Grant Thornton

MINISTERSTVO PRŮMYSLU A OBCHODU

Financováno Evropskou unií
NextGenerationEU

Analýza kybernetických rizik souvisejících s provozováním 5G sítí pro privátní (uzavřené) sítě a poskytování veřejných služeb, vč. dopadů přístupů Open RAN a Open Core na bezpečnost 5G sítí

Připraveno pro Ministerstvo průmyslu a obchodu

[Srpen 2024]

Národní plán obnovy

Obsah

Seznam zkratek a vysvětlivek

3GPP	Partnerství třetí generace mezi telekomunikačními standardizačními organizacemi (3rd Generation Partnership Project)
AES	Pokročilý šifrovací standard (Advanced Encryption Standard)
AI	Umělá inteligence (Artificial Intelligence)
API	Aplikační programové rozhraní (Application Programming Interface)
CA	Certifikační autorita (Certification Authority)
CU	Centralized Units
DDoS	Distribuované odmítnutí služby (Distributed Denial of Service)
DDS	Dynamické sdílení spektra (Dynamic Spectrum Sharing)
DoS	Odmítnutí služby (Denial of Service)
DRP	Plán obnovy po katastrofě (Disaster Recovery Plan)
DTLS	Zabezpečení transportní vrstvy pro datagramy (Datagram Transport Layer Security)
DU	Distributed Units
E2EE	Šifrování od konce ke konci (End-to-End Encryption)
EAP-AKA	Rozšiřitelný autentizační protokol - autentizace a dohodnutí klíče (Extensible Authentication Protocol-Authentication and Key Agreement)
EDR	Detekce a reakce na koncové body (Endpoint Detection and Response)
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost (European Network and Information Security Agency)
FCC	Federální komise pro komunikace (Federal Communications Commission)
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
IAM	Správa identit a přístupu (Identity and Access Management)
IEEE	Institut elektrotechnických a elektronických inženýrů (Institute of Electrical and Electronics Engineers)
IoT	Internet věcí (Internet of Things)
IP	Internetový protokol (Internet Protocol)
IPSec	Zabezpečení internetového protokolu (Internet Protocol Security)
IRT	Tým pro reakci na incidenty (Incident Response Team)
ISACs	Centra pro sdílení a analýzu informací (Information Sharing and Analysis Centers)
ITU	Mezinárodní telekomunikační unie (International Telecommunication Union)
MFA	Vícefaktorová autentizace (Multi-Factor Authentication)
ML	Strojové učení (Machine Learning)
NFV	Virtualizace síťových funkcí (Network Functions Virtualization)
Open Core	otevřené jádro sítě / otevřená páteřní síť
Open RAN	Otevřená Rádiová přístupová síť (Open Radio Access Network)
PFCP	Řídící protokol pro přesměrování paketů (Packet Forwarding Control Protocol)
PKI	Infrastruktura veřejných klíčů (Public Key Infrastructure)
QoS	Kvalita služeb (Quality of Service)
RAN	Rádiová přístupová síť (Radio Access Network)
RBAC	Řízení přístupu založené na rolích (Role-based access control)
SDN	Softwarově definované sítě (Software-Defined Networking)

SSH	Bezpečný shell - kryptografický síťový protokol pro bezpečný přístup k síťovým službám (Secure Shell)
STIX	Strukturovaný výraz informací o hrozbách (Structured Threat Information eXpression)
TLS	Zabezpečení transportní vrstvy (Transport Layer Security)
UDP	Uživatelský datagramový protokol (User Datagram Protocol)
UIM	Sjednocená správa identit (Unified Identity Management)
VPN	Virtuální privátní sítě (Virtual Private Network)

Manažerské shrnutí

5G technologie představuje revoluční skok ve světě telekomunikací, přinášející nejen rychlejší a spolehlivější připojení, ale i zcela nové možnosti pro průmyslové aplikace a veřejné služby. Zavedení 5G sítí je klíčovým faktorem pro realizaci koncepce "Internetu věcí" (IoT), který umožňuje propojení milionů zařízení, od chytrých domácností až po autonomní vozidla a inteligentní infrastrukturu. 5G sítě slibují zlepšení v několika klíčových oblastech jako vyšší rychlosti přenosu dat, které umožňují stahování a streamování obsahu ve vysokém rozlišení okamžitě, výrazně nižší prodlevy v odezvě (latence), což je klíčové pro aplikace vyžadující reálný čas, jako jsou autonomní vozidla, průmyslová automatizace a telemedicína, a podporu mnohem většího počtu zařízení na jednotku plochy, což je zásadní pro rozvoj chytrých měst a IoT aplikací. 5G technologie se navzdory těmto přínosům potýká také s novými kybernetickými hrozbami a bezpečnostními výzvami. Komplexní architektura 5G sítí, která zahrnuje velké množství různých zařízení a systémů, zvyšuje potenciálně rozsah útoku a rozšiřuje směrování zranitelnosti.

Klíčová kybernetická rizika 5G sítí

1. **Komplexita sítě**: Větší složitost a heterogenita zařízení a systémů zvyšuje pravděpodobnost zranitelností a útoků.
2. **Povaha 5G architektury**: Distribuovaná architektura 5G sítí zvyšuje potenciální rozsah útoku, což může vést k narušení integrity a dostupnosti služeb.
3. **Dodavatelský řetězec**: Závislost na různých dodavatelích hardwaru a softwaru může přinášet bezpečnostní rizika spojená s nedostatečnou kontrolou nad celým řetězcem (operátoři, výrobci zařízení, softwarovými vývojáři, dodavatelé)
4. **Soukromí a ochrana dat**: Zvýšené množství dat a jejich šíření mezi různými částmi sítě zvyšuje riziko narušení soukromí a úniku citlivých informací.
5. **Rušení signálu a útoky na signál**: 5G technologie může být zranitelná vůči fyzickým útokům, jako jsou rušení a odposlouchávání signálu.

Hlavní přínosy a rizika užití Open RAN a Open Core lze shrnout následovně:

1. **Open RAN**
   - **Přínosy**: Umožňuje flexibilitu a interoperabilitu mezi zařízeními různých dodavatelů, což může vést ke snížení nákladů a inovacím.
2. **Open Core**
   - **Přínosy**: Open Core také zlepšuje interoperabilitu a flexibilitu sítě. Navíc umožňuje rychlejší a efektivnější nasazení nových služeb.
   - **Rizika**:
     - Zavedení standardizovaných otevřených rozhraní může zvýšit riziko kybernetických útoků, pokud nejsou adekvátně zabezpečena.
     - Navíc závislost na softwarových řešeních třetích stran může zvýšit nebo vést k novým typům zranitelnosti.

V souvislosti s identifikovanými riziky pro přístupy Open RAN/Open Core musí být aplikována alespoň níže doporučovaná bezpečnostní opatření:

1. **Posílení bezpečnostních standardů a kontrol**: Zavedení robustních bezpečnostních opatření a standardů pro všechny části 5G sítě.
2. **Monitoring a detekce anomálií**: Implementace pokročilých systémů pro monitorování a detekci neobvyklých aktivit v síti.
3. **Bezpečnostní audit dodavatelů**: Důkladné prověřování a auditování všech dodavatelů zapojených do výstavby a provozu 5G sítí.
4. **Ochrana dat a soukromí**: Nasazení silných šifrovacích mechanismů a přísných pravidel pro ochranu dat.
5. **Školení a povědomí**: Pravidelné školení personálu a zvyšování povědomí o aktuálních hrozbách a bezpečnostních opatřeních.

Závěr

Přístupy Open RAN a Open Core nabízejí flexibilitu a interoperabilitu, ale zároveň zvyšují potenciální bezpečnostní rizika kvůli otevřeným rozhraním a závislosti na softwarových řešeních třetích stran. Pro úspěšné a bezpečné nasazení 5G technologií je nezbytné přijmout komplexní bezpečnostní opatření, jako je posílení standardů, monitorování sítě, audit dodavatelů, ochrana dat a pravidelné školení personálu. Celkově lze říci, že pečlivě vyvážený přístup k bezpečnosti umožní plně využít potenciál 5G sítí a současně minimalizovat související kybernetická rizika.

1 Úvod

Sítě 5G rozšiřují možnosti přenosu informací včetně těch citlivých. Je proto nutné analyzovat kybernetickou odolnost a možnosti zranitelnosti těchto sítí s ohledem na přístupy jako jsou Open RAN nebo Open Core.

