2014/24/EU Evropskega parlamenta in Sveta ([13]) ter bi lahko podprle razvoj mehanizmov pomoči – kot je na primer vozlišče za pomoč – kupcem iz javnega sektorja pri nakupu rešitev na področju kibernetske varnosti.

(16) Visoka raven varstva podatkov in zasebnosti je pomemben element pri zagotavljanju varnosti omrežij 5G. Na ravni Unije so bila določena tudi pravila, ki zagotavljajo varnost obdelave osebnih podatkov, vključno z elektronskimi komunikacijami. Splošna uredba o varstvu podatkov ([14]) določa obveznost obdelave osebnih podatkov na način, ki zagotavlja njihovo varnost, vključno s preprečevanjem nepooblaščene uporabe ali dostopa

([6]) Direktiva 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL L 108, 24.4.2002, str. 33) in posamične direktive.

([7]) Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L 321, 17.12.2018, str. 36).

([8]) Direktiva 2002/20/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o odobritvi elektronskih komunikacijskih omrežij in storitev (Direktiva o odobritvi) (UL L 108, 24.4.2002, str. 21).

([9]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

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

([11]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, UL L 194, 19.7.2016, str. 1.

([12]) Predlog Uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti) (COM (2017) 477 final 2017/0225(COD)).

([13]) Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

([14]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

do osebnih podatkov in opreme, ki se uporablja za obdelavo. Direktiva o zasebnosti in elektronskih komunikacijah določa posebna pravila o varovanju zaupnosti komunikacij in terminalske opreme končnih uporabnikov. Poleg tega ponudnikom storitev nalaga obveznost, da sprejmejo ustrezne tehnične in organizacijske ukrepe za zagotavljanje varnosti svojih storitev.

(17) Unija je sprejela tudi instrument, ki bo varoval kritično infrastrukturo in tehnologije, na primer tiste, ki se uporabljajo v komunikacijah, in državam članicam omogočil, da pregledajo neposredne tuje naložbe zaradi varnosti ali javnega reda, ter vzpostavijo mehanizem za sodelovanje, s katerim bodo lahko države članice in Komisija izmenjevale informacije in izražale pomisleke v zvezi s posebnimi naložbami ([15]).

(18) Države članice in gospodarski subjekti trenutno sprejemajo pomembne pripravljalne ukrepe za obsežno uvajanje omrežij 5G. Več držav članic je izrazilo zaskrbljenost glede morebitnih varnostnih tveganj, povezanih z omrežji 5G v okviru izvajanja postopkov za podelitev pravic do uporabe v radiofrekvenčnih pasovih, določenih za omrežja 5G ([16]), in proučujejo ukrepe za odpravo teh tveganj.

(19) Pri obravnavanju tveganj za kibernetsko varnost v omrežjih 5G bi bilo treba upoštevati tako tehnične kot druge dejavnike. Tehnični dejavniki lahko vključujejo šibke točke na področju kibernetske varnosti, ki jih je mogoče izkoristiti za pridobitev nepooblaščenega dostopa do informacij (kibernetsko vohunjenje, tako iz gospodarskih kot političnih razlogov) ali za druge zlonamerne cilje (kibernetski napadi, usmerjeni v motenje ali uničevanje sistemov in podatkov). Med pomembnimi vidiki, ki bi jih bilo treba upoštevati, sta potreba po zaščiti omrežij v celotnem življenjskem ciklu in potreba, da se zajame vsa zadevna oprema, tudi v fazah zasnove, razvoja, javnega naročanja, izgradnje, obratovanja in vzdrževanja omrežij 5G.

(20) Med drugimi dejavniki so lahko tudi regulativne ali druge zahteve, ki se naložijo dobaviteljem opreme za informacijsko in komunikacijsko tehnologijo. Pri oceni pomembnosti takih dejavnikov bi bilo treba med drugim upoštevati splošno tveganje vpliva tretje države, zlasti v zvezi z njegovim modelom upravljanja, odsotnost sporazumov o sodelovanju na področju varnosti ali podobnih ureditev, kot so na primer sklep o ustreznosti varstva, glede varstva podatkov med Unijo in zadevno tretjo državo oziroma ali je zadevna država pogodbenica večstranskih, mednarodnih ali dvostranskih sporazumov o kibernetski varnosti, boju proti kibernetski kriminaliteti ali varstvu podatkov.

(21) Kot pomemben korak pri razvoju pristopa Unije k kibernetski varnosti omrežij 5G bi bilo treba oceno tveganja izvesti in zaključiti na nacionalni ravni. Države članice bi tako lahko na podlagi te ocene prilagodile nacionalne ukrepe glede varnostnih zahtev in obvladovanja tveganja.

