

ODPOVEDE EURÓPSKEJ KOMISIE NA OSOBITNÚ SPRÁVU EURÓPSKEHO DVORA AUDÍTOROV:

„ZAVÁDZANIE SIETÍ 5G V EÚ: ONESKORENIE V ZAVÁDZANÍ SIETÍ, PRIČOM BEZPEČNOSTNÉ OTÁZKY ZOSTÁVAJÚ NEVYRIEŠENÉ“

ZHRNUTIE

Úvodné pripomienky Komisie

I. Zavádzanie sietí 5G rýchlym a bezpečným spôsobom je hlavnou prioritou Európskej komisie. Ochrana sietí 5G pred kybernetickými hrozbami sa zakladá na posudzovaní a zmiernení hrozieb a rizík. Tieto hrozby a riziká spoločne identifikovali a posúdili členské štáty s podporou Komisie a agentúry ENISA a na tomto základe sa určil súbor komplexných opatrení na zmiernenie týchto rizík. Hoci sa v niektorých členských štátoch ešte stále pokračuje v práci, veľká väčšina členských štátov už sprísnila bezpečnostné požiadavky týkajúce sa sietí 5G na základe súboru nástrojov EÚ alebo ich práve sprísňuje.

Súbor nástrojov EÚ bol uznaný ako komplexný rámec na riešenie bezpečnostných rizík sietí 5G.

Koordinovaný postup v oblasti kybernetickej bezpečnosti sietí 5G na úrovni EÚ a súbor nástrojov EÚ zapadajú do širšieho európskeho rámca na ochranu elektronických komunikačných sietí a iných kritických infraštruktúr a dopĺňajú existujúce opatrenia, ako je európsky kódex elektronických komunikácií, telekomunikačný rámec, akt o kybernetickej bezpečnosti a smernica o sieťovej a informačnej bezpečnosti (smernica NIS) a prípadne pravidlá voľného pohybu stanovené v zmluve a Charte základných práv Európskej únie.

III. Siete 5G budú v nasledujúcich rokoch zohrávať kľúčovú úlohu v našom digitálnom hospodárstve a spoločnosti. Musíme zabezpečiť, aby siete 5G boli kyberneticky bezpečné a odolné proti rastúcim kybernetickým hrozbám a incidentom. Preto Komisia a členské štáty zaviedli koordinačný proces zameraný na vymedzenie a vykonávanie komplexného rámca pre bezpečnosť sietí 5G vo forme súboru nástrojov opatrení na zmiernenie rizika, ktoré boli dohodnuté v januári 2020, s cieľom koordinovaným spôsobom účinne riešiť hlavné riziká pre siete 5G, ako je hackerstvo, špionáž a sabotáž. Hoci sa v niektorých členských štátoch ešte stále pokračuje v práci, veľká väčšina členských štátov už sprísnila bezpečnostné požiadavky týkajúce sa sietí 5G na základe súboru nástrojov EÚ alebo ich práve sprísňuje.

VII. Súbor nástrojov EÚ poskytuje rámec na podporu konzistentnosti na vnútornom trhu, pričom sa rešpektujú právomoci v oblasti národnej bezpečnosti v tejto oblasti.

Pokiaľ ide o prístup členských štátov k vysoko rizikovým predajcom, Komisia sa domnieva, že konečné posúdenie bude možné vykonať len vtedy, keď bude k dispozícii viac informácií.

Zatiaľ čo prebieha vykonávanie, Komisia spolupracuje s členskými štátmi v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti s cieľom podporiť zosúladenie a konvergenciu v súvislosti s vnútroštátnymi prístupmi.

IX. Prvá zarážka – Komisia prijíma odporúčanie.

Druhá zarážka – Komisia prijíma odporúčanie.

Tretia zarážka – Komisia prijíma odporúčanie.

Komisia vykoná posúdenie s prihliadnutím na vnútroštátne právomoci.

