ODPORÚČANIA

ODPORÚČANIE KOMISIE (EÚ) 2019/534

z 26. marca 2019

Kybernetická bezpečnosť sietí 5G

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 292,

keďže:

(1) Komisia uznala zavedenie sieťových technológií 5. generácie (5G) za hlavný faktor umožňujúci budúce digitálne služby a za prioritu pre stratégiu digitálneho jednotného trhu. Komisia prijala akčný plán pre oblasť 5G s cieľom zabezpečiť, aby Únia mala od roku 2020 infraštruktúru pripojiteľnosti potrebnú pre svoju digitálnu transformáciu ([1]).

(2) Základom sietí 5G budú súčasné sieťové technológie 4. generácie (4G). Tieto siete budú poskytovať nové kapacity služieb a stanú sa ústrednou infraštruktúrou a základným nástrojom pre mnohé odvetvia hospodárstva Únie. Po spustení budú siete 5G tvoriť základ pre širokú škálu služieb nevyhnutných pre fungovanie vnútorného trhu a zachovanie a fungovanie dôležitých spoločenských a hospodárskych funkcií, ako sú energetika, doprava, bankovníctvo a zdravotníctvo, ako aj priemyselných riadiacich systémov. Digitálna infraštruktúra a siete 5G sa budú čoraz viac využívať aj pri organizovaní demokratických procesov, ako sú voľby.

(3) Z dôvodu závislosti mnohých kritických služieb od sietí 5G by dôsledky systémového a rozsiahleho narušenia boli mimoriadne závažné. V dôsledku toho je zaistenie kybernetickej bezpečnosti sietí 5G pre Úniu otázkou strategického významu v čase, keď sú kybernetické útoky na vzostupe a sú sofistikovanejšie než kedykoľvek predtým.

(4) Prepojená a nadnárodná povaha infraštruktúr, ktoré tvoria základ digitálneho ekosystému, a cezhraničný charakter príslušných hrozieb znamenajú, že všetky výrazné zraniteľné miesta a/alebo kybernetické bezpečnostné incidenty týkajúce sa sietí 5G čo i len v jednom členskom štáte, by mali vplyv na Úniu ako celok. Preto by sa mali prijať opatrenia na podporu vysokej spoločnej úrovne kybernetickej bezpečnosti sietí 5G.

(5) Členské štáty potvrdili potrebu opatrení na úrovni Únie. Európska rada vo svojich záveroch z 21. marca 2019 so záujmom očakáva odporúčanie Komisie týkajúce sa spoločného prístupu k bezpečnosti sietí 5G ([2]).

(6) Hlavným cieľom by malo byť zabezpečenie európskej suverenity pri plnom rešpektovaní európskych hodnôt otvorenosti a tolerancie ([3]). Zahraničné investície do strategických odvetví, akvizícia kritických aktív, technológií a infraštruktúry v Únii a dodávanie kritických zariadení môžu takisto predstavovať riziká pre bezpečnosť Únie.

(7) Kybernetická bezpečnosť sietí 5G je kľúčová na zabezpečenie strategickej autonómie Únie, ako sa uvádza v spoločnom oznámení „EÚ – Čína: strategická vízia“ ([4]).

(8) V uznesení Európskeho parlamentu o bezpečnostných hrozbách súvisiacich s rastúcou čínskou technologickou prítomnosťou v Únii sa Komisia a členské štáty vyzývajú, aby prijali opatrenia na úrovni Únie ([5]).

(9) Toto odporúčanie rieši riziká v oblasti kybernetickej bezpečnosti sietí 5G stanovením usmernení o vhodných analýzach rizík a riadiacich opatreniach na vnútroštátnej úrovni, o vypracovaní koordinovaného európskeho posúdenia rizík a o zavedení postupu na vypracovanie spoločného súboru najlepších opatrení na riadenie rizík.

(10) Zaviedol sa silný legislatívny rámec Únie na ochranu elektronických komunikačných sietí.

