ENISA: 5G design a architektura globálních mobilních sítí; hrozby, rizika, zranitelná místa, aspekty kybernetické bezpečnosti – Duben 2023

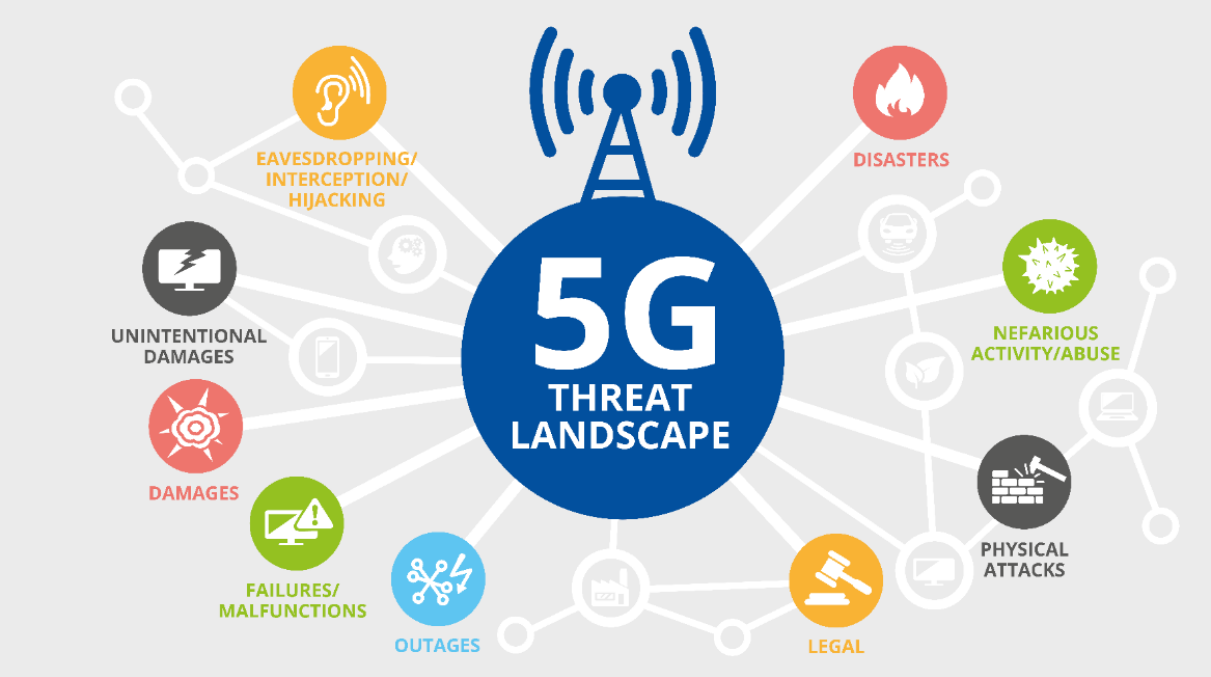
Autor: Evropská komise a Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

Zdroj: Článek Evropské komise (Březen 2023) a

Zpráva ENISA k bezpečnosti 5G sítí (Prosinec 2020)

Souhrn

Evropská Komise (dále jen „EK“) formu odborného článku komentuje materiál Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) z roku 2020, vydaný pod názvem „Krajina hrozeb pro sítě 5G-aktualizované hodnocení hrozeb pro pátou generaci mobilních telekomunikačních sítí.“



Rámec 5G, prosazovaný ENISA je ve své komplexní zprávě jedinečný ve vztahu k rozsáhlé literatuře spojené s doménou 5G a roztříštěnému charakteru vědeckých zpráv souvisejících s technologií 5G.

Role agentury ENISA v Evropské Unii (dále jen „EU“) jako lídra v určování tempa rozvoje sítí 5G je uznávána v legislativě EU a jejích směrnicích. Je důležité, že jeho strategické směřování se zaměřuje na budoucí implementace sítí 5G ze strany prodejců, operátorů a praktiků. To by mělo EU vybavit nezbytnou odolností, aby odolala náporům hybridních hrozeb na její panevropskou síť.

ENISA vyniká mezi ostatními předními hráči v aréně 5G, protože učinila strategické rozhodnutí integrovat aspekty kybernetické bezpečnosti s hrozbami, riziky a zranitelností do architektury 5G hned od začátku proces návrhu a vývoje. 5G je komunikační standard páté generace mobilních telefonů. Jedná se o nástupce 4G, který bude rychlejší než předchozí generace

ENISA spolu s EK také portfolio nástrojů a souvisejících dokumentů souvisejících s opatřeními ke zmírnění rizik, které mohou odborníci použít na konkrétní zranitelná místa za účelem zvýšení odolnosti proti nechtěným hrozbám.

Národní a mezinárodní normalizační organizace přistupují ke svým příslušným úkolům nespojitým způsobem a řeší specifické normy ve velmi úzkém kontextu, a tak se stávají obětí zaostávání za důležitou prací, kterou vykonaly globální iniciativy, jako je 3GPP/SA3 a její průmysloví partneři. které tak dramaticky ovlivnily úsilí ENISA.

