MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Evropská Unie koordinuje hodnocení rizika kybernetické bezpečnosti sítí 5G.

Zdroj: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

Autor: Networks and Informations Systems Cooperation Group

Sítě 5G budou hrát ústřední roli při dosahování digitální transformace hospodářství a společnosti Evropské Unie (dále jen EU). Sítě 5G mají potenciál umožnit a podporovat širokou škálu aplikací a funkcí, které daleko přesahují poskytování mobilních komunikačních služeb mezi koncovými uživateli. Kybernetická bezpečnost sítí 5G je nezbytná pro ochranu ekonomik EU i jejích společností a pro umožnění plného potenciálu důležitých příležitostí, které přinesou. Je také zásadní pro zajištění strategické autonomie EU.

Tento dokument vznikl během roku 2019 za aktivní spolupráce členských států EU a European Union Agency for Cybersecurity (dále jen ENISA). Dokument na vysoké úrovni uvádí klíčová společná zjištění, vyplývající z vnitrostátních posouzení rizik sítí 5G, prováděných každým členským státem. Zdůrazňuje prvky, které mají pro EU zvláštní strategický význam. Jejím cílem není předložit vyčerpávající analýzu všech relevantních aspektů nebo typů jednotlivých rizik kybernetické bezpečnosti souvisejících se sítěmi 5G, ale klasifikovat skupiny rizik a ukázat možnosti jejich eliminace.

Definice:

„5G sítě znamenají soubor všech příslušných prvků síťové infrastruktury pro mobilní a bezdrátové komunikační technologie používané pro připojení a služby s přidanou hodnotou s pokročilými výkonovými charakteristikami, jako je velmi vysoká rychlost a kapacita dat, komunikace s nízkou latencí, mimořádně vysoká spolehlivost nebo podpora velkého počtu připojených zařízení. Mohou zahrnovat prvky starší sítě, založené na předchozích generacích mobilní a bezdrátové komunikační technologie, jako je 4G nebo 3G. Sítě 5G by měly být chápány tak, že zahrnují všechny relevantní části sítě. “

Z technologického hlediska budou sítě 5G využívat řadu nových technických funkcí ve srovnání se současnou situací ve stávajících sítích. **Tyto nové funkce přinesou řadu nových bezpečnostních výzev.** Zejména zvýší složitost telekomunikačního dodavatelského řetězce v bezpečnostní analýze s tím, že se různí stávající nebo noví hráči, jako jsou integrátoři, poskytovatelé služeb nebo dodavatelé softwaru, ještě více zapojí do konfigurace a správy klíčových částí. sítě. **Je pravděpodobné, že některé citlivé funkce, které se v současné době vykonávají ve fyzicky a logicky odděleném jádru, budou přesunuty blíže k okraji sítě, což vyžaduje přesunutí příslušných bezpečnostních kontrol, aby zahrnovaly kritické části celé sítě.** Pokud nebudou řádně spravovány, očekává se, že tyto nové funkce zvýší celkovou plochu útoku a počet potenciálních vstupních bodů pro útočníky a také zvýší šance na škodlivé předstírání zosobnění částí sítě a funkcí.

MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Cílem akčního plánu EU 5G7 je podpořit úsilí EU o nasazení infrastruktur a služeb 5G na jednotném digitálním trhu. Stanovuje plán veřejných a soukromých investic do infrastruktury 5G v EU a cíl nejpozději do konce roku 2020 pro zavedení komerčních sítí 5G

Hlavní zúčastněné strany v infrastruktuře sítí 5G:

- Provozovatelé mobilních sítí: subjekty poskytující uživatelům mobilní síťové služby, které provozují svou vlastní síť pomocí třetích stran.
- Dodavatelé provozovatelů mobilních sítí: subjekty poskytující služby nebo infrastrukturu za účelem budování anebo provozování mobilních sítí.
- Ostatní dodavatelé třetích stran: například poskytovatelé cloudové infrastruktury, systémoví integrátoři, dodavatelé zabezpečení a údržby, výrobce přenosových zařízení.
- Výrobci připojených zařízení a související poskytovatelé služeb: subjekty poskytující objekty nebo služby, které se budou připojovat k sítím 5G (např. Smartphony, připojená vozidla, elektronické zdravotnictví) a související komponenty služeb.
- Ostatní zúčastněné strany: včetně poskytovatelů služeb a obsahu a koncových uživatelů mobilních sítí 5G.