(22) Treba bi bilo vzpostaviti usklajevanje, da se zagotovi učinkovitost ukrepov za obravnavanje teh groženj za kibernetsko varnost, saj so ti ukrepi bistveni za nemoteno delovanje notranjega trga ter za varstvo osebnih podatkov in zasebnosti.

(23) Nacionalne ocene tveganja bi morale biti podlaga za usklajeno oceno tveganja na ravni Unije, sestavljeno iz kartiranja groženj in skupnega pregleda, ki ga izvajajo države članice, in sicer ob podpori Komisije in skupaj z Evropsko agencijo za kibernetsko varnost (ENISA).

(24) Ob upoštevanju nacionalnih ocen tveganja in ocen tveganja na ravni Unije bi morala skupina za sodelovanje oblikovati nabor orodij za opredelitev vrst tveganj za kibernetsko varnost in možnih ukrepov za zmanjšanje tveganj na področjih, ki vključujejo certificiranje, preskušanje in nadzor dostopa. Opredeliti bi morala tudi možne posebne ukrepe, ki bi bili primerni za obravnavanje tveganj, ki bi jih ugotovila ena ali več držav članic. Skupina za sodelovanje bi morala delovati ob podpori Evropske agencije za kibernetsko varnost (ENISA), Europola, Organa evropskih regulatorjev za elektronske komunikacije (BEREC) ter Obveščevalnega in situacijskega centra EU. Ta nabor orodij bi moral Komisiji pomagati pri razvoju minimalnih skupnih zahtev za nadaljnje zagotavljanje visoke ravni kibernetske varnosti omrežij 5G po vsej Uniji.

(25) Ob sprejemanju ukrepov za obravnavanje tveganj, povezanih s kibernetsko varnostjo, bi bilo treba pri izgradnji enotnega omrežja upoštevati spodbujanje kibernetske varnosti prek raznolikosti dobaviteljev.

([15]) Uredba (EU) 2019/452 Evropskega parlamenta in Sveta z dne 19. marca 2019 o vzpostavitvi okvira za pregled neposrednih tujih naložb v Uniji (UL L 79I, 21.3.2019, str. 1).

([16]) V letu 2019 je postopek dražbe v vsaj enem frekvenčnem pasu predviden v 11 državah članicah: Avstriji, Belgiji, Češki, Franciji, Grčiji, Irski, Litvi, Madžarski, Nemčiji, Nizozemski in Portugalski. Za leto 2020 je predvidenih še šest dražb, in sicer v Litvi (različne frekvence), na Malti, Poljskem in Slovaškem, v Španiji in v Združenem kraljestvu. *Vir*: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) To priporočilo ne bi smelo posegati v pristojnosti držav članic, kar zadeva dejavnosti v zvezi z javno varnostjo, obrambo, nacionalno varnostjo in dejavnostmi države na področju kazenskega prava, vključno s pravico držav članic, da iz razlogov nacionalne varnosti iz svojih trgov izključijo ponudnike ali ponudnike storitev –

SPREJELA NASLEDNJE PRIPOROČILO:

I. **CILJI**

(1) Da bi se podprl razvoj pristopa Unije k zagotavljanju kibernetske varnosti omrežij 5G, so v tem priporočilu opredeljeni ukrepi, ki jih je treba sprejeti, da lahko:

(a) države članice ocenijo tveganja za kibernetsko varnost, ki vplivajo na omrežja 5G na nacionalni ravni, in sprejmejo potrebne varnostne ukrepe;

(b) države članice in ustrezne institucije, agencije ter drugi organi Unije skupaj pripravijo usklajeno oceno tveganja na ravni Unije, ki temelji na nacionalni oceni tveganja;

(c) skupina za sodelovanje, ustanovljena v skladu z Direktivo (EU) 2016/1148 (v nadaljnjem besedilu: skupina za sodelovanje), opredeli morebiten skupni sklop ukrepov, ki jih je treba sprejeti za zmanjšanje tveganj za kibernetsko varnost, povezanih z infrastrukturami, ki podpirajo digitalni ekosistem, zlasti omrežji 5G.

II. **OPREDELITEV POJMOV**

(2) V tem priporočilu se uporabljata naslednji opredelitvi pojmov:

(a) „omrežja 5G“ pomeni sklop vseh relevantnih elementov omrežne infrastrukture za mobilno in brezžično in brezžično komunikacijsko tehnologijo, ki se uporabljajo za povezljivost in storitve dodane vrednosti, z značilnostmi naprednega delovanja, kot so zelo velika hitrost prenosa podatkov in zmogljivost, komunikacije z nizko stopnjo zakasnitve, ultravisoka stopnja zanesljivosti ali podpiranje številnih povezanih naprav. Ti lahko vključujejo podedovane omrežne elemente, ki temeljijo na prejšnjih generacijah mobilne in brezžične komunikacijske tehnologije, kot sta 4G ali 3G. Pojem omrežja 5G je treba razumeti tako, da zajema vse ustrezne dele omrežja;

(b) „infrastruktura, ki podpira digitalni ekosistem“ pomeni infrastrukturo, ki se uporablja za omogočanje digitalizacije v širokem naboru kritičnih aplikacij v gospodarstvu in družbi.