([1]) COM(2016) 588 final.
([2]) Závery Európskej rady z 21. a 22. marca 2019.
([3]) Správa o stave Únie v roku 2018 – Čas na európsku suverenitu, 12. septembra 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) Rámec Únie v oblasti elektronických komunikácií ([6]) podporuje hospodársku súťaž, vnútorný trh a záujmy koncových používateľov a pomocou európskeho kódexu elektronickej komunikácie ([7]) sleduje dodatočný cieľ v oblasti pripojiteľnosti vyjadrený v podobe výsledkov: všeobecný prístup k pevnému a mobilnému pripojeniu s veľmi vysokou kapacitou pre všetkých občanov a podniky v Únii a jeho využívanie, pri ochrane záujmov občanov Únie. V smernici 2002/21/ES sa od členských štátov vyžaduje, aby zabezpečili zachovanie integrity a bezpečnosti verejných komunikačných sietí. Ich povinnosťou je zaistiť, aby podniky, ktoré poskytujú verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby, prijali technické a organizačné opatrenia na primerané riadenie rizík spojených s bezpečnosťou sietí a služieb. Takisto sa v nej stanovuje, že príslušné národné regulačné orgány majú právomoci (vrátane právomoci vydávať záväzné usmernenia) na zabezpečenie dodržiavania týchto povinností.

(12) Okrem toho smernica Európskeho parlamentu a Rady 2002/20/ES ([8]) umožňuje členským štátom, aby na účely ochrany dôvernosti komunikácií v súlade so smernicou Európskeho parlamentu a Rady 2002/58/ES ([9]) k všeobecnému povoleniu pripojili podmienky týkajúce sa zabezpečenia verejných sietí proti neoprávnenému prístupu.

(13) Na podporu plnenia týchto povinností zriadila Únia niekoľko orgánov spolupráce. Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), Komisia, členské štáty a národné regulačné orgány vypracovali pre národné regulačné orgány technické usmernenia týkajúce sa oznamovania bezpečnostných incidentov, bezpečnostných opatrení, hrozieb a aktív ([10]). Skupina pre spoluprácu zriadená smernicou Európskeho parlamentu a Rady (EÚ) 2016/1148 ([11]) (ďalej len „skupina pre spoluprácu“) združuje príslušné orgány s cieľom podporovať a uľahčovať spoluprácu, najmä poskytovaním strategického usmernenia pre činnosti siete jednotiek pre riešenie počítačových bezpečnostných incidentov, ktorá na technickej úrovni uľahčuje operačnú spoluprácu.

(14) Budúci rámec certifikácie kybernetickej bezpečnosti ([12]) by mal poskytnúť nevyhnutný podporný nástroj na zaistenie konzistentnej úrovne bezpečnosti. Mal by umožňovať rozvoj systémov certifikácie kybernetickej bezpečnosti s cieľom reagovať na potreby používateľov zariadení a softvéru, ktoré využívajú 5G. Obrovský význam týchto infraštruktúr by mal byť dôvodom, aby sa rozvoj príslušných európskych systémov certifikácie kybernetickej bezpečnosti pre výrobky, služby alebo procesy informačných a komunikačných technológií používaných v sieťach 5G stal okamžitou prioritou. Členské štáty a účastníci trhu by sa mali aktívne zapájať do rozvoja takýchto systémov certifikácie vrátane poskytovania podpory pri definovaní špecifických profilov ochrany pre siete 5G.

(15) Ak neexistuje harmonizované právo Únie, členské štáty môžu prostredníctvom vnútroštátnych technických predpisov prijatých v súlade s právom Únie stanoviť, že európsky systém certifikácie kybernetickej bezpečnosti by mal byť povinný. Členské štáty takisto využívajú európske systémy certifikácie kybernetickej bezpečnosti v kontexte verejného obstarávania a smernice Európskeho parlamentu a Rady 2014/24/EÚ ([13]) a mohli by podporovať rozvoj mechanizmov pomoci (ako napr. centra pomoci) slúžiacich verejným obstarávateľom pri nákupe kyberneticko-bezpečnostných riešení.

(16) Vysoká úroveň ochrany údajov a súkromia je dôležitým prvkom pri zaisťovaní bezpečnosti sietí 5G. Na úrovni Únie sa stanovili aj pravidlá zaisťujúce bezpečnosť spracovania osobných údajov, a to aj v oblasti elektronických komunikácií. Vo všeobecnom nariadení o ochrane údajov ([14]) sa stanovuje povinnosť spracovávať osobné údaje spôsobom, ktorým sa zaistí ich bezpečnosť, vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení. V smernici

([6]) Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) (Ú. v. ES L 108, 24.4.2002, s. 33) a osobitné smernice.

([7]) Smernica Európskeho Parlamentu a rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (Ú. v. EÚ L 321, 17.12.2018, s. 36).

([8]) Smernica Európskeho parlamentu a Rady 2002/20/ES zo 7. marca 2002 o povolení na elektronické komunikačné siete a služby (smernica o povolení) (Ú. v. ES L 108, 24.4.2002, s. 21).