Hodnocení rizik kybernetické bezpečnosti 5G členskými státy EU.

Tento dokument se řídí přístupem, stanoveným v metodice hodnocení rizik ISO/IEC: 27005. Odráží hodnocení sady parametrů:

- hlavní typy hrozeb, které představují sítě 5G,
- hlavní aktéři hrozeb,
- hlavní aktiva a jejich citlivost,
- hlavní zranitelnosti,
- hlavní rizika a související scénáře.

Hrozby.

Nasazení sítí 5G probíhá ve složité globální hrozbě kybernetické bezpečnosti, která se vyznačuje zejména nárůstem útoků v dodavatelském řetězci. Celkově jsou považovány za nejdůležitější hrozby hlavní tradiční kategorie hrozeb: jedná se o hrozby spojené s ohrožením důvěrnosti, dostupnosti a integrity.

Řada **scénářů ohrožení** zaměřených na sítě 5G se týká zejména:

- přerušení místní nebo globální 5G sítě (dostupnost);
- špionáž provozu/dat v síťové infrastruktuře 5G (důvěrnost);
- úprava nebo přesměrování provozu/dat v síťové infrastruktuře 5G (integrita anebo důvěrnost);
- zničení nebo změna jiných digitálních infrastruktur nebo informačních systémů prostřednictvím sítí 5G (integrita anebo dostupnost).

Závažnost konkrétních scénářů hrozeb pro sítě 5G se tedy může lišit podle řady **faktorů**, zejména:

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

- počet a typ ovlivněných uživatelů;
- doba trvání události před detekcí nebo nápravou;
- druh ovlivněných služeb (veřejná bezpečnost, pohotovostní služby, zdravotnictví, vládní činnosti, elektřina, voda atd.) a rozsah poškození nebo ekonomických ztrát;
- druh porušených informací.

Níže uvedená tabulka popisuje různé subjekty ohrožení posuzované členskými státy:

TITLE	DESCRIPTION
Non-Adversary/ Accidental	Non-adverserial/accidental threats manifest themselves as events that result from human error, natural phenomena, and systems failures.
Individual hacker	Individual hackers represent amateur criminal or hobbyist hackers driven by financial motivation or a desire for notoriety.
Hacktivist group	This threat actor has a political agenda. Their goal is to either create public attacks that help them distribute propaganda, or to cause damage to organizations they are opposed to. The ultimate goal is to find a way to benefit their cause or gain awareness for their issue.
Organised crime group	Organised crime groups are motivated by financial gain.
Insider	In the context of the security of 5G networks an insider threat refers to an insider working within a mobile network operator, or a mobile network's supplier. An insider may work for an organised crime group, a hacktivist group or a State actor, but individual motivations are not excluded.
State actor or state-backed actor	The motivations of this category of attacker are primarily political.
Other possible actors: Cyber-terrorists and corporate entities	Cyber terrorists are motivated by political aims and are likely to have very similar capabilities as an organised crime group. Corporate entities may seek to gain competitive advantage in the technological area through Intellectual Property (IP) theft, theft of sensitive commercial data or by causing reputational or operational damage to their global competitors through cyberattacks.

