Európska komisia

SÚBOR NÁSTROJOV EÚ PRE BEZPEČNOSŤ 5G

SÚBOR SPOĽAHLIVÝCH A KOMPLEXNÝCH OPATRENÍ PRE KOORDINOVANÝ PRÍSTUP EÚ K BEZPEČNÝM SIEŤAM 5G

marec 2021
#Cybersecurity

5G: nová technológia

Siete 3G nám priniesli mobilné pripojenie na internet a 4G zasa mobilné širokopásmové pripojenie. Od 5G sa očakáva, že ako prepojovacia infraštruktúra otvorí cestu novým produktom a službám a ovplyvní všetky zložky spoločnosti. Bude medzi ne patriť:

ELEKTRONICKÉ ZDRAVOTNÍCTVO

- diaľkové monitorovanie zdravia, záznamy pacientov a inteligentná diagnostika
- využívanie robotov na pomoc chirurgom a skvalitnenie liečebných výsledkov

INTELIGENTNÉ SIETE

- vysokoúčinné elektrické vedenia a zriedkavejšie, menšie výpadky
- jednoduchšie zavádzanie s nižším vplyvom na životné prostredie

TOVÁRNE BUDÚCNOSTI

- lepšie riadenie urgentných vnútorných procesov
- diaľkový prístup ku strojovým zariadeniam

MÉDIÁ A ZÁBAVA

- intenzívnejší zážitok pri zobrazovaní, ako je napr. virtuálna realita
- ultrarýchle aplikácie s vysokou šírkou pásma, napr. pri videoprenose

MOBILITA

- prepojená a automatizovaná mobilita v záujme nulovej nehodovosti
- umožnenie prepojenia vo všetkých druhoch dopravy

Európa je najvyspelejším regiónom pokiaľ ide o rozsiahle zavádzanie 5G vo vertikálnych odvetviach (do ktorých sa do konca roka 2020 investovala takmer 1 miliarda EUR), vrátane dopravných koridorov 5G. Na konci roka 2020 boli služby 5G k dispozícii v 500 európskych mestách.

Kybernetická bezpečnosť 5G: nevyhnutný predpoklad

Siete 5G budú tvoriť kostru našich čoraz digitalizovanejších hospodárstiev a spoločnosti. Týkajú sa miliárd pripojených predmetov a systémov vrátane tých, ktoré sa používajú v kritických sektoroch, ako je energetika, doprava, bankovníctvo či zdravotníctvo, a tých, ktoré sa používajú v systémoch priemyselnej kontroly a ktoré obsahujú citlivé informácie a podporujú bezpečnostné systémy. Zaistenie kybernetickej bezpečnosti a odolnosti sietí 5G je preto nevyhnutné.

Siete 5G však zároveň ponúkajú viac potenciálnych vstupných miest pre útočníkov – okrem iného z dôvodu menej centralizovanej architektúry, výpočtovej sily špičkovej inteligencie, potreby väčšieho počtu antén a zvýšenej závislosti od softvéru.