ÚVOD

04. Komisia uznáva existenciu bezpečnostných rizík sietí 5G, poukazuje však na to, že sieťové technológie a normy 5G môžu priniesť aj zlepšenie bezpečnosti v porovnaní s predchádzajúcimi generáciami sietí.

PRIPOMIENKY

30. Zatiaľ čo siete 4G sa už môžu zaoberať širokou škálou služieb, siete 5G by mali predstavovať značný skok dopredu, čo je veľká zmena v porovnaní so 4G, takže hlavnou výzvou je prechod zo 4G na 5G a zavádzanie 5G v celej EÚ. Riziko vzniku digitálnej priepasti stále existuje, ale v rámci politického programu Cesta k digitálnemu desaťročiu sa toto riziko plánuje riešiť ako politická priorita, a to vo vzťahu k trajektóriám, ktoré vedú k splneniu cieľa v oblasti sietí 5G, ktorým je dosiahnutie 100 % pokrytia všetkých obývaných oblastí do roku 2030, čím sa podpora členské štáty, aby prijali opatrenia v tejto oblasti, najmä pokiaľ ide o prístup vo vidieckych oblastiach.

32. Stredisko pre monitorovanie 5G bolo spoľahlivým zdrojom na monitorovanie zavádzania sietí 5G v EÚ a mimo nej, aj keď sa vyskytli určité nedostatky. Útvary Komisie očakávajú, že vzhľadom na nového dodávateľa budú k dispozícii aktuálnejšie informácie.

Spoločná odpoveď Komisie na body 48 a 49:

Komisia považuje výber nástroja (odporúčanie) a prístup založený na spolupráci s členskými štátmi na identifikáciu rizík a zmierňujúcich opatrení za najvhodnejší postup na riešenie bezpečnostných rizík sietí 5G rýchlym, účinným a zosúladeným spôsobom.

Komisia sa rozhodla pre odporúčanie a pre spoluprácu s členskými štátmi pri identifikácii rizík a zmierňujúcich opatrení vzhľadom na zložitosť a prierezový charakter tejto témy v rámci vnútroštátnych právomocí a právomocí EÚ a významný rozmer národnej bezpečnosti. Komisia okrem toho zohľadnila aj skutočnosť, že členské štáty majú veľmi odlišný vnútroštátny kontext (štruktúra trhu, spôsobilosti v oblasti kybernetickej bezpečnosti, spravodajské informácie o hrozbách atď.).

Súbor nástrojov EÚ predstavuje pohotový nástroj založený na riziku s cieľom riešiť bezpečnostné výzvy, ktorý umožnil včas a efektívne riešiť aspekty kybernetickej bezpečnosti 5G.

Komisia vo svojom oznámení „Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov“ z januára 2020 oznámila, že poskytne podporu vykonávania opatrení súboru nástrojov súvisiacich s bezpečnostnými požiadavkami, najmä pokiaľ ide o príslušné ustanovenia európskych pravidiel v oblasti elektronických komunikácií, a zohľadní pridanú hodnotu možných vykonávacích aktov, v ktorých sa podrobne uvádzajú technické a organizačné bezpečnostné opatrenia, s cieľom doplniť vnútroštátne predpisy a zvýšiť účinnosť a konzistentnosť bezpečnostných opatrení uložených prevádzkovateľom.

Spoločná odpoveď Komisie na body 51 a 52:

V súvislosti s preskúmaním odporúčania Komisie, ktoré sa uskutočnilo v decembri 2020, Komisia uskutočnila rozhovory s príslušnými orgánmi všetkých členských štátov. Koordinovanú činnosť Európy v oblasti kybernetickej bezpečnosti 5G kvalifikovali ako včasnú, účinnú a primeranú. Prístup založený na spolupráci medzi vnútroštátnymi orgánmi, Komisiou, agentúrou ENISA a ďalšími príslušnými zainteresovanými stranami sa považoval za vhodný na riešenie tejto zložitej otázky. Umožnil včasné vymedzenie spoločných cieľov a metodík a zároveň umožnil členským štátom prispôbiť opatrenia svojim vnútroštátnym okolnostiam.