Pro tento účel by vypracovaná studie měla:

- Identifikovat a analyzovat potenciální zranitelnosti v 5G sítích souvisejících s přístupy Open RAN a Open Core a zhodnotit jejich potenciální dopady na celkovou bezpečnost dané mobilní sítě.
- Zhodnotit potenciální i možné typy kybernetických útoků, které mohou ohrozit integritu, důvěrnost a dostupnost dat v rámci jek privátních, tak veřejných 5G sítí vybudovaných v prostředí Open RAN.
- Analyzovat možnosti a rizika související se správou identit a přístupů v rámci takovýchto 5G sítí a posoudit potenciální slabé místa v systémech autentizace a autorizace.
- Zhodnotit rizika a bezpečnostní aspekty spojené s implementací Open RAN a Open Core architektur do 5G sítí z pohledu rizika spojeného s narušením integrity datového přenosu v takovýchto 5G sítích a navrhnout způsob zajištění, aby data zůstala nedotčena a nezměněna během přenosu.
- Prověřit a zhodnotit opatření pro ochranu takovýchto 5G sítí před možnou nepovolenou komunikací se zahraničními servery (např. odesílání dat nebo přijímaní povelů a příkazů ze zahraniční) a navrhnout možný způsob odhalování takovýchto negativních jevů.
- Prověřit a zhodnotit schopnosti 5G sítí vybudovaných v prostředí Open RAN odolávat distribuovaným útokům odepření služby (DDoS) a navrhnout způsob zajištění, jak by měla být zajištěna dostupnost sítí i při jejím vysokém zatížení.
- Navrhnout systém pro pravidelné auditování a monitorování bezpečnostních opatření v takovýchto 5G sítích a navrhnout způsob zajištění okamžité reakce na možné bezpečnostní incidenty.
- Prověřit, zda není ohroženo zálohování a obnova dat v takovýchto sítích 5G.
- Vytvořit rámcový přehled, jak je zajištěna problematika využívání zařízení Open RAN a Open Core v jiných technologicky vyspělých zemích a doporučit aplikaci případných best practices.

1.1 Poučení a prohlášení zpracovatele

Zpracovatel neposkytuje žádná prohlášení a nenese žádnou odpovědnost s ohledem na pravost, správnost, přesnost či úplnost jakýchkoliv informací, které byly zjištěny z veřejných zdrojů.

Studie (dále jen „studie“) byla vypracována v rozsahu a s relevancí ke dni jejího zpracování, tj. ke dni uvedenému v záhlaví studie. Zpracovatel neodpovídá za případné změny relevantních skutečností a předpisů, ke kterým došlo po tomto uvedeném datu. Studie či její dílčí obsah nesmí být jakkoliv kopírován či měněn, nesmí být zpřístupněn třetím osobám ani s ním nesmí být jinak disponováno bez výslovného předchozího písemného souhlasu zpracovatele. Každé takové jednání bude považováno za neoprávněné. Výklady, hodnocení, názory a závěry jsou platné pouze v celkovém kontextu studie.

1.2 Seznam zdrojů

1.2.1 EU zdroje

- Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019, o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

- Doporučení Evropské komise ke kybernetické bezpečnosti 5G sítí ze dne 26. března 2019

- Usnesení Evropského parlamentu ze dne 12. března 2019 o bezpečnostních hrozbách souvisejících se zvyšující se technologickou přítomností Číny v EU a o případných opatřeních na úrovni EU za účelem jejich omezení (2019/2575 (RSP))

- Sdělení Komise Evropskému Parlamentu, Radě (EU), Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Bezpečné zavádění sítí 5G v EU – Implementace souboru opatření EU ze dne 29. ledna 2020

- Zpráva členských států EU ke koordinovanému hodnocení rizik kybernetické bezpečnosti EU v sítích 5G ze dne 9. října 2019

- Soubor opatření EU pro kybernetickou bezpečnost sítí 5G (EU Toolbox)

- Bezpečné nasazení 5G v EU: Provádění souboru nástrojů EU – sdělení Evropské komise ze dne 29. ledna 2020

- Dokument ENISA: Posouzení hrozeb pro pátou generaci mobilních telefonů telekomunikační sítě (5G) z listopadu 2019

1.2.2 ČR zdroje

- Ústavní zákon č. 1/199 Sb., Ústava České republiky, ve znění pozdějších předpisů (dále jen „Ústava“)
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů (dále jen „ZoBČR“)
- Zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „ZZOU“)
- zákon č. 127/2005 Sb, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“)
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“)
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“)
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů (dále jen „ZTOPO“)
- Zákon č. 349/1999 Sb., o Veřejném ochránci práv, ve znění pozdějších předpisů (dále jen „ZVOP“)
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „VKB“)
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů

1.2.3 On-line zdroje

- Stát křísí Cell Broadcast pro rozesílání výstrah před nebezpečím do mobilů https://www.lupa.cz/clanky/stat-znovu-krisi-cell-broadcast-pro-rozesilani-vystrah-pred-nebezpecim-do-mobilu/

- https://www.lupa.cz/market-voice/pripojit-k-5g-cestujici-nestaci-budoucnost-zeleznice-se-jmenuje-frmcs/

- https://op.europa.eu/en/publication-detail/-/publication/8c6755a1-4f55-11ed-92ed-01aa75ed71a1/language-en/format-PDF/source-search

- Spouštění sítí 5G v EU: při zavádění sítí dochází ke zpoždění a bezpečnostní problémy zůstávají nevyřešeny (https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/cs/index.html)

- Prostředí hrozeb ENISA pro sítě 5G (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/@@download/fullReport)

- Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (Národní úřad pro kybernetickou a informační bezpečnost - Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (gov.cz))

2 Identifikace a analýza potenciálních zranitelností v 5G sítích souvisejících s přístupy Open RAN a Open Core

Open RAN architektura zahrnuje různé komponenty, jako jsou distribuované jednotky (DU), centralizované jednotky (CU) a základnové jednotky (Base Units - BU). Základnové jednotky hrají klíčovou roli v rámci rádiové přístupové sítě (RAN) tím, že poskytují fyzickou vrstvu pro komunikaci mezi uživatelskými zařízeními a sítí.

Tato kapitola se soustředí na hlavní komponenty 5G sítí, jakými jsou:

- Rozhraní mezi jednotkami Open RAN,
- Řízení a správa sítě Open RAN,
- Dodavatelský řetězec Open RAN
- SDN a virtualizace funkcí síťových prvků
- Interoperabilita a integrace Open Core
- Aktualizace a správa záplat Open Core

a identifikuje s nimi spojené potenciální zranitelnosti a bezpečnostní výzvy.

2.1 Rozhraní mezi jednotkami Open RAN

Rozhraní mezi základnovými jednotkami (BU), distribuovanými jednotkami (DU) a centralizovanými jednotkami (CU) v Open RAN architektuře, je klíčovým prvkem, který umožňuje flexibilitu a interoperabilitu v rádiové přístupové síti. Toto otevřené rozhraní, známé jako OPEN RAN, podporuje komunikaci a koordinaci mezi různými částmi sítě, což umožňuje operátorům kombinovat a přizpůsobovat technologie od různých výrobců. Avšak právě tato otevřenost a komplexnost mohou zvýšit bezpečnostní rizika. Text dále poskytuje přehled potenciálních zranitelností týkajících se rozhraní.

2.1.1 Odposlech a manipulace s daty

Rozhraní mezi BU, DU a CU přenáší rovněž citlivé informace, včetně uživatelských dat a řídicích signálů. Pokud komunikace mezi těmito jednotkami není řádně šifrována a zabezpečena, mohou útočníci tyto informace odposlouchávat nebo dokonce manipulovat s přenášenými daty. Taková situace pak způsobí únik citlivých informací, narušení služeb nebo umožní útočníkům uskutečnit podvodné aktivity.

Odposlech a manipulace s daty v rámci Open RAN architektury, zejména mezi základnovými jednotkami (BU), distribuovanými jednotkami (DU) a centralizovanými jednotkami (CU), mohou vést k různým typům podvodných aktivit. Zde jsou některé konkrétní příklady podvodných aktivit, které by mohly nastat:

1. Cloning útoky
   Pokud útočník dokáže odposlechnout a získat citlivé informace z komunikace, může je použít k vytvoření klonů zařízení. Tyto klonované zařízení se pak mohou připojit k síti, čímž umožňují útočníkovi přístup k síti a jejím službám bez povolení. To může vést k neautorizovanému využívání služeb, přenosu škodlivého obsahu nebo dalších aktivit způsobujících škody.
2. Podvržení falešných zpráv (Spoofing)
   Manipulace s daty může umožnit útočníkovi vložit falešné zprávy do komunikace. Například útočník může podvrhnout zprávy, které vypadají, že pocházejí z důvěryhodného zdroje, aby přiměl síťové komponenty k provedení nežádoucích akcí, jako je přesměrování provozu, deaktivace určitých funkcí nebo narušení služeb.
3. Man-in-the-Middle (MitM) útoky

V MitM útoku útočník odposlouchává a případně mění komunikaci mezi dvěma stranami, aniž by o tom tyto strany věděly. V kontextu Open RAN může útočník zachytit a upravit přenášená data. To může vést k narušení důvěrnosti a integrity dat, a umožnit útočníkovi získat citlivé informace nebo ovlivnit další chování sítě.

4. Útoky na fakturaci a zneužití služeb
   Útočníci mohou manipulovat s daty, změnit účtování a hlavně pak převody za služby nebo vytvořit falešné záznamy o využívání služeb. Například mohou upravit náležitosti faktur a pozměnit zcela úhrady za služby. Takové jednání pak způsobí finanční ztráty pro poskytovatele služeb a naruší důvěru zákazníků.
5. Distribuce malwaru a phishing
   Manipulace s daty se může odehrát také v podobě vkládání škodlivého softwaru nebo phishingových odkazů do komunikace. Útočník pak může přimět uživatele nebo síťové komponenty k stažení a spuštění škodlivého kódu a následně k další kompromitaci sítě a systémů, krádeži dat nebo narušení služeb.