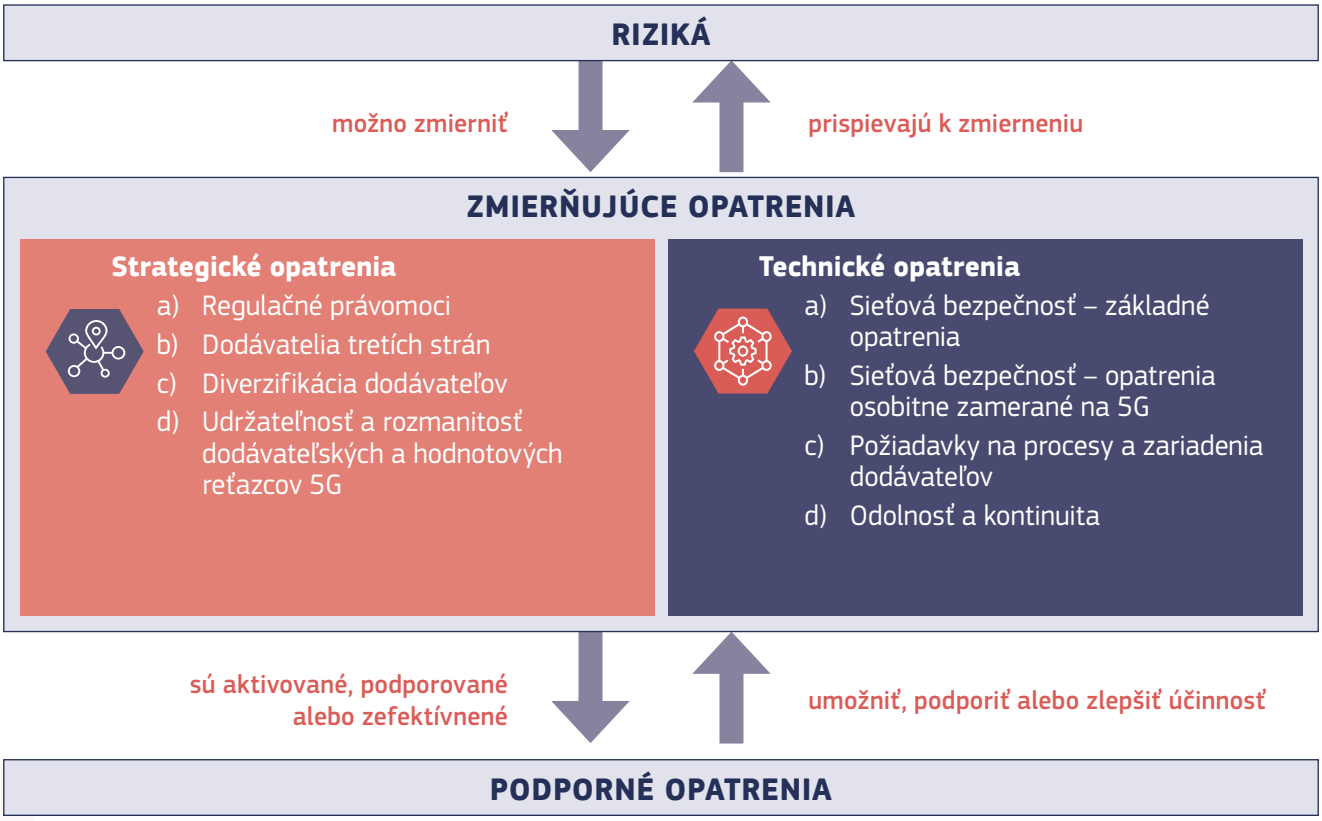
Celoúnijné posúdenie rizík: scenáre rizík

Celoúnijné koordinované posúdenie rizík týkajúce sa bezpečnosti sietí 5G identifikuje deväť hlavných rizík zoskupených do piatich rizikových scenárov.

I – Scenáre rizika týkajúce sa nedostatočných bezpečnostných opatrení	R1 – Nesprávna konfigurácia sietí R2 – Chýbajúce kontroly prístupu
II – Scenáre rizika týkajúce sa dodávateľského reťazca 5G	R3 – Nízka kvalita produktu R4 – Závislosť od akéhokoľvek jediného dodávateľa v rámci jednotlivých sietí alebo nedostatočná rozmanitosť na celoštátnej úrovni
III – Scenáre rizika týkajúce sa spôsobu práce hlavných útočníkov	R5 – Zasahovanie štátu cez dodávateľský reťazec 5G R6 – Využívanie sietí 5G na organizovanú trestnú činnosť alebo zameranie sa na koncových používateľov
IV – Scenáre rizika týkajúce sa vzájomnej závislosti medzi sieťami 5G a inými kritickými systémami	R7 – Závažné narušenie kritickej infraštruktúry alebo služieb R8 – Hromadné zlyhanie sietí v dôsledku prerušenia dodávok elektrickej energie alebo iných podporných systémov
V – Scenáre rizika týkajúce sa zariadení koncového používateľa	R9 – Využívanie internetu vecí, bezdrôtových mikrotelefónov alebo inteligentných zariadení

Súbor nástrojov EÚ pre bezpečnosť 5G

Na základe koordinovaného posúdenia rizík zo strany EÚ, pokiaľ ide o bezpečnosť sietí 5G, sa v súbore nástrojov stanovuje celá škála bezpečnostných opatrení, ktorých cieľom je účinne zmierňovať riziká a zaručiť zavádzanie bezpečných 5G sietí v celej Európe. Uvádzajú sa v ňom podrobné **plány na zmiernenie** každej z identifikovaných hrozieb a odporúča sa súbor **kľúčových strategických a technických opatrení**, ktoré by mali prijať všetky členské štáty a/alebo Komisia.