([9]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

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

([11]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

([12]) Návrh Nariadenie Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“) [COM (2017) 477 final – 2017/0225 (COD)].

([13]) Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

([14]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

o súkromí a elektronických komunikáciách sa stanovujú osobitné pravidlá ochrany dôvernosti komunikácie a koncových zariadení koncových používateľov. Ukladá sa v nej aj povinnosť poskytovateľom služieb prijať primerané technické a organizačné opatrenia na zaistenie bezpečnosti svojich služieb.

(17) Únia takisto prijala nástroj, ktorým sa bude chrániť kritická infraštruktúra a technológie, ako napríklad tie, ktoré sa používajú v komunikácii, a to tak, že členským štátom umožní preverovať priame zahraničné investície z hľadiska bezpečnosti alebo verejného poriadku, a vytvorením mechanizmu spolupráce, v rámci ktorého si členské štáty a Komisia budú môcť vymieňať informácie a vyjadrovať obavy v súvislosti s konkrétnymi investíciami ([15]).

(18) Členské štáty a prevádzkovatelia v súčasnosti prijímajú dôležité prípravné kroky smerujúce k rozsiahlemu zavádzaniu sietí 5G. Niekoľko členských štátov vyjadrilo obavy týkajúce sa možných bezpečnostných rizík súvisiacich so sieťami 5G, ktoré sa môžu objaviť v rámci vykonávania postupov udeľovania práv na využívanie rádiových frekvenčných pásiem určených pre siete 5G ([16]) a preskúmali opatrenia na riešenie týchto rizík.

(19) Riešenie rizík v oblasti kybernetickej bezpečnosti sietí 5G by malo zohľadňovať technické aj iné faktory. Medzi technické faktory môžu patriť aj zraniteľné miesta z hľadiska kybernetickej bezpečnosti, ktoré možno využiť na získanie neoprávneného prístupu k informáciám (kybernetická špionáž, či už z ekonomických alebo politických dôvodov) alebo na iné škodlivé účely (kybernetické útoky zamerané na narušenie alebo zničenie systémov a údajov). Medzi dôležité aspekty, ktoré treba zvážiť, by mala patriť potreba chrániť siete počas ich celého životného cyklu a potreba zahrnúť všetky príslušné zariadenia, a to aj vo fáze navrhovania, vývoja, obstarávania, zavedenia, prevádzky a údržby sietí 5G.

(20) Iné faktory môžu zahŕňať regulačné alebo iné požiadavky, ktoré boli uložené dodávateľom zariadení informačných a komunikačných technológií. Pri posúdení významu týchto faktorov by sa malo okrem iného zohľadniť celkové riziko vplyvu tretej krajiny, najmä v súvislosti s jej modelom riadenia, absenciou dohôd o spolupráci v oblasti bezpečnosti alebo podobných opatrení, ako napr. rozhodnutí o primeranosti, súvisiacich s ochranou údajov medzi Úniou a dotknutou treťou krajinou, alebo či je táto krajina zmluvnou stranou viacstranných, medzinárodných alebo dvojstranných dohôd v oblasti kybernetickej bezpečnosti, boja proti počítačovej kriminalite alebo ochrany údajov.

(21) Jedným z dôležitých krokov pri rozvoji prístupu Únie ku kybernetickej bezpečnosti sietí 5G by malo byť vykonanie a dokončenie posúdenia rizika na vnútroštátnej úrovni. Členské štáty by mohli na základe tohto posúdenia upraviť vnútroštátne opatrenia týkajúce sa bezpečnostných požiadaviek a riadenia rizík.

(22) Je potrebné posilňovať koordináciu, aby sa zabezpečila účinnosť opatrení zameraných na riešenie týchto kybernetických hrozieb, ktoré sú nevyhnutné pre hladké fungovanie vnútorného trhu a pre ochranu osobných údajov a súkromia.

(23) Vnútroštátne posúdenia rizika by mali byť základom pre koordinované posúdenie rizika na úrovni Únie, ktoré pozostáva z mapovania situácie v súvislosti s kybernetickými hrozbami a spoločného preskúmania, ktoré majú vykonať členské štáty s podporou Komisie a Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA).