Například se může uskutečnit podvržení falešné aktualizace softwaru v této podobě:

1. Odposlech a zjištění slabiny: Útočník odposlouchává komunikaci mezi BU a DU a zjistí, že je plánována softwarová aktualizace.
2. Podvržení falešné zprávy: Útočník zašle falešnou zprávu o aktualizaci softwaru, která vypadá, že pochází od důvěryhodného zdroje.
3. Distribuce škodlivého kódu: Falešná aktualizace obsahuje škodlivý kód, který je nainstalován na základnové jednotky (BU).
4. Útok: Škodlivý kód umožňuje útočníkovi získat kontrolu nad BU, sledovat komunikaci, sbírat citlivá data nebo narušit funkčnost sítě.

2.1.2 Nespolehlivá autentizace a autorizace

Dalším slabým místem může být u komponent sítě spolehlivost při ověřování identity ostatních prvků v síti a při ověřování oprávnění ostatních prvků komunikovat v síti. Slabiny v mechanismech autentizace a autorizace mohou umožnit neautorizovaným subjektům přistupovat k síťovým funkcím nebo provádět operace, které by měly být povoleny pouze důvěryhodným komponentám.

2.1.3 Nedodržovaná standardizace a neřízená implementace

Standardizace a implementace jsou klíčovými prvky pro zajištění bezpečnosti v Open RAN architektuře. Přestože O-RAN Alliance poskytuje standardy a specifikace pro zabezpečení komunikace mezi různými komponentami, jako jsou základnové jednotky (BU), distribuované jednotky (DU) a centralizované jednotky (CU), **existují různé zranitelnosti**, které mohou ohrozit tuto architekturu.

- Nesprávná implementace standardů
    - Popis: I když existují jasné standardy pro zabezpečení komunikace mezi DU a CU, ne všichni výrobci a operátoři umí tyto standardy implementovat správně nebo je dodržet
    - Příklad zranitelnosti: Chyby při implementaci šifrovacích protokolů mohou umožnit odposlech nebo manipulaci s daty.
- Nedostatečná kompatibilita
    - Popis: Různí dodavatelé mohou implementovat standardy O-RAN různými způsoby, což může vést k problémům s kompatibilitou. Tyto problémy mohou způsobit, že některé bezpečnostní funkce nebudou fungovat správně.
    - Příklad zranitelnosti: Pokud jedna komponenta nepodporuje určitou bezpečnostní funkci, může to narušit celkovou bezpečnostní architekturu sítě.
- Neprováděné aktualizace a záplatování
    - Popis: Standardy se vyvíjejí a nové bezpečnostní hrozby vyžadují pravidelné aktualizace a záplaty. Zranitelnosti mohou vzniknout, pokud aktualizace nejsou aplikovány včas nebo nejsou dostupné pro všechny komponenty sítě.
    - Příklad zranitelnosti: Známé zranitelnosti ze starších verzí softwaru, které nebyly záplatovány, mohou být zneužity útočníky.
- Dílčí rozhraní jako slabý článek
    - Popis: Komunikace mezi DU a CU zahrnuje několik rozhraní, která musí být bezpečně implementována. Pokud některá rozhraní nejsou dostatečně zabezpečená, mohou být využita k útokům.
    - Příklad zranitelnosti: Útoky typu man-in-the-middle (MitM) na nezabezpečená rozhraní mohou umožnit útočníkům odposlouchávat nebo manipulovat s komunikací.
- Omezené testování bezpečnosti
    - Popis: Testování bezpečnosti je kritické pro identifikaci zranitelností před nasazením do produkčního prostředí. Nedostatečné testování může znamenat, že některé zranitelnosti zůstávají neodhalené.
    - Příklad zranitelnosti: Propustnost protokolů na testovacím prostředí a implementace do produkce může být zneužita po nasazení systému.
- Nezabezpečená správa klíčů a certifikátů
    - Popis: Správa kryptografických klíčů a certifikátů je klíčová pro zajištění bezpečné komunikace. Slabiny v tomto procesu mohou vést k úniku nebo zneužití klíčů.
    - Příklad zranitelnosti: Pokud jsou klíče uloženy nezabezpečeným způsobem nebo pokud jsou certifikáty spravovány bez dostatečné kontroly, může dojít k jejich kompromitaci a nabourání se do systému.

Potenciální zranitelnosti rozhraní v 5G sítích **se zejména eliminují zabezpečením na úrovni síťové architektury, na úrovni protokolu, uplatňováním standardizace a řízenou implementací**. Zabezpečení proti zranitelnostem spočívá v kontinuálním a pravidelném provádění činností, jakými jsou:

- Provádění pravidelných auditů a testování bezpečnost - pravidelné penetrační testy a audity konfigurace mohou pomoci odhalit a opravit zranitelnosti.
- Dodržování standardů a testování kompatibility mezi různými komponentami od různých dodavatelů.
- Pravidelná aktualizace software, tj. udržování všech komponent aktuálními s nejnovějšími záplatami a bezpečnostními aktualizacemi.
- Implementace robustní správy klíčů a certifikátů, tzn. zajištění bezpečného generování, ukládání a správy kryptografických klíčů a certifikátů.
- Vzdělávání a školení, tzn. zajistit, aby byl lidé v organizaci byli obeznámeni s bezpečnostními postupy a ICT odborníci byli schopni implementovat a udržovat bezpečnostní opatření podle standardů O-RAN Alliance.

- **Zabezpečení síťové infrastruktury**

Kromě softwarového zabezpečení je nutné zabezpečit i fyzickou infrastrukturu BU, DU a CU. To zahrnuje ochranu před fyzickým narušením, zajištění bezpečného umístění a přístupu k jednotkám, a ochranu před riziky jako je sabotáž nebo krádež zařízení

- **Zabezpečení na úrovni protokolu**

Protože Open RAN podporuje širokou škálu protokolů pro komunikaci mezi BU, DU a CU, je zásadní zajistit, aby všechny tyto protokoly byly pevně zabezpečeny proti různým typům útoků, jako jsou DoS (Denial of Service) útoky, útoky prostřednictvím replikace nebo vkládání škodlivých dat do komunikace.

V této oblasti se uplatňují pevné autentizační protokoly, jejichž význam spočívá zejména v níže uvedených přínosech:

1. Zajištění identity: Pevné autentizační protokoly zajišťují, že každá komponenta v síti může důvěryhodně ověřit identitu ostatních komponent, se kterými komunikuje. To je klíčové pro prevenci podvržení identity (spoofing) a dalších forem útoků, kde útočník předstírá, že je legitimní entitou.
2. Ochrana proti neautorizovanému přístupu: Silné autentizační mechanismy zabraňují neautorizovaným entitám přístup k síťovým zdrojům a datům. To je nezbytné pro ochranu citlivých informací a pro zajištění, že pouze oprávněné entity mohou komunikovat a provádět operace v síti.
3. Integrita a důvěrnost dat: Kromě ověření identity zabezpečují autentizační protokoly mechanismy pro zajištění integrity a důvěrnosti dat. To znamená, že data přenášená mezi komponentami nemohou být změněna nebo odposlechnuta bez odhalení.

Dnešní autentizační prvky pracují s různými typy pevných autentizačních protokolů, jakými jsou:

1. Public Key Infrastructure (PKI): PKI využívá spárování veřejného a soukromého klíče pro ověřování identity. Každá entita má certifikát vydaný důvěryhodnou certifikační autoritou (CA), který je používán k ověření identity při každé komunikaci.
    - Příklad: Při navázání spojení mezi BU a DU se použijí certifikáty pro oboustrannou autentizaci, kde každá strana ověřuje identitu druhé strany pomocí veřejného klíče obsaženého v certifikátu.
2. Kerberos: Kerberos je autentizační protokol, který používá tickety pro autentizaci. Je založen na symetrické kryptografii a důvěryhodné třetí straně, známé jako Key Distribution Center (KDC).
    - Příklad: Při komunikaci mezi DU a CU může Kerberos poskytovat tickety, které ověřují, že obě strany jsou autorizovány ke komunikaci bez nutnosti opakovaného zadávání hesel.
3. EAP (Extensible Authentication Protocol): EAP funguje jako rámec pro autentizaci, který podporuje různé metody autentizace, jako jsou EAP-TLS (Transport Layer Security) nebo EAP-AKA (Authentication and Key Agreement).
    - Příklad: EAP-TLS může být použit pro zabezpečení bezdrátové komunikace mezi BU a uživatelskými zařízeními, kde je autentizace prováděna pomocí certifikátů.

- **Standardizace a implementace**

I když standardy OPEN RAN Alliance definují zabezpečení komunikace mezi BU, DU a CU, závisí na výrobcích a operátorech, jak tyto standardy implementují. Nedostatky v implementaci nebo nedodržení nejlepších postupů mohou vést k zranitelnostem.

Je zásadní, aby byla přijata rozsáhlá bezpečnostní opatření, včetně silného šifrování, pevných autentizačních protokolů, pravidelného bezpečnostní testování, pravidelné aktualizace a školení personálu ohledně bezpečnostních rizik a postupů. Tím se výrazně sníží riziko útoků a zajistí bezpečnější provoz v Open RAN sítích.