Závery o súbore nástrojov EÚ: kľúčové opatrenia

Členské štáty by mali mať zavedené opatrenia a právomoci na zmiernenie rizík. Predovšetkým by mali:

- posilniť **bezpečnostné požiadavky** na **prevádzkovateľov mobilných sietí**,
- posúdiť rizikový profil dodávateľov a uplatňovať príslušné **obmedzenia na dodávateľov, ktorí sa považujú za vysokorizikových**, vrátane vylúčenia kľúčových aktív,
- zabezpečiť, aby každý prevádzkovateľ mal primeranú **stratégiu viacerých dodávateľov** s cieľom **vyhnúť sa** akejkoľvek **väčšej závislosti** od jedného dodávateľa alebo ju **minimalizovať** a zabrániť závislosti od dodávateľov, ktorí sa považujú za vysokorizikových.

Európska komisia spolu s členskými štátmi by mali prijať opatrenia na:

- zachovanie **rôznorodého** a **udržateľného dodávateľského reťazca 5G** s cieľom zabrániť dlhodobej závislosti, a to aj:
  - využitím existujúcich nástrojov EÚ (preverovanie priamych zahraničných investícií, nástroje na ochranu obchodu, hospodárska súťaž),
  - ďalším posilnením kapacít EÚ v oblasti technológií 5G a budúcich generácií s využitím príslušných programov a financovania EÚ,
- uľahčením koordinácie medzi členskými štátmi, pokiaľ ide o **normalizáciu**, s cieľom dosiahnuť konkrétne bezpečnostné ciele a rozvíjať príslušné **systémy certifikácie** v celej EÚ.

Okrem toho by sa mal rozšíriť **mandát skupiny pre spoluprácu v oblasti sietí a informačných systémov** o podporu, monitorovanie a hodnotenie vykonávania súboru nástrojov.

Plány na zmiernenie rizík – príklady opatrení súboru nástrojov

V súbore nástrojov sa identifikujú plány na zmiernenie rizík v prípade každej z deviatich rizikových oblastí opísaných v správe EÚ o koordinovanom posúdení rizík. Pozostávajú z možných kombinácií opatrení v závislosti od ich účinnosti.

Súbor nástrojov poskytuje usmernenia týkajúce sa objektívnych kritérií vrátane technických a netechnických rizikových faktorov, s cieľom posúdiť rizikový profil dodávateľov, t. j. riziko interferencie z krajiny mimo EÚ, schopnosť dodávať a postupy kybernetickej bezpečnosti.

SM03	**Posudzovanie rizikového profilu dodávateľov a uplatňovanie obmedzení pre dodávateľov, ktorí sa považujú za vysokorizikových – vrátane potrebných výnimiek v záujme účinného zmiernenia rizík – v prípade kľúčových aktív**	Pre vnútroštátne príslušné orgány a prevádzkovateľov mobilných sietí vytvoriť rámec s jednoznačnými kritériami pri zohľadnení rizikových faktorov uvedených v odseku 2.37 koordinovaného posúdenia rizík na úrovni EÚ a s doplnením informácií špecifických pre danú krajinu (napríklad posúdenie hrozieb vnútroštátnymi bezpečnostnými službami) s cieľom: – vykonávať prísne posudzovanie rizikových profilov všetkých relevantných dodávateľov na vnútroštátnej úrovni a/alebo na úrovni EÚ (napríklad spoločne s inými členskými štátmi alebo inými prevádzkovateľmi mobilných sietí), – na základe posúdenia rizikového profilu uplatňovať obmedzenia – vrátane potrebných výnimiek v záujme účinného zmiernenia rizík – v prípade kľúčových aktív vymedzených v správe o koordinovanom posúdení rizík na úrovni EÚ ako kritické alebo citlivé (napríklad funkcie jadrovej siete, funkcie sieťového riadenia a zosúladenia a funkcie prístupovej siete), – vykonať kroky na zabezpečenie toho, aby prevádzkovatelia mobilných sietí mali zavedené primerané kontroly a postupy riadenia potenciálnych zvyškových rizík, ako sú napríklad pravidelné audity a posúdenia rizík dodávateľského reťazca, prísne riadenie rizík a/alebo osobitné požiadavky na dodávateľov na základe ich rizikových profilov.