(24) So zreteľom na posúdenia rizika na vnútroštátnej úrovni a na úrovni Únie by skupina pre spoluprácu mala vytvoriť súbor nástrojov na identifikáciu rizík v oblasti kybernetickej bezpečnosti a možných opatrení na zmiernenie rizík v oblastiach vrátane certifikácie, testovania a kontrol prístupu. Takisto by mala určiť prípadné osobitné opatrenia vhodné na riešenie rizík, ktoré identifikoval jeden alebo viacero členských štátov. Skupina pre spoluprácu by mala využiť podporu Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA), Europolu, Orgánu európskych regulátorov pre elektronické komunikácie (BEREC) a Spravodajského a situačného centra EÚ. Komisia by mala z tohto súboru nástrojov čerpať pri vypracúvaní minimálnych spoločných požiadaviek na ďalšie zabezpečenie vysokej úrovne kybernetickej bezpečnosti sietí 5G v celej Únii.

(25) Pri prijímaní opatrení na riešenie rizík v oblasti kybernetickej bezpečnosti by sa pri budovaní akejkoľvek siete mala zvážiť podpora kybernetickej bezpečnosti prostredníctvom rozmanitosti dodávateľov.

([15]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie (Ú v EÚ L 79I, 21.3.2019, s. 1.).

([16]) Aukčný postup, pokiaľ ide minimálne o jedno frekvenčné pásmo, je na rok 2019 naplánovaný v 11 členských štátoch: Rakúsko, Belgicko, Česká republika, Francúzsko, Nemecko, Grécko, Maďarsko, Írsko, Holandsko, Litva, Portugalsko. Na rok 2020 je naplánovaných ďalších šesť aukcií: Španielsko, Malta, Litva (rôzne frekvencie), Slovensko, Poľsko, Spojené kráľovstvo. Zdroj: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Toto odporúčanie by nemalo mať vplyv na právomoci členských štátov, pokiaľ ide o činnosti týkajúce sa verejnej bezpečnosti, obrany, národnej bezpečnosti a činností štátu v oblasti trestného práva vrátane práva členských štátov vylúčiť poskytovateľov alebo dodávateľov zo svojich trhov z dôvodov národnej bezpečnosti.

PRIJALA TOTO ODPORÚČANIE:

I. **CIELE**

1. V záujme rozvoja prístupu Únie k zaisteniu kybernetickej bezpečnosti sietí 5G sa v tomto odporúčaní uvádzajú opatrenia, ktoré by sa mali prijať s cieľom umožniť:

   a) členským štátom posudzovať riziká v oblasti kybernetickej bezpečnosti s vplyvom na siete 5G na vnútroštátnej úrovni a prijímať potrebné bezpečnostné opatrenia;

   b) členským štátom a príslušným inštitúciám, agentúram a iným orgánom Únie spoločne vypracovať koordinované posúdenie rizík na úrovni Únie, ktoré bude vychádzať z vnútroštátneho posúdenia rizika;

   c) skupine pre spoluprácu zriadenej podľa smernice (EÚ) 2016/1148 (ďalej len „skupina pre spoluprácu“) identifikovať prípadný spoločný súbor opatrení, ktoré sa majú prijať s cieľom zmierniť riziká v oblasti kybernetickej bezpečnosti súvisiace s infraštruktúrami, ktoré tvoria základ digitálneho ekosystému, a najmä sietí 5G.

II. **VYMEDZENIE POJMOV**

2. Na účely tohto odporúčania:

   a) „siete 5G“ sú súbory všetkých príslušných prvkov sieťovej infraštruktúry pre mobilné a bezdrôtové komunikačné technológie používané na pripojenie a služby s pridanou hodnotou s pokročilými výkonnostnými charakteristikami, ako sú veľmi vysoká rýchlosť a kapacita prenosu dát, malé oneskorenie komunikácie, ultravysoká spoľahlivosť či podpora veľkého počtu pripojených zariadení. Môžu zahŕňať tradičné sieťové prvky založené na predchádzajúcich generáciách mobilných a bezdrôtových komunikačných technológií ako 4G alebo 3G. Sieťami 5G by sa mali rozumieť všetky príslušné časti siete.

   b) „infraštruktúry, ktoré tvoria základ digitálneho ekosystému“ sú infraštruktúry používané s cieľom umožniť digitalizáciu širokej škály kritických aplikácií v hospodárstve a spoločnosti.