III. **UKREPI NA NACIONALNI RAVNI**

(3) Države članice bi morale do 30. junija 2019 izvesti oceno tveganja omrežne infrastrukture 5G, vključno z opredelitvijo najbolj občutljivih elementov, kjer bi imele kršitve varnosti znaten negativen učinek. Do istega datuma bi morale države članice pregledati tudi varnostne zahteve in metode obvladovanja tveganja, ki se uporabljajo na nacionalni ravni, da bi se upoštevale kibernetske grožnje, ki lahko izhajajo iz (i) tehničnih dejavnikov, kot so posebne tehnične značilnosti omrežij 5G, in (ii) drugih dejavnikov, kot sta pravni in politični okvir, ki lahko velja za dobavitelje opreme za informacijsko in komunikacijsko tehnologijo v tretjih državah.

(4) Na podlagi nacionalne ocene tveganja in pregleda ter ob upoštevanju stalnega usklajenega ukrepanja na ravni Unije bi morale države članice:

(a) posodobiti varnostne zahteve in metode obvladovanja tveganja, ki se uporabljajo v zvezi z omrežji 5G;

(b) posodobiti relevantne obveznosti, naložene podjetjem, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve v skladu s členoma 13a in 13b Direktive 2002/21/ES;

(c) splošni odobritvi dodati pogoje v zvezi z varnostjo javnih omrežij pred nepooblaščenim dostopom in od podjetij, ki sodelujejo v morebitnih prihodnjih postopkih za podeljevanje pravic uporabe radijskih frekvenc v pasovih 5G, zahtevati zaveze glede skladnosti z varnostnimi zahtevami za omrežja v skladu z Direktivo 2002/20/ES;

(d) uporabiti druge preventivne ukrepe, namenjene blažitvi morebitnih tveganj za kibernetsko varnost.

(5) Ukrepi iz točke 4 bi morali vključevati okrepljene obveznosti za dobavitelje in upravljavce, da zagotovijo varnost občutljivih delov omrežja in, kadar je to primerno, obveznosti zagotavljanja ustreznih informacij pristojnim nacionalnim organom v zvezi z načrtovanimi spremembami v elektronskih komunikacijskih omrežjih ter zahteve, da nacionalni revizijski / certifikacijski laboratoriji za namene varnosti in integritete predhodno preverijo specifične komponente in sisteme informacijske tehnologije za namene varnosti in celovitosti.

(6) Skupne varnostne preglede bi morale izvajati dve ali več držav članic, in sicer z uporabo in izmenjavo ustreznega tehničnega strokovnega znanja in zmogljivosti v zvezi z infrastrukturami, ki podpirajo digitalni ekosistem in omrežja 5G, na primer kadar isto podjetje upravlja ali gradi omrežno infrastrukturo v več kot eni državi članici ali kadar so v njihovih omrežnih konfiguracijah znatne podobnosti. Evropska agencija za kibernetsko varnost (ENISA), Europol in Organ evropskih regulatorjev za elektronske komunikacije (BEREC) bi morale prednostno obravnavati prošnje držav članic za podporo na tem področju. Rezultate teh pregledov bi bilo treba sporočiti skupini za sodelovanje in mreži skupin za odzivanje na incidente na področju računalniške varnosti.

IV. **USKLAJENO UKREPANJE NA RAVNI UNIJE**

(7) Za razvoj skupnega pristopa k obravnavi tveganj za kibernetsko varnost v zvezi z omrežji 5G bi morale države članice do 30. aprila 2019 v skupini za sodelovanje začeti delovati v okviru namenskega poteka dela. Države članice bi morale povabiti ustrezne organe, da po potrebi sodelujejo pri delu skupine za sodelovanje.

Usklajena evropska ocena tveganja

(8) Države članice bi si morale izmenjevati informacije med seboj in z ustreznimi organi Unije, da bi oblikovale skupno zavest o obstoječih in potencialnih tveganjih za kibernetsko varnost, povezanih z omrežji 5G.

(9) Države članice bi morale svoje nacionalne ocene tveganja do 15. julija 2019 posredovati Komisiji in Evropski agenciji za kibernetsko varnost (ENISA).