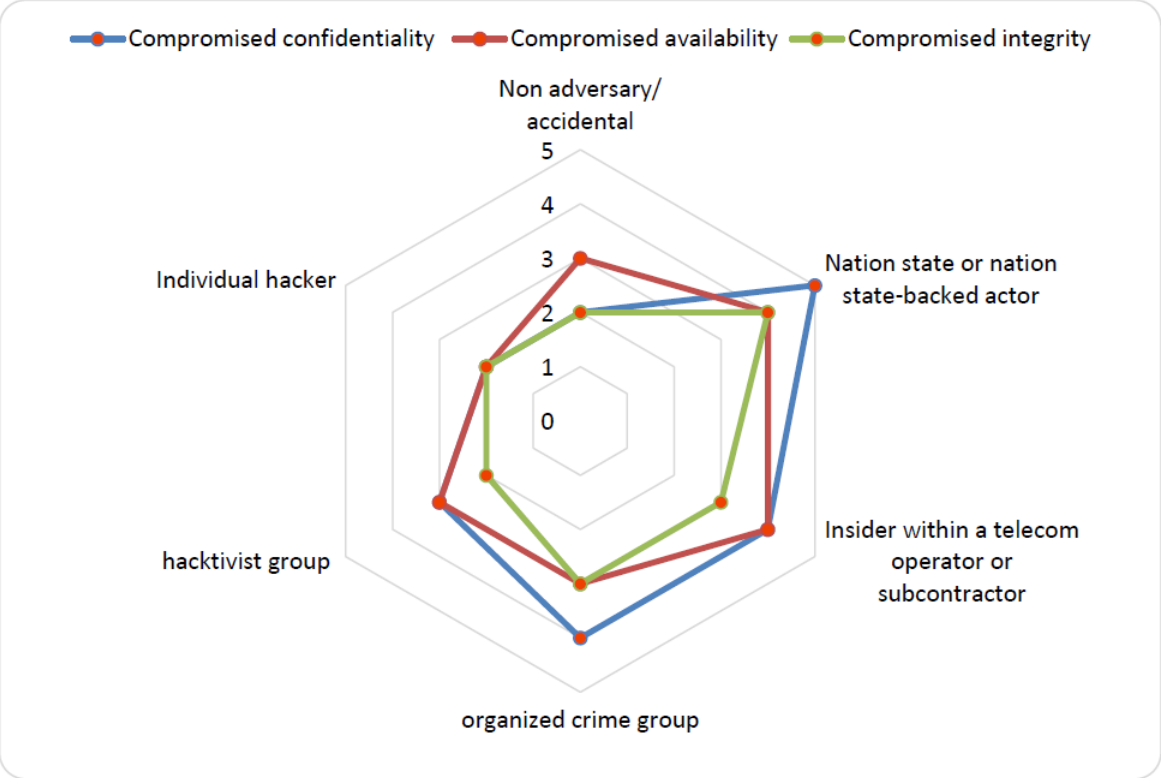
Hrozby, které představují státy nebo státem podporované subjekty, jsou považovány za nejdůležitější. Kombinace motivace, úmyslu a schopnosti na vysoké úrovni umožňuje státům páchat útoky, které mohou být velmi složité a mají velký dopad na základní služby pro širokou veřejnost, čímž se zhoršuje důvěra v mobilní technologie a operátory. Například státy nebo subjekty podporované státem mohou způsobit rozsáhlý výpadek nebo významné narušení telekomunikačních služeb využíváním nezdokumentovaných funkcí nebo útokem na vzájemně závislé kritické infrastruktury.

Ve vztahu ke státním a státem podporovaným aktérům hrozí zvláštní hrozba z kybernetických útočných iniciativ zemí mimo EU.

MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Konsolidovaný pohled na kategorii hrozeb podle aktérů hrozeb:



Zranitelnost.

- Chyby zabezpečení, související s hardwarem, softwarem, procesy a zásadami,
- nedostatek specializovaného a vyškoleného personálu pro zabezpečení, monitorování a údržbu sítí 5G,
- nedostatek odpovídajících vnitřních bezpečnostních kontrol a monitorovacích postupů,
- nedostatek systémů řízení bezpečnosti a nedostatků v postupech řízení rizik,
- nedostatek nebo nedostatečné postupy zabezpečení nebo provozní údržby,
- nedostatečný design sítě a architektura (včetně chybějícího efektivního rozvoje),
- nedostatečná fyzická bezpečnost pro síťovou a IT infrastrukturu,
- nedostatečné zásady pro místní a vzdálený přístup k síťovým komponentům,
- nedostatek nebo nedostatečné požadavky na zabezpečení v procesu zadávání zakázek,
- nedostatečný proces správy změn,
- souhrn zranitelností specifických pro dodavatele, například pravděpodobnost, že bude dodavatel ovlivněn ze země mimo EU, schopnost dodavatele zajistit dodávky, celková kvalita produktů a postupů kybernetické bezpečnosti dodavatele atd.

MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Hlavní typy rizik.