III. **OPATRENIA NA VNÚTROŠTÁTNEJ ÚROVNI**

3. Členské štáty by do 30. júna 2019 mali vykonať posúdenie rizika sieťovej infraštruktúry 5G vrátane určenia najcitlivejších prvkov, v prípade ktorých by narušenie bezpečnosti malo významný negatívny vplyv. Členské štáty by mali do toho istého dátumu preskúmať aj bezpečnostné požiadavky a metódy riadenia rizík uplatniteľné na vnútroštátnej úrovni s cieľom zohľadniť kybernetické hrozby, ktoré môžu vyplynúť z i) technických faktorov, ako sú špecifické technické vlastnosti sietí 5G, a ii) iných faktorov, ako je právny a politický rámec, ktorý sa môže vzťahovať na dodávateľov zariadení informačných a komunikačných technológií v tretích krajinách.

4. Na základe tohto vnútroštátneho posúdenia rizika a preskúmania a s prihliadnutím na prebiehajúce koordinované opatrenia na úrovni Únie by členské štáty mali:

   a) aktualizovať uplatňované bezpečnostné požiadavky a metódy riadenia rizík so zreteľom na siete 5G;

   b) aktualizovať príslušné povinnosti uložené podnikom, ktoré poskytujú verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby podľa článkov 13a a 13b smernice 2002/21/ES;

   c) pripojiť podmienky k všeobecnému povoleniu týkajúcemu sa zabezpečenia verejných sietí proti neoprávnenému prístupu a požadovať záväzky od podnikov, ktoré sa zúčastňujú na akýchkoľvek pripravovaných postupoch udeľovania práv na využívanie rádiových frekvencií v pásmach 5G, pokiaľ ide o dodržiavanie bezpečnostných požiadaviek na siete podľa smernice 2002/20/ES;

   d) uplatňovať iné preventívne opatrenia zamerané na zmiernenie potenciálnych rizík v oblasti kybernetickej bezpečnosti.

5. Opatrenia uvedené v bode 4 by mali zahŕňať posilnené povinnosti dodávateľov a prevádzkovateľov, pokiaľ ide o zaistenie bezpečnosti citlivých častí sietí, a v prípade potreby aj povinnosti, ako je poskytovanie relevantných informácií o plánovaných zmenách v elektronických komunikačných sieťach a zavedenie požiadavky, aby vnútroštátne audítorské/certifikačné laboratóriá na účely bezpečnosti a integrity vopred otestovali špecifické komponenty a systémy informačných technológií.

6. Spoločné preskúmania bezpečnosti by mali vykonávať dva alebo viacero členských štátov, pričom by mali využívať a zdieľať vhodné technické odborné znalosti a zariadenia týkajúce sa infraštruktúr, ktoré tvoria základ digitálneho ekosystému a sietí 5G, napríklad vtedy, keď ten istý podnik prevádzkuje alebo buduje sieťovú infraštruktúru vo viac ako jednom členskom štáte, alebo ak sú si konfigurácie siete veľmi podobné. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA), Europol a Orgán európskych regulátorov pre elektronické komunikácie (BEREC) by mali uprednostniť žiadosti členských štátov o podporu v tejto oblasti. Výsledky týchto preskúmaní by sa mali postúpiť skupine pre spoluprácu a sieti jednotiek pre riešenie počítačových bezpečnostných incidentov.

IV. **KOORDINOVANÉ OPATRENIA NA ÚROVNI ÚNIE**

7. S cieľom rozvíjať spoločný prístup k riešeniu rizík v oblasti kybernetickej bezpečnosti, pokiaľ ide o siete 5G, by členské štáty mali v rámci skupiny pre spoluprácu do 30. apríla 2019 začať fungovať v rámci samostatného pracovného okruhu. Členské štáty by mali vyzvať príslušné orgány, aby sa v prípade potreby zúčastňovali na práci skupiny pre spoluprácu.

Koordinované európske posúdenie rizika

8. Členské štáty by si mali vymieňať informácie medzi sebou a s príslušnými orgánmi Únie s cieľom zvyšovať spoločné povedomie o existujúcich a potenciálnych rizikách v oblasti kybernetickej bezpečnosti spojených so sieťami 5G.

9. Členské štáty by mali postúpiť svoje vnútroštátne posúdenia rizík Komisii a Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA) do 15. júla 2019.

10. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) by mala dokončiť špecifické mapovanie situácie v súvislosti s kybernetickými hrozbami pre siete 5G. Tento proces by mala podporovať skupina pre spoluprácu a sieť jednotiek pre riešenie počítačových bezpečnostných incidentov zriadená podľa smernice (EÚ) 2016/1148.