(10) Evropska agencija za varnost omrežij in informacij (ENISA) bi morala dokončati kartiranje groženj posebej za omrežja 5G. Za proces bi morali podpirati skupina za sodelovanje in mreža skupin za odzivanje na incidente na področju računalniške varnosti, vzpostavljeni v skladu z Direktivo (EU) 2016/1148.

(11) Ob upoštevanju vseh teh elementov bi morale države članice ob podpori Komisije in skupaj z Evropsko agencijo za kibernetsko varnost (ENISA) do 1. oktobra 2019 dokončati skupni pregled izpostavljenosti tveganjem, povezanim z infrastrukturami, ki podpirajo digitalni ekosistem, zlasti omrežji 5G, in sicer na ravni Unije.

(12) V skupnem pregledu bi morali prednost nameniti analizi tveganj, povezanih s posebej občutljivimi ali ranljivimi elementi, ki so vključeni v jedrne elemente omrežij 5G, operativnim in vzdrževalnim središčem ter elementi dostopovnega omrežja 5G, ki se uporabljajo v industriji.

(13) V drugi fazi bi bilo treba ta skupni pregled razširiti na druge strateške elemente digitalne vrednostne verige.

Skupni nabor orodij Unije za obravnavanje tveganj

(14) Pri delu skupine za sodelovanje bi bilo treba opredeliti najboljše prakse, ki se uporabljajo na nacionalni ravni, kot je določeno v točki 4. Na podlagi teh nacionalnih dobrih praks bi bilo treba do 31. decembra 2019 sprejeti nabor ustreznih, učinkovitih in sorazmernih ukrepov za zmanjševanje ugotovljenih tveganj za kibernetsko varnost na nacionalni ravni in ravni Unije; ta nabor ukrepov bo Komisiji pomagal pri razvoju minimalnih skupnih zahtev za nadaljnjo zagotovitev visoke ravni kibernetske varnosti omrežij 5G po vsej Uniji.

(15) Ta nabor orodij bi moral vključevati:

(a) seznam vrst varnostnih tveganj, ki lahko vplivajo na kibernetsko varnost omrežij 5G (npr. tveganje v zvezi z dobavno verigo, tveganje ranljivosti programske opreme, tveganje pri nadzoru dostopa, tveganja, ki izhajajo iz pravnega in političnega okvira, ki lahko v tretjih državah velja za dobavitelje opreme za informacijsko in komunikacijsko tehnologijo) in

(b) sklop možnih ukrepov za zmanjšanje tveganja (npr. certificiranje strojne opreme, programske opreme ali storitev, ki ga opravi tretja oseba, formalni preskusi strojne in programske opreme ali preverjanje skladnosti, postopki za zagotavljanje obstoja in izvajanja nadzora dostopa, identifikacija izdelkov, storitve ali dobavitelji, za katere se šteje, da potencialno niso varni, itd.). Ti ukrepi bi morali obravnavati vse vrste varnostnega tveganja, ki se ob oceni tveganja ugotovijo v eni ali več državah članicah.

(16) Ko bodo razvite evropske certifikacijske sheme za kibernetsko varnost, ki se bodo uporabljale za omrežja 5G, bi morale države članice v skladu s pravom Unije sprejeti nacionalne tehnične predpise, ki bodo določali obvezno certificiranje izdelkov, storitev ali sistemov, zajetih v teh shemah.

(17) Države članice bi morale skupaj s Komisijo opredeliti pogoje v zvezi z varnostjo javnih omrežij pred nepooblaščenim dostopom, ki se dodajo splošni odobritvi, in varnostne zahteve za omrežja za potrebe zahtev po zavezah od podjetij, ki sodelujejo v postopkih za podeljevanje pravic uporabe spektra pasov 5G v skladu z Direktivo 2002/20/ES. Te bi se morale, če je to mogoče, odražati v ukrepih, sprejetih v točki 4(c).

(18) Države članice bi morale v sodelovanju s Komisijo razviti posebne varnostne zahteve, ki bi se lahko uporabljale v okviru javnih naročil, povezanih z omrežji 5G. To bi moralo vključevati obvezne zahteve za izvajanje certifikacijskih shem za kibernetsko varnost na področju javnih naročil, če takšne sheme še niso zavezujoče za vse dobavitelje in upravljavce.

V. **PREGLED**

(19) Države članice bi morale sodelovati s Komisijo, da bi za določitev ustreznih nadaljnjih korakov ocenile učinke tega priporočila do 1. oktobra 2020. Pri tej oceni bi bilo treba upoštevati rezultate usklajene ocene tveganja Unije in nabora orodij Unije.

V Strasbourgu, 26. marca 2019

Za Komisijo
Julian KING
Član Komisije