I. Scénáře rizik související s nedostatečnými bezpečnostními opatřeními.

- Chybná konfigurace sítí: využívá špatně nakonfigurované systémy a architekturu, státní herec proniká do sítě 5G prostřednictvím svých externích rozhraní, což vede ke kompromitaci základních funkcí sítě, nebo využívá uzly pro výpočet hrany, aby ohrozily informace důvěrnost a narušit distribuované služby.
- Nedostatek řízení přístupu: subdodavatel s oprávněními správce v síti provádí nepříznivé kroky, což vede k narušení důvěrnosti anebo integrity anebo narušení dostupnosti. Činnost subdodavatele může být způsobena zákonným požadavkem uloženým třetí zemí nebo nečestným chováním zaměstnanců dodavatele.

II. Rizikové scénáře související s dodavatelským řetězcem 5G.

- poruchy nebo zranitelnosti zařízení v důsledku staršího vybavení, špatných procesů softwarového inženýrství nebo špatného řízení zranitelnosti,
- závislost na kterémkoli dodavateli, buď na úrovni jednotlivé sítě, nebo na celostátní úrovni nebo v celé EU.
- nízká kvalita vybavení (špionáž ze strany státních nebo státem podporovaných aktérů, kteří používají malware k zneužití síťových komponent nekvalitní kvality nebo neúmyslných zranitelností ovlivňujících citlivé prvky v základní síti, jako jsou funkce virtualizace sítě),
- závislost (provozovatel mobilní sítě získává velké množství citlivých síťových komponent nebo služeb od jednoho dodavatele)

III. Rizikové scénáře související s modem operandi hlavních aktérů hrozeb.

Některé scénáře rizika jsou přímo spojeny s typickými schopnostmi a záměrem hlavních činitelů hrozeb, např. jejich potenciální úmysly provést určité typy útoků a jejich schopnost využít určité útočné vektory.

Zejména nepřátelské třetí země mohou vyvíjet tlak na dodavatele 5G s cílem usnadnit kybernetické útoky sloužící jejich národním zájmům. Míra expozice tomuto riziku je silně ovlivněna mírou, do jaké má dodavatel přístup k síti, zejména jeho nejcitlivější aktiva, a rizikovým profilem jednotlivého dodavatele. Rovněž se výrazně zvyšuje, pokud nejsou zavedeny dostatečné kontroly zabezpečení a přístupu. K rušení může dojít různými způsoby, např. využíváním vložených neúmyslných chyb zabezpečení nebo prostřednictvím záměrně vložených chyb zabezpečení.

Kromě toho sítě 5G mohou být také cílem sofistikovaného škodlivého jednání organizovaného zločinu za účelem zisku. Méně silní aktéři, jako jsou skupiny organizovaného zločinu, mohou také obchodovat s odborníky na narušení sítě za účelem finančního zisku.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Související scénáře rizika:

- Státní zásah prostřednictvím dodavatelského řetězce 5G: aktér nepřátelského státu vyvíjí tlak na dodavatele v jeho jurisdikci, aby poskytoval přístup k citlivým síťovým aktivům prostřednictvím (záměrně nebo neúmyslně) vložených zranitelností.
- Využívání sítí 5G organizovaným zločinem: převzetím kontroly nad kritickou částí architektury sítě 5G narušuje skupina organizovaného zločinu různé služby pro výkupné podniky, které se na tyto služby spoléhají, nebo samotný provozovatel mobilní sítě.
- Alternativně může skupina organizovaného zločinu za použití podobné útočné cesty cílit také na konečné uživatele, např. injekcí falešných zpráv uživatelům v síti jako součást rozsáhlého „phishingového“ útoku nebo online podvodů nebo pomocí kompromitované sítě k získání přístupu k důvěrným údajům o uživatelích (např. autentizační kódy druhého faktoru) za účelem dalšího zisku.

IV. Scénáře rizika související se vzájemnými závislostmi mezi sítěmi 5G a jinými kritickými systémy.

Vzhledem k předpokládané vzájemné závislosti mezi sítěmi 5G a mnoha dalšími systémy v kritických oblastech (např. zdravotnictví, autonomní vozidla, dodávky energie, plynu a vody, obrana) může zhoršení nebo selhání služeb 5G vést k významnému narušení těchto systémů.