Minimální standardy pro rozhraní mezi jednotkami Open RAN vytváří Open RAN Alliance, a to pak zejména:

1. **O-RAN Architecture Description (O-RAN.WG1.O-RAN-Architecture-Description-v02.00)**: Tento dokument poskytuje celkový přehled architektury Open RAN, včetně komunikace mezi DU a CU a příslušných bezpečnostních aspektů.
2. **O-RAN Security Focus Group (O-RAN-SFG)**: Skupina expertů zaměřená na bezpečnostní standardy a doporučení pro Open RAN, která vydává specifikace a pokyny týkající se zabezpečení různých komponent Open RAN architektury.
3. **O-RAN Fronthaul Interface Specifications (O-RAN.WG4.CUS.0-v01.00)**: Tento dokument specifikuje rozhraní mezi DU a CU a upravuje bezpečnostní opatření pro zajištění bezpečné komunikace.

2.2 Řízení a správa sítě Open RAN

Činnosti řízení a správa sítě v kontextu Open RAN jsou pro efektivní fungování a optimalizaci rádiové přístupové sítě. Tyto aspekty jsou důležité zejména vzhledem k rozdělené architektuře Open RAN, kde různé komponenty a funkce mohou být poskytovány odlišnými dodavateli.

Zranitelnosti a bezpečnostní výzvy řízení a správy sítě Open RAN se týkají především automatizace a inteligentního řízení, sdílení informací a celkové koordinace.

2.2.1 Automatizace a inteligentní řízení

Open RAN podporuje pokročilou automatizaci a využívání umělé inteligence (AI) a strojového učení (ML) pro dynamické řízení a optimalizaci sítě. Tyto technologie umožňují efektivnější správu zdrojů, lepší kvalitu služeb a snižují náklady, jsou také spojeny **s potenciálními zranitelnosti, jako jsou**:

- Zneužití automatizačních skriptů a algoritmů: Útočníci se mohou pokusit manipulovat s automatizačními procesy nebo vstupy AI/ML modelů, aby narušili operace sítě nebo získali neautorizovaný přístup.
    - Zranitelnosti v algoritmech a jejich implementaci - algoritmy AI/ML mohou obsahovat chyby nebo mohou být špatně implementovány, což může vést k nesprávným rozhodnutím nebo k exploataci ze strany útočníků.
        - Chyby v kódu: Bugy nebo chyby v implementaci AI/ML algoritmů mohou vést k nesprávným výsledkům nebo ke zhroucení systémů.
        - Nedostatečná robustnost: Algoritmy, které nejsou dostatečně robustní, mohou být citlivé na malé změny v datech nebo mohou být snadno oklamány speciálně vytvořenými vstupy.
    - Zranitelnost v důsledku nesprávné konfigurace automatizovaných rozhodovacích systémů a limitů rozhodovacích systémů - automatizované systémy rozhodování mohou výrazně zefektivnit správu sítě, ale pokud nejsou správně navrženy nebo konfigurovány, mohou způsobit vážné problémy.
        - Falešně pozitivní/negativní výsledky: AI/ML modely mohou generovat falešně pozitivní nebo negativní výsledky, což může vést k nežádoucím akcím, jako je blokování legitimních uživatelů nebo povolení škodlivého provozu.
        - Přetížení systému: Automatizované systémy mohou provádět akce, které vedou k přetížení nebo nestabilitě sítě, pokud nejsou správně kalibrovány nebo monitorovány

- Narušení zabezpečení dat pro AI/ML: Kvalita a bezpečnost dat používaných pro trénování AI/ML modelů je klíčová. Škodlivá nebo zkreslená data mohou vést k nesprávným rozhodnutím nebo zranitelnostem.
    - Manipulace s trénovacími daty: Útočníci mohou úmyslně vkládat škodlivá nebo zkreslená data do trénovací sady, což vede k vytvoření modelů, které dělají chybné předpovědi nebo rozhodnutí.
    - Útoky typu „poisoning“: Při poisoning útocích jsou trénovací data záměrně infikována tak, aby modely generovaly předem určené chyby nebo zranitelnosti.

Potenciální zranitelnosti v AI/ML **se zejména eliminují zavedením následujících opatření:**

- Kvalitní a bezpečná trénovací data – zajištění, aby trénovací data byla čistá, relevantní a bez škodlivých vzorů formou:
    - Validace a filtrace dat: Implementovat procesy pro validaci a filtrování trénovacích dat, aby se zajistila jejich kvalita a integrita.
    - Monitorování a auditování datových zdrojů: Pravidelně monitorovat a auditovat zdroje trénovacích dat, aby se zabránilo vniknutí škodlivých nebo zkreslených dat.
- Robustní algoritmy a implementace – vývojem a implementací robustních AI/ML algoritmů, které jsou odolné vůči různým typům útoků a chyb, aplikované alespoň:
    - Testováním a validací algoritmů: Provádět důkladné testování a validaci AI/ML algoritmů před nasazením do produkčního prostředí.
    - Red teamingem a penetračním testováním: Využívat red teaming a penetrační testování k identifikaci a opravě potenciálních zranitelností v AI/ML systémech.
- Monitorování a správa automatizovaných systémů- zajištění nepřetržitého monitorování a správy automatizovaných systémů, aby byly včas identifikovány a řešeny případné problémy. Představuje zejména opatření:
    - Průběžného monitorování výkonu: Implementovat nástroje pro průběžné monitorování výkonu a chování AI/ML modelů a automatizovaných systémů.
    - Alertingu a incident response: Zavést systém alertů a plán incident response pro rychlou reakci na případné anomálie nebo nesprávná rozhodnutí generovaná automatizovanými systémy.

2.2.2 Sdílení informací a koordinace

Open RAN pracuje se sdílením informací mezi různými sítěmi a s různými dodavateli, což se promítá do zvýšených požadavků na koordinaci a optimalizaci. Sdílení musí být pečlivě zabezpečeno, aby se zabránilo **úniku informací včetně těch citlivých** a aby přístup k relevantním datům získali pouze autorizované entity.

Ochrana v oblasti sdílení informací a koordinace se uskutečňuje na úrovni řízení přístupů a identity, uplatňováním bezpečnostních protokolů a standardů a monitorováním incidentů a včasným reagováním na ně.

- **Řízení přístupu a identity**

Zabezpečení přístupu k řídicím a správním funkcím zahrnuje zejména nastavení ve smyslu:

- Silné autentizace a autorizace uživatelů: Zajištěním, že pouze oprávněné osoby mohou provádět změny v konfiguraci sítě nebo přistupovat k citlivým datům.
- Role-based access control (RBAC): Definováním přístupových práv na základě rolí uživatelů v organizaci zajišťuje, že každý má přístup pouze k těm datům a operacím, které jsou pro jeho roli nezbytné.

- **Implementace bezpečnostních protokolů a standardů**

Implementace silných bezpečnostních protokolů a dodržování průmyslových standardů jsou klíčové pro zabezpečení komunikace a datových přenosů mezi různými komponentami sítě. Realizuje se prostřednictvím:

- Šifrování: Zajištění bezpečného přenosu dat mezi různými částmi sítě.
- Ověřováním integrity dat a autentizace původu dat: Ověření pravosti a integrity přenášených dat.

- **Monitorování a reakce na incidenty**

Průběžné monitorování sítě a rychlá reakce na bezpečnostní incidenty jsou nezbytné pro identifikaci a řešení potenciálních hrozeb. Spočívá pak zejména v:

- Detekci anomálií a narušení: Využití AI/ML pro identifikaci neobvyklých aktivit, které mohou naznačovat bezpečnostní hrozby.
- Plánováním a standardizací reakce na incidenty: Připravenost a schopnost rychle reagovat na bezpečnostní incidenty minimalizuje potenciální škody.

2.3 Dodavatelský řetězec Open RAN

Dodavatelský řetězec v kontextu Open RAN architektury přináší **výzvy a zranitelnosti** v důsledku jeho inherentně rozmanité a distribuované povahy. V Open RAN jsou tradiční, monolitické dodavatelské modely nahrazeny více otevřenými a modulárními přístupy, což umožňuje operátorům kombinovat řešení od různých výrobců. Zatímco to přináší značné výhody z hlediska flexibility a transparentnosti, inovací a možná i nákladů, je třeba počítat se zranitelnostmi a bezpečnostními výzvami níže uvedenými.

2.3.1 Bezpečnostní rizika více dodavatelů

Open RAN architektura umožňuje integraci komponent od různých dodavatelů. To snižuje závislost na jednom výrobci a může vést k inovacím a snížení nákladů. Nicméně, dodavatelský řetězec také přináší **specifická bezpečnostní rizika**, zvláště pokud zahrnuje rizikové dodavatele.

- Zranitelnosti na úrovni kompatibility a integrace - Komponenty od různých dodavatelů nemusí spolupracovat hladce a bezpečně. Různé bezpečnostní standardy a implementace mohou způsobit problémy s kompatibilitou.
    - Nekompatibilní bezpečnostní opatření: Rozdílné implementace bezpečnostních protokolů mohou vést k bezpečnostním mezerám, které mohou útočníci zneužít.
    - Slabé body v integraci: Nesprávně integrované systémy mohou vytvořit zranitelná místa, která mohou být cílem útoků.

- Zranitelnosti na úrovni kvality a bezpečnosti jednotlivých komponent - Kvalita a bezpečnost softwaru a hardwaru od různých dodavatelů se může výrazně lišit. Nízká kvalita nebo nedostatečně zabezpečené komponenty mohou ohrozit celou síť.
    - Nízká kvalita softwaru/hardwaru: Komponenty s nedostatečnými bezpečnostními opatřeními mohou být snadno zneužity.
    - Nezabezpečené aktualizace a záplaty: Pokud dodavatelé nedodávají pravidelné a bezpečné aktualizace, mohou komponenty zůstat zranitelné vůči novým hrozbám.