Súbor nástrojov poskytuje usmernenia týkajúce sa citlivosti sieťových prvkov a funkcií.

TM03	**Zabezpečenie prísnych kontrol prístupu**	Zabezpečiť, aby prevádzkovatelia mobilných sietí uplatňovali primerané, pružné a overiteľné technické opatrenia na zaistenie: – uplatňovania prísnych kontrol prístupu k sieti, – uplatňovania zásady minimálnych práv, čo zabezpečuje, že rôzne práva v sieti (napríklad práva prístupu medzi funkciami siete, práva správcov siete, konfigurácia virtualizácie) sú minimalizované, – uplatňovania zásady oddelenia funkcií, – zavedenia postupov na zabezpečenie toho, aby tieto pravidlá boli stále účinné a vyvíjali sa so sieťou. Pri stanovení politík kontroly prístupu by sa mala osobitná pozornosť venovať zabezpečeniu toho, aby vzdialený prístup tretích strán, predovšetkým dodávateľov, ktorí sa považujú za vysokorizikových, bol minimalizovaný a/alebo zamedzený, kedykoľvek je to možné. Keď je vzdialený prístup potrebný, napríklad na riešenie prevádzkových výpadkov, prevádzkovateľ mobilnej siete by mal uplatniť primerané overovanie, autorizáciu, vedenie záznamov a vykonávanie auditu, aby bol jasne viditeľný prístup k údajom a zmeny konfigurácie alebo zmeny siete.

Harmonogram politiky EÚ v oblasti kybernetickej bezpečnosti 5G

22. marca 2019
Závery Európskej rady

26. marca 2019
Európska komisia uverejnila **odporúčanie** pre členské štáty, aby prijali konkrétne kroky v záujme posúdenia kyberneticko-bezpečnostných rizík sietí 5G a posilnenia opatrení na zníženie rizík.

9. októbra 2019
Členské štáty dokončili celoúnijné koordinované posúdenie rizík týkajúce sa bezpečnosti sietí 5G.

21. novembra 2019
Agentúra EÚ pre kybernetickú bezpečnosť uverejnila rozsiahlu správu o hrozbách súvisiacich so sieťami 5G.

29. januára 2020
Členské štáty uverejnili súbor zmierňujúcich opatrení. Oznámenie Komisie o vykonávaní súboru nástrojov EÚ [COM(2020) 50 final z 29. januára 2020].

júl 2020
Správa o pokroku pri vykonávaní súboru nástrojov

október 2020
Európska rada vyzvala EÚ a členské štáty, aby „v plnej miere využívali súbor nástrojov pre kybernetickú bezpečnosť 5G“ a „uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov v prípade kľúčových aktív.“

december 2020
Nová stratégia kybernetickej bezpečnosti EÚ a **Správa** o vplyve odporúčania Komisie na kybernetickú bezpečnosť sietí 5G

Do júna 2021
Komisia vyzýva členské štáty, aby **dokončili vykonávanie hlavných opatrení súboru nástrojov**

Ďalšie kroky (v rámci Stratégie kybernetickej bezpečnosti EÚ pre digitálne desaťročie)

- Dokončiť vykonávanie hlavných opatrení súboru nástrojov do druhého štvrťroka 2021.
- Zabezpečiť, aby sa identifikované riziká koordinovaným spôsobom primerane zmiernili, najmä s cieľom minimalizovať vystavenie vysokorizikovým dodávateľom a zabrániť závislosti od týchto dodávateľov na vnútroštátnej úrovni aj na úrovni EÚ.
- Pokračovať v prehlbovaní koordinácie na úrovni EÚ so zameraním na kľúčové ciele:

1. Zabezpečenie konvergentných národných prístupov k účinnému zmierňovaniu rizík v celej EÚ

2. Podpora nepretržitej výmeny znalostí a budovania kapacít

3. Podpora odolnosti dodávateľského reťazca a iných bezpečnostných strategických cieľov EÚ

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021

Úrad pre vydávanie publikácií Európskej únie

Print ISBN 978-92-76-37758-0 doi:10.2759/90646 KK-02-21-626-SK-C
PDF ISBN 978-92-76-37736-8 doi:10.2759/664193 KK-02-21-626-SK-N

2021-05-25