Naopak, jiné kritické infrastruktury, na nichž jsou závislé sítě 5G, jako jsou energetické sítě a systémy ICS, mají známé zranitelnosti, které mohou být cílem kybernetických útoků. Potenciál ztráty základních služeb provozovatelům sítí 5G je možný buď v důsledku selhání služby poskytovatelem služeb (např. napájení), nebo v důsledku kybernetického útoku na subjekt závislý na kritické informační infrastruktuře. Řízení vyhrazeného řezu aktérem, který je vně sítě, může také zvýšit vystavení kybernetickým hrozbám. V posledních letech mnoho aktérů ohrožení vyvinulo tyto schopnosti, včetně herců podporovaných státem.

Na úrovni EU jsou bezpečnostní požadavky týkající se ekosystému sítí 5G a souvisejících kritických systémů stanoveny zejména v právních předpisech EU o telekomunikacích a ve směrnici NIS. Mezi další příslušné rámce na úrovni EU a na vnitrostátní úrovni patří pravidla ochrany údajů a soukromí (zejména obecné nařízení o ochraně údajů a směrnice o soukromí a elektronických komunikacích), jakož i požadavky vztahující se na kritické infrastruktury.

Na vnitrostátní úrovni přijaly členské státy různé přístupy k provádění výše uvedených bezpečnostních ustanovení ak jejich prosazování. Pokud se na provozovatele mobilních sítí vztahují závazná pravidla, mohou se vztahovat na různé typy technických a organizačních opatření.

Provozovatelé mobilních sítí mohou již navíc uplatňovat různá bezpečnostní opatření, například: technická opatření (např. šifrování, autentizace, automatizace, detekce anomálií)

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

nebo procesní opatření (např. správa zranitelnosti, plánování incidentů a reakcí, správa uživatelských oprávnění) , plánování obnovy po katastrofě).

Závěry a další postup.

Tato zpráva identifikuje řadu důležitých bezpečnostních výzev, které pravděpodobně způsobí nebo zintenzivní příchod sítí 5G, přičemž bude brát v úvahu vyvíjející se povahu technologie a prostředí 5G.

Konkrétně:

a) Technologické změny zavedené 5G zvýší celkovou útočnou plochu a počet potenciálních vstupních bodů pro útočníky.

b) Tyto nové technologické funkce budou mít větší význam pro závislost provozovatelů mobilních sítí na dodavatelích třetích stran a na jejich roli v dodavatelském řetězci 5G.

c) Velká závislost na jediném dodavateli zvyšuje expozici a důsledky možného selhání tohoto dodavatele. Zhoršuje také možné důsledky slabostí nebo slabých míst a jejich možné zneužití subjekty ohrožení, zejména pokud se závislost týká dodavatele, který představuje vysoký stupeň rizika.

d) Pokud dojde k realizaci některých nových případů použití předpokládaných pro 5G, sítě 5G budou koncovou důležitou součástí dodavatelského řetězce mnoha kritických IT aplikací, a proto nebudou ovlivněny nejen požadavky na důvěrnost a soukromí, ale také integrita a dostupnost těchto sítí, což se z hlediska EU stane hlavním problémem národní bezpečnosti a velkou výzvou v oblasti bezpečnosti.

Za účelem řešení výše popsaných rizik a plného využití potenciálních bezpečnostních příležitostí spojených s technologií 5G lze zvážit různé typy opatření. Některá z těchto opatření jsou již zavedena, alespoň částečně. Týká se to zejména bezpečnostních požadavků, které se vztahují na předchozí generace mobilních sítí a které zůstávají platné pro budoucí nasazení sítí 5G.

<u>Struktura dokumentu:</u>

1. Úvod.

- Politický kontext a postup
- Rozsah: 5G sítě a související aplikace K
- Klíčové technologické novinky 5G sítí
- Ekosystém 5G a nasazení v EU

2. Hodnocení rizik kybernetické bezpečnosti 5G členskými státy EU.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

- Hrozby a hráči ohrožení.
- B. Aktiva.
- C. Zranitelnosti.
- D. Scénáře rizika.
  - Scénáře rizik související s nedostatečnými bezpečnostními opatřeními,
  - rizikové scénáře související s dodavatelským řetězcem 5G,
  - scénáře rizik související s mody operandi hlavních činitelů hrozeb,
  - scénáře rizika související se vzájemnými závislostmi mezi sítěmi 5G a jinými kritickými systémy,
  - scénáře rizik související se zařízeními koncového uživatele,
- E. Stávající zmírňující opatření a základní úroveň zabezpečení.

3) Závěry a cesta vpřed.