Hlavní struktura rámce ENISA se skládá z osmi hlavních aktiv: řízení a organizace, síťové produkty, organizace, procesy, služby, propojení, data a protokoly.

Strategické směřování agentury ENISA se jasně projevuje v široké škále právních předpisů, směrnic a zpráv o kybernetické bezpečnosti vydávaných Evropskou unií (EU) a/nebo Evropskou komisí (EK), včetně komplexní strategie kybernetické bezpečnosti.

Role ENISA v EU a ES je jednoznačně definována v zákoně o kybernetické bezpečnosti z roku 2017 (13), a to takto:

„Agentura by měla být Komisi nápomocna prostřednictvím poradenství, stanovisek a analýz týkajících se všech záležitostí Unie souvisejících s rozvojem politiky a práva, aktualizací a přezkumem v oblasti kybernetické bezpečnosti, včetně ochrany kritické infrastruktury a kybernetické odolnosti. Agentura by měla působit jako referenční bod pro poradenství a odborné znalosti pro odvětvové politické a právní iniciativy Unie, pokud jde o záležitosti související s kybernetickou bezpečností.“

Zákon o kybernetické bezpečnosti navíc v roce 2019 udělil agentuře ENISA trvalý mandát s dalšími zdroji a uložil jí nové úkoly pro její operace, včetně vytvoření rámce pro certifikaci kybernetické bezpečnosti. V červnu 2021 agentura zřídila místní kancelář v Bruselu, která ji začala více zviditelňovat u EU a ES, protože od roku 2004 má ENISA sídlo v Aténách. Jejím mandátem v Bruselu je udržovat pravidelnou a systematickou spolupráci s unijními institucemi a agenturami, jako je Evropská služba pro vnější činnost, Europol a Evropská obranná agentura a další subjekty zapojené do kybernetické bezpečnosti. Plány například zahrnují další rozvoj společné kybernetické jednotky jako virtuální platforma nástrojů pro kybernetickou bezpečnost a fyzická platforma postavená na agenturách ENISA a Computer Emergency Response Team (CERT-EU) přilehlých kancelářích v Bruselu. Cílem jednotky je posílit spolupráci mezi institucemi EU, agenturami a různými orgány v členských státech.

Pokud jde o nově vytvořené Evropské centrum kybernetické kompetence (ECCC) a síť, jejímž cílem je posílit kapacitu a konkurenceschopnost EU v oblasti kybernetické bezpečnosti, ENISA rozšiřuje aktivity mimo své koridory, aby se prostřednictvím svého výkonného ředitele zapojila do správní rady ECCC.

Role agentury ENISA v kybernetické bezpečnosti je dále posílena nedávnou formulací obsaženou v NIS 2 (prosinec 2020), významné směrnici Evropského parlamentu, která nastiňuje opatření pro vysokou úroveň bezpečnosti síťových a informačních systémů v celé Unii a která se zasazuje o systémové a strukturální změny směrnice NIS z roku 2016. Upřednostňovaná varianta politiky zahrnuje sdílené odpovědnosti a mechanismy zaměřené na podporu větší důvěry mezi členskými státy a orgány a průmyslem a na sdílení informací. Tato možnost by rovněž „… zajistila větší zapojení agentury ENISA v rámci jejího současného mandátu do poskytování přesného přehledu o stavu kybernetické bezpečnosti v Unii“.

ENISA s ohledem na povinné kontroly 3GPP

Povinné kontroly specifikované 3GPP lze rozdělit do dvou kategorií:

i) povinné kontroly pro implementaci jsou bezpečnostní opatření a protokoly, které musí poskytovatelé sítí zavést do svých sítí 5G,
ii) povinné kontroly pro použití jsou bezpečnostní opatření a postupy, které musí uživatelé sítě dodržovat, aby zajistili bezpečnost sítě a jejich vlastní zařízení.

Povinné kontroly pro implementaci: Tyto kontroly specifikují bezpečnostní opatření a protokoly, které musí poskytovatelé sítí implementovat do svých 5G sítí, aby zajistili bezpečnost a spolehlivost sítě. Tyto kontroly jsou primárně zaměřeny na zabezpečení síťové infrastruktury, jejích prvků a jejích komunikačních tras.

Příklady povinných kontrol pro implementaci zahrnují řízení přístupu, autentizaci uživatele, důvěrnost dat, ochranu integrity a segmentování sítě. Tyto kontroly zavádějí poskytovatelé sítí a poskytovatelé služeb.