V súbore nástrojov EÚ a v správe o pokroku, ktorú uverejnila skupina pre spoluprácu v oblasti kybernetickej bezpečnosti v júli 2020, sa odporúča vymedziť plány vykonávania a/alebo prechodné obdobia pre tých prevádzkovateľov, ktorí v súčasnosti používajú zariadenia vysoko rizikových dodávateľov alebo ktorí už uzavreli zmluvy s vysoko rizikovými dodávateľmi pred prijatím súboru nástrojov EÚ (napr. zohľadnením cyklov modernizácie zariadení, najmä migrácie sietí 5G od „nie nezávislých“ po „nezávislé“).

55. Komisia berie na vedomie pripomienky Európskeho dvora audítorov.

S cieľom ďalej podporiť ich vykonávanie boli kritériá súboru nástrojov na posudzovanie vysoko rizikových dodávateľov predmetom početných výmen medzi príslušnými vnútroštátnymi orgánmi v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti, a to od schválenia súboru nástrojov EÚ.

56. Súborom nástrojov EÚ sa odporúča, aby sa pri posudzovaní rizikového profilu dodávateľov zohľadnili rizikové faktory uvedené v koordinovanom posúdení rizík na úrovni EÚ, ako aj informácie týkajúce sa jednotlivých krajín (napr. posúdenie hrozieb zo strany vnútroštátnych bezpečnostných služieb atď.).

61. Schopnosť dodávateľa zaistiť dodávky je jedným z kritérií odporúčaných súborom nástrojov EÚ na posúdenie rizikového profilu dodávateľov. Schopnosť zaistiť dodávky by mohla byť ovplyvnená aj možnými obchodnými sankciami, ktorým čelí konkrétny predajca, ako sa uvádza v rizikovom scenári o „závislosti“ v koordinovanom posúdení rizík na úrovni EÚ.

Spoločná odpoveď Komisie na body 70 a 73:

Komisia a členské štáty si vymieňajú podrobné informácie o vykonávaní súboru nástrojov na vnútroštátnej úrovni v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti. Pokiaľ ide o zverejňovanie neverejných informácií, sú zaň zodpovedné členské štáty.

Spoločná odpoveď Komisie na body 74 až 76 a rámček 5:

Súbor nástrojov EÚ poskytuje rámec na podporu konzistentnosti na vnútornom trhu, pričom sa rešpektujú právomoci v oblasti národnej bezpečnosti v tejto oblasti.

Pokiaľ ide o prístup členských štátov k vysoko rizikovým predajcom, Komisia sa domnieva, že konečné posúdenie bude možné vykonať len vtedy, keď bude k dispozícii viac informácií.

Zatiaľ čo prebieha vykonávanie, Komisia spolupracuje s členskými štátmi v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti s cieľom podporiť zosúladienie a konvergenciu v súvislosti s vnútroštátnymi prístupmi.

ZÁVERY A ODPORÚČANIA

81. Zavádzanie sietí 5G rýchlym a bezpečným spôsobom je pre Komisiu hlavnou prioritou. Ochrana sietí 5G pred kybernetickými hrozbami sa zakladá na posudzovaní a zmiernovaní hrozieb a rizík. Tieto hrozby a riziká spoločne identifikovali a posúdili členské štáty s podporou Komisie a agentúry ENISA a na tomto základe sa určil súbor komplexných opatrení na zmiernenie týchto rizík. Hoci sa v niektorých členských štátoch ešte stále pokračuje v práci, veľká väčšina členských štátov už sprísnila bezpečnostné požiadavky týkajúce sa sietí 5G na základe súboru nástrojov EÚ alebo ich práve sprísňuje.

