



SÚBOR NÁSTROJOV EÚ PRE BEZPEČNOSŤ 5G

Súbor spolaahlivých a komplexných opatrení pre
koordinovaný prístup EÚ k bezpečným sieťam 5G

Január 2020
#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. Medzi prínosy bude patriť:



ELEKTRONICKÉ ZDRAVOTNÍCTVO

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



INTELEKTUÁLNE 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 z hľadiska komerčného zavádzania služieb 5G medzi najpokročilejšími regiónmi sveta. Do tohto úsilia sa investovala 1 miliarda eur vrátane 300 miliónov eur z finančných prostriedkov EÚ. Očakáva sa, že do konca roka budú prvé služby 5G k dispozícii v 138 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.

Časový rámec



26. marca
2019

Správa
Európskeho
parlamentu.



22. marca
2019

Závery
Európskej rady.



26. marca
2019

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 celounijné koordinované posúdenie rizík týkajúce sa bezpečnosti sietí 5G.



21. novembra
2019

Agentúra EÚ pre kybernetickú bezpečnosť ENISA 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.



30. apríla
2020

Komisia vyzýva členské štáty, aby prijali prvé konkrétne a merateľné kroky na realizáciu kľúčových opatrení.



30. júna
2020

Komisia vyzýva členské štáty, aby vypracovali správu o vykonávaní kľúčových opatrení.



do októbra
2020

Preskúmanie odporúčaní Komisie prijatého 26. marca 2019.

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, ktoré umožnia účinne zmiernovať riziká a zaručia zavádzanie bezpečných 5G sietí v celej Európe. Uvádzajú sa v ňom podrobné **plány na zmiernenie** každej z identifikovaných hrozieb a odporúča sa súbor **klúčových strategických a technických opatrení**, ktoré by mali prijať všetky členské štáty a/alebo Komisia.



STRATEGICKÉ OPATRENIA

- regulačné právomoci
- dodávatelia – tretie strany
- diverzifikácia dodávateľov
- udržateľnosť a rozmanitosť dodávateľských a hodnotových reťazcov 5G



TECHNICKÉ OPATRENIA

- sieťová bezpečnosť – základné opatrenia
- sieťová bezpečnosť – opatrenia osobitne zamerané na 5G
- požiadavky na procesy a zariadenia dodávateľov
- odolnosť a kontinuita

Plány na zmiernenie rizík

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

Závery súboru nástrojov EÚ: klúčové opatrenia

Členské štáty: mali by mať zavedené opatrenia a právomoci na zmiernenie rizík. Mali by sa zamerať najmä na tieto aspekty:

- posilniť **bezpečnostné požiadavky na prevádzkovateľov mobilných sietí**,
- posúdiť rizikový profil dodávateľov a uplatňovať príslušné obmedzenia na dodávateľov, ktorí sa považujú za vysokorizikových, vrátane vylúčenia klúčových aktív, ak je to potrebné,
- 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 PZI, nástroje na ochranu obchodu, hospodárska súťaž),
 - ďalším posilnením kapacít EÚ v oblasti technológií 5G a budúcich generácií s využitím príslušných programov a financovania EÚ,
- uľahčenie koordinácie medzi členskými štátmi, pokiaľ ide o **normalizáciu**, s cieľom dosiahnuť konkrétne bezpečnostné ciele a rozvíjať príslušné **systemy certifikácie** v celej EÚ.

Okrem toho by sa mal rozšíriť mandát **skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti** o podporu, monitorovanie a hodnotenie vykonávania súboru nástrojov.

© Európska únia, 2020

Reprodukcia je povolená len pod podmienkou uvedenia zdroja. Pravidlá na opakované použitie dokumentov Európskej komisie sa riadia rozhodnutím 2011/833/EÚ (Ú. v. EÚ L 330, 14.12.2011, s. 39). Na akékoľvek použitie alebo reprodukciu prvkov, ktoré nie sú vo vlastníctve Európskej únie, môže byť potrebné získať povolenie priamo od príslušných nositeľov práv.

Pokiaľ sa neuvádza inak, všetky obrázky © Európska únia.

Print ISBN 978-92-76-15576-8 doi:10.2775/964572 NA-03-20-052-SK-C
PDF ISBN 978-92-76-15573-7 doi:10.2775/367105 NA-03-20-052-SK-N