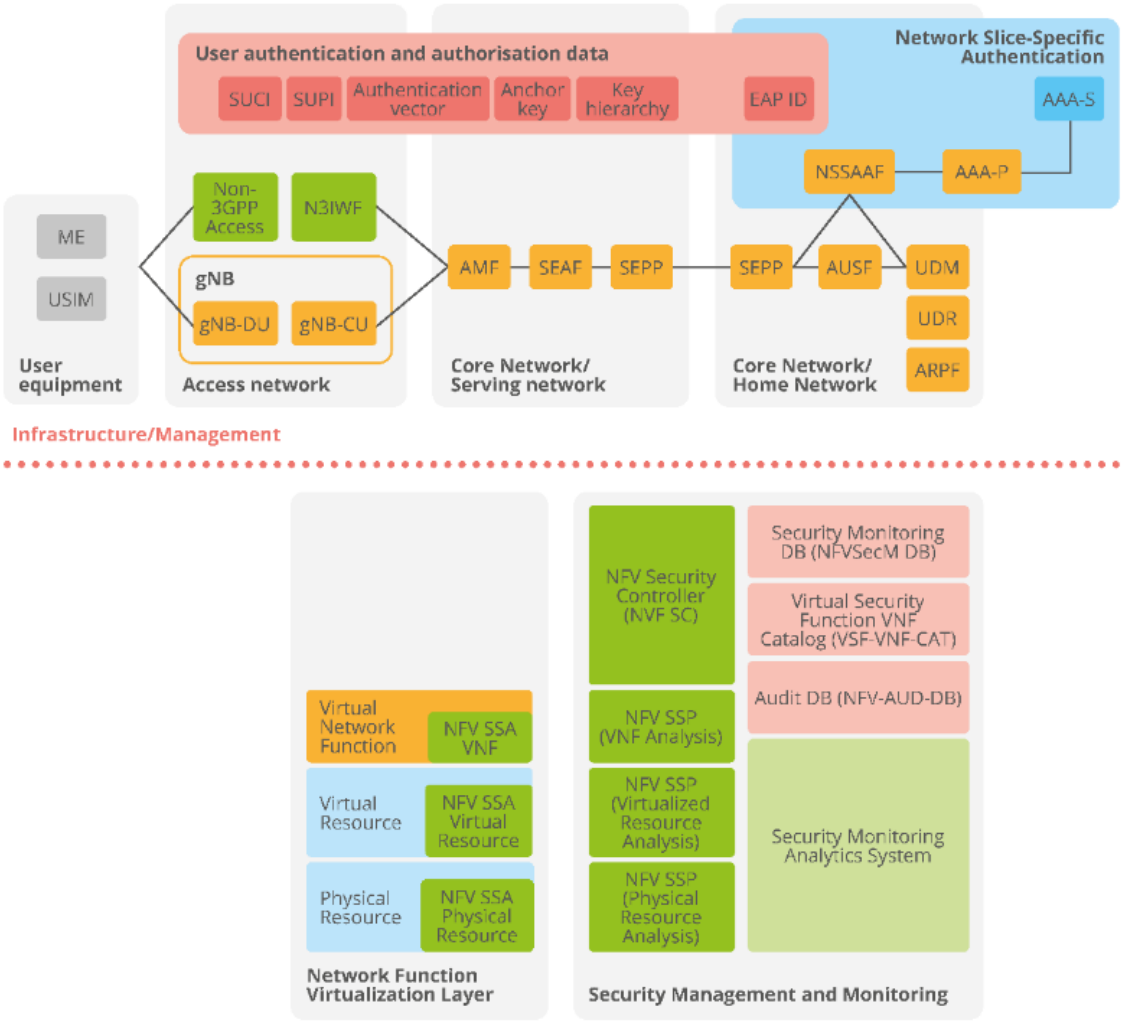
Povinné kontroly pro použití: Tyto kontroly specifikují bezpečnostní opatření a postupy, které musí uživatelé sítě dodržovat, aby zajistili bezpečnost sítě a ochránili svá vlastní zařízení a data. Tyto kontroly se zaměřují na zajištění toho, aby zařízení připojená k síti byla bezpečná a aby uživatelé dodržovali správné bezpečnostní protokoly a zásady.

Příklady povinných ovládacích prvků pro použití zahrnují zásady hesel, řízení přístupu uživatelů, ověřování zařízení a šifrování dat. Tyto kontroly jsou vynuceny na uživatelích a zařízeních připojených k síti.

Hlavní úlohou ENISA je podporovat členské státy EU při posilování jejich schopností v oblasti kybernetické bezpečnosti a podporovat spolupráci mezi členskými státy EU, soukromým sektorem a výzkumnou komunitou.

V rámci své role poskytuje ENISA pokyny a osvědčené postupy v oblasti kybernetické bezpečnosti, posuzuje rizika kybernetické bezpečnosti a podporuje rozvoj certifikačních schémat kybernetické bezpečnosti. Nemá však formální vynucovací pravomoci a jeho role je zaměřena především na poradenství a podporu. Namísto toho odpovědnost za vynucování povinného používání bezpečnostních kontrol spočívá na členských státech Evropské unie. Každý členský stát EU má své vlastní zákony a předpisy týkající se kybernetické bezpečnosti a je odpovědný za vymáhání těchto zákonů a zajištění toho, aby byla zavedena opatření kybernetické bezpečnosti na ochranu jejich organizací, občanů a dat.

Tento strategický přístup připravuje půdu pro implementaci nových infrastruktur, počítačových modelů a aplikací budoucnosti, které budou muset odolat sofistikovaným globálním náporům hybridních hrozeb.



Architektura zabezpečení 5G