Súbor nástrojov EÚ poskytuje komplexný rámec na riešenie bezpečnostných rizík sietí 5G.

83. Siete 5G predstavujú značný skok dopredu, čo je veľká zmena v porovnaní so 4G, takže hlavnou výzvou na zabránenie vzniku digitálnej priepasti je prechod zo 4G na 5G v celej EÚ.

Špecifikácie 5G sa vzťahujú na celú škálu ukazovateľov výkonnosti, najmä pokiaľ ide o vertikálne prípady použitia. To môže okrem iného zahŕňať požiadavky na spoľahlivosť, rýchlosť okamžitej prevádzky, flexibilitu vykonávania, úroveň bezpečnosti.

Odporúčanie 1 – Presadzovať rovnomerné a včasné zavádzanie sietí 5G v rámci EÚ

a) Komisia prijíma odporúčanie.

Komisia spolupracuje s členskými štátmi na vypracovaní spoločného vymedzenia očakávanej kvality služieb sietí 5G. V kontexte digitálneho desaťročia a navrhovaného rozhodnutia o programe digitálnej

politiky do roku 2030 má Komisia v úmysle spolupracovať s členskými štátmi na spoločnom prístupe ku kvalite služieb 5G v EÚ vrátane porovnateľnosti meraní a údajov z monitorovania.

Kvalita služieb sa nevzťahuje len na rýchlosť a oneskorenie, ale zahŕňa celú škálu ukazovateľov výkonnosti, najmä pokiaľ ide o vertikálne prípady použitia.

Komisia má v úmysle spolupracovať s členskými štátmi s cieľom vymedziť takéto merania, ako aj vykonávať ročné kontroly a odporúčať politiky, opatrenia a činnosti na dosiahnutie plného pokrytia sieťami 5G do roku 2030.

V rámci programu digitálnej politiky sa vytvorí spoľahlivé riadenie prostredníctvom mechanizmu monitorovania a spolupráce, aby sa zabezpečil pokrok pri plnení cieľov stanovených v politickom programe vrátane zavádzania sietí 5G a v tejto súvislosti sa členským štátom odporúča nápravné opatrenia.

b) Komisia prijíma odporúčanie.

c) Komisia prijíma odporúčanie.

Odporúčanie 2 – Podporovať zosúladený prístup členských štátov k bezpečnosti sietí 5G

a) Komisia prijíma odporúčanie.

Komisia spolu s členskými štátmi posúdi potrebu ďalších činností alebo podpory, a to napríklad vo forme usmernení týkajúcich sa určitých aspektov súboru nástrojov EÚ.

b) Komisia prijíma odporúčanie.

Monitorovanie a podávanie správ bude vykonávať Komisia v úzkej spolupráci s členskými štátmi a agentúrou ENISA.

c) Komisia prijíma odporúčanie.

Odporúčanie 3 – Monitorovať prístupy členských štátov k bezpečnosti sietí 5G a posúdiť vplyv rozdielov na účinné fungovanie jednotného trhu

a) Komisia prijíma odporúčanie.

b) Komisia prijíma odporúčanie.

Komisia vykoná posúdenie s prihliadnutím na vnútroštátne právomoci.

V rámci súboru nástrojov EÚ je na členských štátoch, aby rozhodli o presnom rozsahu príslušných reštrikcií a/alebo nevyhnutných vylúčení kľúčových aktív, ktoré sú v koordinovanom posúdení rizík na úrovni EÚ vymedzené ako kritické a citlivé (napr. funkcie jadrovej siete, funkcie riadenia a organizácie siete a funkcie prístupu k sieti), s cieľom účinne zmierniť identifikované riziká, a to aj pri zohľadnení posúdenia hrozieb zo strany vnútroštátnych spravodajských služieb. Členské štáty majú právo prijať opatrenia týkajúce sa národnej bezpečnosti vrátane možných reštrikcií alebo vylúčení vysoko rizikových predajcov.

SK

SK