11. Pri zohľadnení všetkých týchto prvkov by členské štáty s podporou Komisie a spolu s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) mali do 1. októbra 2019 dokončiť spoločné preskúmanie vystavenia celej Únie rizikám súvisiacim s infraštruktúrami, ktoré tvoria základ digitálneho ekosystému, a najmä sietí 5G.

12. V rámci tohto spoločného preskúmania by sa mala uprednostniť analýza rizík, ktoré sa vzťahujú na mimoriadne citlivé alebo zraniteľné prvky obsiahnuté v hlavných prvkoch sietí 5G, na stredisko prevádzky a údržby, ako aj na prvky prístupovej siete 5G, ktoré sa používajú na priemyselné účely.

13. V druhej fáze by sa toto spoločné preskúmanie malo rozšíriť na ďalšie strategické prvky digitálneho hodnotového reťazca.

Spoločný súbor nástrojov Únie na riešenie rizík

14. Práca skupiny pre spoluprácu by mala identifikovať osvedčené postupy uplatňované na vnútroštátnej úrovni typu uvedeného v bode 4. Na základe týchto vnútroštátnych osvedčených postupov by sa do 31. decembra 2019 mal schváliť súbor vhodných, účinných a primeraných opatrení na riadenie prípadných rizík s cieľom zmierniť zistené riziká v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie, podľa ktorého by Komisia vypracovala minimálne spoločné požiadavky v záujme ďalšieho zaistenia vysokej úrovne kybernetickej bezpečnosti sietí 5G v celej Únii.

15. Tento súbor nástrojov by mal zahŕňať:

a) zoznam typov bezpečnostných rizík, ktoré môžu ovplyvniť kybernetickú bezpečnosť sietí 5G (napr. riziko dodávateľského reťazca, riziko zraniteľného softvéru, riziko v prípade kontroly prístupu, riziká vyplývajúce z právneho a politického rámca, ktorý sa môže vzťahovať na dodávateľov zariadení informačných a komunikačných technológií v tretích krajinách); a

b) súbor možných zmierňujúcich opatrení (napr. certifikácia hardvéru, softvéru alebo služieb uskutočnená treťou stranou, formálne hardvérové a softvérové testy alebo kontroly zhody, procesy na zabezpečenie existencie kontrol prístupu a ich presadzovanie, identifikovať výrobky, služby alebo dodávateľov, ktoré resp. ktorí sa považujú za potenciálne nie bezpečných atď.). Uvedené opatrenia by sa mali týkať každého typu bezpečnostného rizika zisteného v jednom alebo viacerých členských štátoch na základe posúdenia rizika.

16. Po vytvorení európskych systémov certifikácie kybernetickej bezpečnosti relevantných pre siete 5G by členské štáty mali v súlade s právom Únie prijať vnútroštátne technické predpisy stanovujúce povinnú certifikáciu výrobkov, služieb alebo systémov informačných a komunikačných technológií, na ktoré sa tieto systémy certifikácie vzťahujú.

17. Členské štáty by spolu s Komisiou mali určiť podmienky týkajúce sa bezpečnosti verejných sietí pred neoprávneným prístupom, ktoré sa majú pripojiť k všeobecnému povoleniu a požiadavkám týkajúcim sa bezpečnosti sietí, s cieľom získať záväzky od podnikov, ktoré sa zúčastňujú na postupoch udeľovania práv na využívanie frekvenčného spektra v pásmach 5G podľa smernice 2002/20/ES. Tie by sa mali podľa možnosti premietnuť do opatrení prijatých v bode 4 písm. c).

18. Členské štáty by mali s Komisiou spolupracovať na vypracovaní osobitných bezpečnostných požiadaviek, ktoré by sa mohli uplatňovať v rámci verejného obstarávania týkajúceho sa sietí 5G. To by malo zahŕňať povinné požiadavky na zavedenie systémov certifikácie kybernetickej bezpečnosti do verejného obstarávania, pokiaľ tieto systémy ešte nie sú pre všetkých dodávateľov a prevádzkovateľov záväzné.

V. **PRESKÚMANIE**

19. Členské štáty by mali s Komisiou spolupracovať na posúdení účinkov tohto odporúčania do 1. októbra 2020 s cieľom určiť vhodné spôsoby napredovania. V tomto posúdení by sa mal zohľadniť výsledok koordinovaného posúdenia rizík v Únii a súbor nástrojov Únie.

V Štrasburgu 26. marca 2019

Za Komisiu
Julian KING
Člen Komisie