- Zranitelnosti na úrovni řízení přístupu a identity - Správa přístupových práv a ověřování identity mezi komponentami od různých dodavatelů může být složitá.
    - Slabé autentizační mechanismy: Pokud některý dodavatel používá slabé autentizační protokoly, může to umožnit neautorizovaný přístup k síti.
    - Nedostatečná kontrola přístupu: Chybějící nebo špatně nastavené kontrolní mechanismy mohou vést k neoprávněnému přístupu k síťovým zdrojům.

- Zranitelnosti spojené s rizikovými dodavateli - Dodavatelé z určitých regionů mohou představovat zvýšené riziko kvůli geopolitickým napětím, sankcím nebo legislativě, která může vyžadovat spolupráci s vládními agenturami.
    - Politicky motivované útoky: Dodavatelé mohou být nuceni spolupracovat s vládami na sledování nebo útocích proti zahraničním sítím.
    - Sankce a omezení: Dodavatelé mohou čelit sankcím, které ovlivňují jejich schopnost poskytovat bezpečné a aktuální produkty.

- Zranitelnosti spojené s nedůvěryhodnými dodavateli -Někteří dodavatelé mohou mít historii bezpečnostních incidentů, nedostatečné bezpečnostní postupy nebo mohou být přímo zapojeni do škodlivých aktivit.
    - Dodávka škodlivých komponent: Dodavatelé mohou záměrně nebo nedbalostí distribuovat komponenty obsahující škodlivý software nebo zranitelnosti.
    - Nedostatečné reakce na incidenty: Nedůvěryhodní dodavatelé mohou nedostatečně reagovat na bezpečnostní incidenty nebo neinformovat své zákazníky o zranitelnostech.

- Zranitelnosti spojené s útoky na dodavatelských řetězec (Supply Chain Attacks) - Útočníci mohou cílit na dodavatelský řetězec, aby vložili zranitelnosti nebo škodlivý software do komponent ještě před jejich doručením.
    - Kompromitace během výroby: Komponenty mohou být kompromitovány během výroby nebo přepravy.
    - Manipulace s aktualizacemi: Útočníci mohou manipulovat s aktualizačními procesy, aby zavedli škodlivé kódy.

Implementací těchto opatření mohou organizace lépe chránit své Open RAN sítě před bezpečnostními hrozbami spojenými s více dodavateli a rizikovými dodavateli, což přispívá k celkové odolnosti a bezpečnosti telekomunikační infrastruktury:

- Důkladným hodnocením a výběrem dodavatelů - Pečlivě vybírat dodavatele na základě jejich bezpečnostních postupů, historie a geopolitických rizik. Lze zajistit např.:
    - Bezpečnostními audity a certifikaci: Požadovat od dodavatelů pravidelné bezpečnostní audity a certifikace.
    - Hodnocením rizik: Provádět pravidelné hodnocení rizik spojených s jednotlivými dodavateli.
- Stanovením jasných požadavků a smluvních podmínek - Definování jasných bezpečnostních požadavků a smluvních podmínek, které dodavatelé musí splňovat.
    - Bezpečnostní požadavky: Jasně definovat bezpečnostní požadavky ve smlouvách, včetně pravidelných aktualizací a záplat, řízení přístupu a ochrany dat.
    - Sankce za nedodržení: Stanovit sankce za nedodržení bezpečnostních požadavků, aby se zajistilo, že dodavatelé budou motivováni dodržovat dohodnuté standardy.
- Monitoring dodavatelského výkonu: Zavedení systému pro průběžné monitorování výkonu dodavatelů, včetně sledování dodržování SLA (Service Level Agreements) a bezpečnostních standardů.
- Implementací silných bezpečnostních protokolů - Zavádět a vynucovat silné bezpečnostní standardy a autentizační protokoly mezi všemi komponentami sítě formou opatření:
    - Pevné autentizační protokoly: Implementovat robustní autentizační mechanismy, jako je PKI nebo Kerberos.
    - Šifrování a integrita dat: Zajistit, aby všechna data přenášená mezi komponentami byla šifrována a ověřena na integritu.
- Průběžným monitorováním a aktualizací - Průběžně monitorovat a aktualizovat všechny komponenty sítě, aby byly zabezpečené proti novým hrozbám. Hrozbám lze předcházet opatřeními:
    - Automatizované aktualizace: Implementovat systémy pro automatizované a bezpečné aktualizace softwaru a hardwaru.
    - Bezpečnostní monitoring: Zavést nástroje pro průběžné monitorování sítě a detekci anomálií nebo potenciálních útoků.

- Nasazením robustní správa a transparentnost dodavatelského řetězce - Zavést robustní správu a transparentnost dodavatelského řetězce a uplatňování správy formou:
    - Sledování dodavatelského řetězce: Používat nástroje a technologie pro sledování původu a integrity komponent během celého jejich životního cyklu.
    - Kontroly a audity: Pravidelně provádět audity a kontroly dodavatelského řetězce, aby se zajistila jeho bezpečnost.

2.3.2 Integrace a Kompatibilita včetně Interoperability v Open RAN

Integrace a kompatibilita jsou klíčovými faktory pro úspěšné nasazení Open RAN architektury, která využívá komponenty od různých dodavatelů. Interoperabilita se týká schopnosti těchto komponent spolupracovat bez problémů, což je nezbytné pro dosažení efektivní a bezpečné sítě. Nicméně, integrace a interoperabilita **přinášejí několik zranitelnosti a bezpečnostních výzev**, které je třeba pečlivě řídit.

- Nekompatibilita mezi různými dodavateli - Komponenty od různých dodavatelů musí být schopné spolupracovat bez problémů. Různé bezpečnostní standardy a implementace mohou způsobit problémy s kompatibilitou. Konkrétně pak:
    - Nekompatibilní bezpečnostní opatření: Rozdílné implementace bezpečnostních protokolů mohou vést k bezpečnostním mezerám, které mohou útočníci zneužít.
    - Slabé body v integraci: Nesprávně integrované systémy mohou vytvořit zranitelná místa, která mohou být cílem útoků.

- Nefunkční Interoperabilita mezi komponentami - Interoperabilita se týká schopnosti různých systémů a komponent pracovat společně efektivně a bezpečně. Nefunkční interoperabilita se vyskytuje jak v hardware, tak software a je spojena hlavně s:
    - Nesprávnou konfigurací: Nesprávná konfigurace může vést k tomu, že komponenty nebudou schopny spolu správně komunikovat, což může způsobit výpadky nebo bezpečnostní problémy.
    - Nejednotnou implementací standardů: Dodavatelé mohou implementovat standardy různými způsoby, což může vést k nesouladu a potenciálním bezpečnostním mezerám.

- Nedostatečné/neúplné testování a validace - Před nasazením do produkčního prostředí nemusí být zajištěno důkladné testování a validace všech komponent.
    - Nedostatečné testování: Pokud testování není dostatečně důkladné, mohou zůstat neodhalené chyby nebo zranitelnosti, které mohou být později zneužity.
    - Chyby v testovacích scénářích: Nesprávné nebo neúplné testovací scénáře mohou vést k falešnému pocitu bezpečí a funkčnosti.

- Chybějící aktualizace a záplaty – neúplné aktualizace a chybějící záplaty narušují bezpečnost a funkčnost sítě. Kompatibilita a interoperabilita nemusí být po aplikaci aktualizací zachována.
    - Neúplné aktualizace: Aktualizace mohou být neúplné nebo nesprávně implementované, což může vést k novým bezpečnostním problémům.
    - Problémy s kompatibilitou po aktualizaci: Po aplikaci aktualizace může dojít k problémům s kompatibilitou mezi různými komponentami.

- Závislosti na třetích stranách - Zvýšená závislost na třetích stranách pro kritické komponenty sítě znamená, že bezpečnost sítě může být ohrožena, pokud jedna z těchto třetích stran čelí bezpečnostnímu incidentu.

Potenciálním zranitelnostem v Integraci a Kompatibilitě včetně Interoperability v Open RAN **se lze vyhnout uplatňováním následujících opatření:**

- Standardizace a certifikace - Dodržování průmyslových standardů a certifikace pomáhá zajistit, že komponenty od různých dodavatelů budou kompatibilní a interoperabilní. Lze ji posílit zejména konkrétními opatřeními:
    - Standardizace protokolů: Implementovat a dodržovat standardizované protokoly a bezpečnostní opatření definovaná organizacemi jako O-RAN Alliance.
    - Certifikace komponent: Vyžadovat, aby všechny komponenty prošly certifikačním procesem, který ověřuje jejich kompatibilitu a bezpečnost.
- Důkladné testování a validace - Před nasazením do produkčního prostředí je nutné provést důkladné testování všech komponent, aby se zajistila jejich kompatibilita a interoperabilita. Účinnými opatřeními jsou:
    - Komplexní testovací scénáře: Vytvořit a provádět komplexní testovací scénáře, které pokrývají všechny možné interakce mezi komponentami.
    - Validace bezpečnostních opatření: Zahrnout do testování i validaci všech bezpečnostních opatření a protokolů.
- Dynamické řízení bezpečnostní politiky - Implementace dynamických nástrojů pro řízení bezpečnostní politiky umožňuje rychlou adaptaci na nové hrozby a změny v síti. Aplikuje se formou:
    - Centralizované správy politik: Používat centralizované nástroje pro správu bezpečnostních politik, které umožňují rychlé a efektivní nasazení změn.
    - Automatizací bezpečnostních aktualizací: Implementovat systémy pro automatizovanou aplikaci bezpečnostních aktualizací a záplat.

- Spolupráce a sdílení informací - Spolupráce mezi operátory, dodavateli a bezpečnostními organizacemi může pomoci identifikovat a řešit bezpečnostní hrozby efektivněji Usnadňují ji opatření:
  - Sdílení informací o hrozbách: Vytvořit mechanismy pro sdílení informací o bezpečnostních hrozbách mezi všemi zúčastněnými stranami.
  - Společné bezpečnostní cvičení: Provádět společná bezpečnostní cvičení a testy, které zahrnují všechny zúčastněné strany, aby se zlepšila připravenost na bezpečnostní incidenty.
- Správa klíčů a certifikátů - Efektivní správa kryptografických klíčů a certifikátů je nezbytná pro zajištění bezpečné komunikace mezi komponentami.
  - Bezpečné generování a ukládání klíčů: Implementovat robustní systémy pro generování a ukládání kryptografických klíčů.
  - Automatizovaná správa certifikátů: Používat nástroje pro automatizovanou správu certifikátů, včetně jejich obnovy a revokace.
- Transparentnost a ověřování - Zajištění transparentnosti a ověřování bezpečnosti a původu komponent a softwaru ve složitém dodavatelském řetězci je klíčové. To zahrnuje důkladné posouzení bezpečnosti dodavatelů a jejich produktů před integrací do sítě, sledování a auditování softwaru a hardware, a zabezpečení proti zneužití, jako je vkládání škodlivého kódu nebo skrytých zadních vrátek.
- Zavedení centralizovaného systému správy záplat a aktualizací - Systémové záplaty a aktualizace jsou nezbytné pro řešení zranitelností. V prostředí Open RAN, kde komponenty pocházejí od různých dodavatelů, pak může být koordinace a aplikace těchto aktualizací složitější a zvyšuje se tak riziko, že některé komponenty zůstanou neaktualizované a zranitelné.
- Omezování závislosti na třetích stranách - Robustní řízení rizik, který zahrnuje všechny úrovně dodavatelského řetězce a důsledné vyžadování opatření pro řízení incidentů u všech dodavatelů umožní reagovat na bezpečnostní incidenty účinně a včas.

2.4 Softwarově definovaná síť (SDN) a virtualizace funkcí síťových prvků (NFV) Open Core

Jedním z klíčových prvků Open Core je použití technologií softwarově definovaných sítí (SDN) a virtualizace funkcí síťových prvků (NFV). Tyto technologie umožňují oddělení hardwarové infrastruktury od softwaru. Open Core v kontextu 5G sítí se odkazuje na použití otevřeného softwaru a standardů v jádru (core) sítě, které umožňují větší flexibilitu, snadnější integraci nových technologií a potenciálně snížení nákladů., které s sebou přinášejí **specifické zranitelnosti a bezpečnostní výzvy**.

V této části se zaměříme na zranitelnosti na úrovni SW, na úrovni HW virtualizace a v souvislosti s interoperabilitou a integrací Open Core.

2.4.1 Softwarově definované sítě (SDN)

SDN umožňuje operátorům efektivně řídit síťový provoz skrze centralizovaný softwarový systém. Toto oddělení kontrolní roviny (řídící logiky) od datové roviny (přeposílání dat) umožňuje dynamické spravování sítě. **Bezpečnostní výzvy zahrnují:**

- Zranitelnosti v řídicí rovině: Jelikož řídicí rovina SDN může řídit celou síť, její kompromitace může mít závažné důsledky, včetně možnosti přesměrování nebo blokování síťového provozu.
- Útoky na rozhraní mezi řídicí a datovou rovinou: Toto rozhraní je klíčové pro správné fungování SDN. Útočníci se mohou pokusit o vkládání škodlivého kódu nebo odposlech komunikace.
- Centralizace jako bod selhání: Centralizovaná řídicí rovina zvyšuje riziko "single point of failure", kde kompromitace centrálního systému může ovlivnit celou síť.

2.4.2 Virtualizace funkcí síťových prvků (NFV)

NFV umožňuje nasazení síťových služeb jako softwarových instancí na standardním hardwaru, což snižuje potřebu dedikovaného síťového hardwaru. **Bezpečnostní výzvy zahrnují:**

- Zranitelnosti ve virtualizační vrstvě: Hypervizory a další komponenty používané pro virtualizaci mohou obsahovat zranitelnosti, které umožňují útočníkům uniknout z virtuálního stroje a ovlivnit hostitelský systém nebo jiné virtuální stroje.
- Zranitelnosti v řízení a v souvislosti s izolací virtuálních síťových funkcí (VNF): Nesprávná konfigurace nebo správa VNF může vést k bezpečnostním zranitelnostem, včetně nedostatečné segmentace mezi VNFs, což může umožnit šíření útoků v síti.

- Zranitelnost v řízení přístupu a identity: V prostředí NFV nemusí být zajištěno, že pouze autorizované entity mohou spravovat a přistupovat k VNFs a nejsou nasazeny robustní systémy pro řízení přístupu a autentizaci, což může usnadnit útočníkům kompromitaci v síti.

Zabezpečení v Open Core architektuře, zejména v kontextu SDN a NFV, vyžaduje komplexní přístup, který zahrnuje pečlivé plánování, implementaci a průběžné monitorování. Důležité je přijmout opatření pro zabezpečení řídicí roviny, zajistit bezpečnou komunikaci mezi řídicí a datovou rovinou, chránit virtualizační infrastrukturu, a zavést efektivní řízení přístupu a identit. To vyžaduje nejen technologická řešení, ale i pečlivou správu a školení zaměstnanců, aby byli obeznámeni s potenciálními hrozbami a nejlepšími postupy pro jejich mitigaci.

2.5 Interoperabilita a integrace Open Core

Interoperabilita v Open Core 5G sítích znamená, že komponenty a systémy od různých dodavatelů musí spolehlivě a bezpečně spolupracovat. Tato spolupráce se může týkat různých aspektů sítě, od hardwaru až po softwarové aplikace. Je klíčová pro využití výhod otevřené architektury a modulárních, efektivních a agilních core sítí. Urychlení inovací v souvislosti s využitím Open Core s sebou přináší i **unikátní zranitelnosti a bezpečnostní výzvy**, které vyžadují zvýšenou pozornost z hlediska bezpečnosti.

- Zranitelnosti spojené s interoperabilitou:
    - Nejednotnost bezpečnostních standardů a implementací: Rozdílné bezpečnostní postupy a technologie mohou vést k zranitelnostem v síti, kde se střetávají různé systémy.
    - Kompatibilita bezpečnostních protokolů: Zajištění, že všechny komponenty sítě používají kompatibilní a aktualizované bezpečnostní protokoly, je zásadní pro prevenci úniku dat a útoků.
    - Správa kryptografických klíčů: Bezpečná výměna a správa kryptografických klíčů mezi různými systémy vyžaduje robustní řešení, která podporují interoperabilitu.

- Zranitelnosti spojené s Integracemi různorodých systémů:
    - Konfigurační a aktualizační chyby: Nesprávná konfigurace nebo zpožděné aplikace aktualizací a záplat mohou otevřít nové bezpečnostní mezery v integrovaných systémech.
    - Složitost síťového designu: Větší složitost může ztížit identifikaci a řešení bezpečnostních hrozeb. Efektivní nástroje pro správu a monitorování sítě jsou nezbytné pro přehlednost a bezpečnost.
    - Zabezpečení API a rozhraní: Integrace často závisí na API a programovatelných rozhraních, které musí být pečlivě zabezpečeny proti neoprávněnému přístupu a útokům.

Pro řešení výzev interoperability a integrace v Open Core 5G sítích je důležité **zavést několik klíčových bezpečnostních opatření:**

- Dynamické řízení bezpečnostní politiky: Využití centralizovaných nástrojů pro dynamické řízení bezpečnostní politiky umožňuje vytvoření adaptivní a proaktivní bezpečnostní architektury v Open RAN sítích. V kontextu stále se měnících hrozeb a různorodého prostředí, kde komponenty pocházejí od různých dodavatelů, je nutné, aby bezpečnostní politika byla nejen robustní, ale také flexibilní a schopná rychle reagovat na nové bezpečnostní výzvy

- Standardizace a certifikace: Podpora a dodržování standardizovaných protokolů a bezpečnostních pravidel pomáhá zajišťovat kompatibilitu a bezpečnost. Certifikace od renomovaných organizací může poskytnout důvěru v bezpečnostní postupy dodavatelů.

- Důkladné testování: Před nasazením do produkčního prostředí je nutné provést důkladné testování interoperability a bezpečnosti, včetně simulačních útoků a penetračního testování.

- Pečlivá správa klíčů a certifikátů: Zabezpečení kryptografických algoritmů, včetně správy klíčů a certifikátů, je zásadní pro zajištění důvěrnosti a integrity komunikace.

- Spolupráce a sdílení informací o hrozbách: Spolupráce mezi operátory, dodavateli a bezpečnostními organizacemi může pomoci identifikovat a řešit bezpečnostní hrozby efektivněji.

Zastavíme se u hlavního pilíře bezpečnostních opatření - dynamické řízení bezpečnostní politiky a ve větším detailu si představíme kromě jednotlivých přínosů i hlavní prvky dynamického řízení.

1. Adaptivita k měnícím se hrozbám - Dynamické řízení umožňuje rychlou adaptaci na nové bezpečnostní hrozby a zranitelnosti. Řízení zahrnuje aktualizaci pravidel a politik v reálném čase, aby bylo možné okamžitě reagovat na nové typy útoků nebo objevené zranitelnosti. Hlavní prvky, které přínosy naplňují:
    - Centralizovaná správa bezpečnostních politik - Zjednodušuje proces řízení a zajišťuje konzistenci napříč celou sítí. Centralizace rovněž umožňuje lepší přehled a kontrolu nad celou bezpečnostní infrastrukturou.

- Automatizace bezpečnostních procesů - Dynamické řízení zahrnuje automatizaci klíčových bezpečnostních procesů, jako jsou detekce a reakce na incidenty, správa záplat a aktualizací, a implementace bezpečnostních pravidel. Automatizace zvyšuje efektivitu a snižuje riziko lidských chyb.

2. Rychlost a kontinuita spolupráce klíčových komponent dynamického řízení bezpečnostní politiky
   - Real-time monitorování a analýza - Implementace nástrojů pro kontinuální monitorování síťového provozu a detekci anomálií. Real-time analýza umožňuje rychlé identifikování podezřelých aktivit a potenciálních bezpečnostních incidentů.
   - Orchestrace bezpečnostních politik - Použití orchestračních nástrojů, které umožňují dynamické nasazení a aktualizaci bezpečnostních politik napříč různými komponentami sítě. To zajišťuje, že všechny části sítě jsou synchronizovány a dodržují aktuální bezpečnostní standardy.
   - Inteligentní reakce na incidenty - Využití umělé inteligence (AI) a strojového učení (ML) pro inteligentní detekci a reakci na bezpečnostní incidenty. Tyto technologie mohou identifikovat vzorce útoků, předvídat budoucí hrozby a automaticky nasazovat protiopatření.
3. Snadné a předvídatelné implementační kroky pro dynamické řízení bezpečnostní politiky
   - Nasazení centralizovaného řízení - Implementace centralizovaného systému pro správu bezpečnostních politik, který umožňuje snadné nasazení a aktualizaci pravidel a politik z jednoho místa.
   - Integrace automatizačních nástrojů - Použití nástrojů pro automatizaci bezpečnostních procesů, jako jsou nástroje pro správu záplat, aktualizace a detekci incidentů. Automatizace by měla zahrnovat schopnost automaticky reagovat na identifikované hrozby.
   - Pravidelné aktualizace a testování - Pravidelné aktualizace bezpečnostních politik a pravidel, založené na nejnovějších informacích o hrozbách. Implementace procesu pro pravidelné testování a auditování těchto politik, aby byla zajištěna jejich účinnost.
   - Školení a vzdělávání personálu - Zajištění, že personál je pravidelně školen a obeznámen s dynamickými bezpečnostními politikami a nástroji. To zahrnuje školení na identifikaci a reakci na bezpečnostní incidenty a používání automatizačních nástrojů.

2.6 Aktualizace a správa záplat Open Core

Aktualizace a správa záplat jsou klíčové aspekty zabezpečení pro jakýkoli software, včetně těch, které tvoří jádro (core) 5G sítí využívající Open Core architekturu. V prostředí Open Core, kde je základem větší míra softwarového řešení a virtualizace, je důležité efektivně spravovat aktualizace a záplaty pro různé softwarové komponenty. I tak je proces aktualizace a správy záplat Open Core vystaven **zranitelnostem a bezpečnostním výzvám**, které uvádí další text.

- Rychlost vydávání záplat: Vzhledem k tomu, že bezpečnostní hrozby se neustále vyvíjejí, dodavatelé softwaru musí rychle reagovat vydáváním záplat. Organizace musí tyto záplaty stejně rychle implementovat, což může být logisticky náročné. Logisticky náročné znamená, že proces vydávání, distribuce a aplikace záplat vyžaduje komplexní koordinaci a zdroje, aby byl proveden efektivně a bez narušení provozu sítě.
  - Nekomplexní pokrytí: Všechny týmy nejsou koordinované a synchronizované, záplatování není plánované a komunikované.
  - Různí dodavatelé: Každý z dodavatelů může mít odlišné postupy a časové rámce pro vydávání záplat.
  - Geografická rozptýlenost: Nasazení záplaty na různých geografických místech přidává další úroveň složitosti, protože různé regiony mohou mít různé požadavky a časové zóny.
  - Narušení služeb: Záplatování neproběhne s minimálním dopadem na zákaznické služby.

- Kompatibilita a závislosti: V prostředí s více dodavateli mohou aktualizace od jednoho dodavatele ovlivnit funkčnost nebo bezpečnost komponent od jiných dodavatelů. Řízení závislostí a kompatibility je klíčové pro udržení stabilní a bezpečné sítě.

- Automatizace versus ruční zásahy: I když automatizace může pomoci zefektivnit proces aplikace záplat, některé aktualizace mohou vyžadovat ruční zásahy nebo konfiguraci, což zvyšuje složitost správy.

Pro vykreslení logistické náročnosti v procesu záplatování popíšeme na příkladu telekomunikační společnost s Open Core architekturou postup, který musí organizace projít, aby jakékoliv nové bezpečnostní záplaty byly nasazeny co nejdříve po jejich vydání.

1. Identifikace zranitelnosti - Bezpečnostní tým společnosti identifikuje novou zranitelnost v jednom z komponent od dodavatele A. Dodavatel A rychle vydá záplatu pro tuto zranitelnost.
2. Distribuce záplaty - Záplata musí být distribuována na všechna místa, kde je komponenta od dodavatele A nasazena. To zahrnuje několik datových center a stovky základnových stanic.
3. Testování záplaty - Před nasazením záplaty v produkčním prostředí musí být záplata důkladně otestována, aby se zajistilo, že nezpůsobí další problémy nebo neslučitelnosti s jinými komponentami. Tento krok zahrnuje testování v laboratorních podmínkách a simulaci reálných scénářů.
4. Koordinace mezi týmy - Nasazení záplaty vyžaduje koordinaci mezi několika týmy, tj. bezpečnostním týmem, týmem pro správu infrastruktury a operativními týmy v různých datových centrech. Každý tým musí být synchronizován a připraven k aplikaci záplaty ve stejném časovém rámci, aby se minimalizovalo narušení provozu.

5. Nasazení záplaty - Záplata musí být aplikována v předem naplánovaném okně údržby, aby se minimalizoval dopad na služby zákazníkům. Vzhledem k tomu, že společnost poskytuje služby v různých časových zónách, musí být záplatování pečlivě naplánováno, aby se vyhnulo špičkovým hodinám provozu.
6. Monitoring po nasazení - Po nasazení záplaty je nutné průběžné monitorování sítě, aby se zajistilo, že nedošlo k žádným nechtěným vedlejším účinkům. To zahrnuje sledování výkonu sítě, hlášení incidentů a zpětnou vazbu od zákazníků.

Efektivní správa aktualizací a záplat je zásadní pro udržení bezpečnosti a stability Open Core 5G sítí. **Implementací těchto doporučených opatření** mohou organizace lépe chránit svou infrastrukturu před neustále se měnícími bezpečnostními hrozbami.

- Pravidelnou inventarizací a hodnocením: Udržovat aktuální přehled o všech softwarových komponentách a jejich verzích v síti. Pravidelně hodnocení a kategorizace softwarové komponenty podle jejich bezpečnostního rizika a důležitosti pro síťovou infrastrukturu napomáhá rychlé reakci.

- Automatizovaným sledováním a nasazováním záplat: Využívat nástroje pro automatizované sledování bezpečnostních zranitelností a aplikaci záplat pomáhá zmenšit časové okno a snížit riziko lidských chyb, kdy může být síť vystavena známým hrozbám.

- Testování před nasazením: Před aplikací záplat nebo aktualizací v produkčním prostředí je důležité provést testování v izolovaném prostředí. To pomáhá identifikovat potenciální problémy s kompatibilitou nebo negativní dopady na výkon předtím, než ovlivní kritickou infrastrukturu.

- Postupy pro nouzové záplatování: Vypracovat a udržovat postupy pro rychlé záplatování v případě objevení kritických bezpečnostních zranitelností, které vyžadují okamžitou reakci. To zahrnuje možnost provádět mimořádné aktualizace mimo pravidelný aktualizační cyklus.

- Školení a osvěta zaměstnanců: Zajistit, aby zaměstnanci odpovědní za správu a bezpečnost sítě byli pravidelně školeni a informováni o nejlepších postupech pro správu záplat a aktualizací, stejně jako o potenciálních hrozbách a způsobech jejich řešení.

- Koordinace s dodavateli: Udržování úzké spolupráce a komunikace s dodavateli, aby bylo možné rychle reagovat na nové hrozby a zajistit rychlé vydání a aplikaci záplat.

3 Zhodnocení potenciálních dopadů na celkovou bezpečnost dané mobilní sítě

Zhodnocení potenciálních dopadů na celkovou bezpečnost 5G mobilních sítí zahrnuje rozbor různých aspektů, od technologických po operacionální a strategické. 5G sítě, jakožto nástupce 4G, přináší významné vylepšení v rychlosti, kapacitě a odezvě, avšak s tím se pojí i nové bezpečnostní výzvy.

Hlavní potenciální dopady, které popisuje následující text, souvisí se samotnými vlastnostmi sítě – open architektury, automatizací/inovacemi, softwarem, virtualizací a dodavatelským řetězcem.

3.1 Rozšíření vstupních bodů a vektorů útoku

Rozšíření vstupních bodů[1] a vektorů[2] útoků v 5G sítích vyžaduje detailnější pohled na to, jak 5G technologie rozšiřuje možnosti pro potenciální útočníky a jaké konkrétní výzvy to přináší pro bezpečnostní týmy.

3.1.1 Rozšíření fyzické přístupnosti v rámci distribuované architektury 5G sítí

5G sítě jsou navrženy s velmi distribuovanou architekturou, která integruje mnoho malých buněk (small cells) pro poskytování vysoké rychlosti a nízké latence. Tyto malé buňky jsou rozmístěny ve veřejných prostorách, včetně městských oblastí, což zvyšuje fyzickou přístupnost a potenciální riziko před útoky.

3.1.2 Další cesty přes IoT zařízení

S rozmachem 5G exponenciálně narůstá počet připojených IoT zařízení, která se stávají součástí sítě. Mnoho těchto zařízení má neadekvátní zabezpečení, což poskytuje útočníkům nové cesty k infiltrovaní sítí a provádění útoků.

3.1.3 Využití nižšího zabezpečení v edge computingu

5G sítě využívají edge computing pro zpracování dat blíže ke zdroji, což snižuje latenci. Nicméně, edge servery mohou být zranitelné vůči útokům, jelikož se nacházejí v méně zabezpečených lokacích a mohou obsahovat citlivá data.

3.1.4 Neadekvátní úroveň identifikace a autentizace rostoucího počtu zařízení

Zajištění, že každé zařízení připojené k síti je legitimní a není kompromitováno, je klíčové. To vyžaduje robustní mechanismy identifikace a autentizace, které jsou schopné zvládnout obrovské množství zařízení v 5G sítích.

---

[1] Definice Rozšíření vstupních bodů útoku: Rozšíření vstupních bodů útoku se vztahuje na celkový rozsah a počet potenciálních vstupních bodů (zranitelností) do systému, které mohou útočníci využít k provedení útoku.

[2]

Definice Širší vektor Útoku: Širší vektor útoku se zaměřuje na různé způsoby a metody, které mohou útočníci použít k proniknutí do systému. To zahrnuje různé techniky a taktiky, které mohou být využity k útoku na systém.

3.1.5 Logisticky náročné nasazování aktualizací a správy rostoucího počtu zařízení

Správa a pravidelné aktualizace softwaru zařízení jsou nezbytné pro udržení jejich bezpečnosti. V prostředí 5G sítí to představuje logistickou výzvu vzhledem k rozsáhlému počtu zařízení.

3.1.6 Dílčí kompromitace sítě s dopadem na celou síťovou infrastrukturu

Pro minimalizaci rizik spojených s rozšíření vstupních bodů a vektorů útoků je důležité implementovat segmentaci[3] a izolaci[4] v rámci 5G sítě. Tím se zajistí, že kompromitace jedné části sítě neovlivní celou síťovou infrastrukturu.

Zabezpečení 5G sítí v kontextu rozšíření vstupních bodů a vektorů útoků vyžaduje komplexní a vrstvený přístup. Je nezbytné investovat do pokročilých technologií pro detekci a reakci na hrozby, jakož i do vzdělávání a osvěty uživatelů o bezpečnostních rizicích. Spolupráce mezi operátory, výrobci zařízení, softwarovými vývojáři a vládními agenturami je klíčová pro vytvoření odolné a bezpečné 5G síťové infrastruktury.

3.2 Dopady na bezpečnost celé sítě vlivem závislosti na softwaru a virtualizaci

Závislosti 5G sítí na softwaru a virtualizaci, s sebou přináší specifické bezpečnostní výzvy. Tato závislost umožňuje rychlé nasazování nových služeb a inovací, ale zároveň zvyšuje riziko softwarových chyb a zranitelností, které mohou útočníci využít.

- Software-Defined Networking (SDN) a Network Functions Virtualization (NFV): - 5G sítě významně využívají SDN a NFV pro flexibilní správu a konfiguraci síťových funkcí. Současně se s flexibilitou zvyšuje potenciál distribuce nebezpečného softwaru a chyb ve virtualizaci do síťové infrastruktury.

- Dynamic Update and Configuration: - Možnost dynamické aktualizace a konfigurace síťových funkcí znamená, že softwarové komponenty mohou být často aktualizovány nebo měněny. Častá změna naopak může urychlit a ovlivnit zavedení nových zranitelností nebo nestabilit do systému.

- Rozšířené softwarové zranitelnosti - Závislost 5G sítí na softwaru znamená, že jakákoli softwarová zranitelnost může mít dalekosáhlé dopady na bezpečnost celé sítě. Útočníci mohou těchto zranitelností využít k získání neoprávněného přístupu, šíření malwaru, nebo provádění denial-of-service (DoS) útoků.

3.2.1 Zvýšené nároky na aktualizaci a rychlost oprav softwarových komponent

Je klíčové zajistit, aby všechny softwarové komponenty byly pravidelně aktualizovány a zabezpečeny proti známým zranitelnostem. To vyžaduje pečlivé sledování bezpečnostních upozornění a rychlou aplikaci oprav.

3.2.2 Zvýšené nároky na vytváření bezpečnostních zón a kontrolních bodů

Uplatnění principů segmentace a izolace na virtuální síťové funkce může pomoci omezit rozsah potenciálních útoků. Vytváření bezpečnostních zón a kontrolních bodů mezi virtuálními funkcemi a službami může zamezit šíření útoků v rámci sítě.

3.2.3 Zvýšené nároky na bezpečnostní testování a ověřování

Intenzivní bezpečnostní testování a ověřování softwaru před jeho nasazením je nezbytné. To zahrnuje použití statické a dynamické analýzy kódu, penetračního testování a revizí zabezpečení k identifikaci a odstranění zranitelností.

[3] Segmentace sítě: Segmentace sítě je proces rozdělení jedné fyzické sítě na více menších, logických sítí, které jsou odděleny a řízeny na základě specifických bezpečnostních politik a potřeb. Zaměřuje se na rozdělení jedné fyzické sítě do menších, logických segmentů, aby se zlepšila správa a bezpečnost komunikace mezi různými částmi sítě.

[4] Izolace sítě: Izolace sítě je proces zajištění, že určité části sítě nebo specifická zařízení nemohou přímo komunikovat s jinými částmi sítě nebo zařízeními, pokud to není explicitně povoleno.Zaměřuje se na zamezení nebo omezení přímé komunikace mezi specifickými částmi sítě, aby se zajistila ochrana kritických systémů a dat.

3.2.4 Hlubší dopad Insider threats

Vzhledem k tomu, že správa a údržba 5G sítí vyžaduje vysoký stupeň přístupu k softwaru a konfiguračním nástrojům, je důležité zavést opatření proti insider threats (hrozbám zevnitř organizace), včetně přístupových práv a monitorování aktivit.

Zabezpečení 5G sítí v kontextu jejich závislosti na softwaru a virtualizaci vyžaduje nejen technická opatření, ale také pečlivé procesní a organizační přístupy. Společnosti a organizace musí investovat do vzdělávání svých týmů, vývoje bezpečnostních politik a procedur, a v neposlední řadě v implementaci pokročilých bezpečnostních nástrojů a technologií pro ochranu proti neustále se vyvíjejícím hrozbám.

3.3 Složitý a rozsáhlý řetězec dodavatelů

5G sítě jsou závislé na rozsáhlém a složitém řetězci dodavatelů, který zahrnuje výrobce hardwaru, poskytovatele softwaru, a služeb telekomunikační infrastruktury. Každý z těchto dodavatelů může představovat potenciální bezpečnostní riziko, pokud jejich produkty nebo služby obsahují zranitelnosti.

3.3.1 Vyšší míra ověřování zabezpečení a produktů

Zajištění, že všechny komponenty a software používané v 5G sítích jsou bezpečné a neobsahují skryté zranitelnosti nebo backdoors, je nesmírně náročné. Zranitelnosti mohou být v produktech záměrně nebo nezáměrně, což zvyšuje riziko špionáže, sabotáže nebo jiných kybernetických útoků.

3.3.2 Nesnáze při výběru dodavatelů a jejich vyloučení

Výběr dodavatelů může být také ovlivněn geopolitickými faktory, kdy určité země nebo regiony mohou představovat vyšší riziko z hlediska špionáže nebo ovlivňování. Toto riziko může vést k vyloučení některých dodavatelů na základě národní bezpečnosti.

Geopolitické riziko v kontextu 5G sítí odkazuje na bezpečnostní výzvy a rizika spojená s politickými a ekonomickými faktory mezi různými zeměmi a regiony. Toto riziko může ovlivňovat výběr dodavatelů, důvěryhodnost technologických řešení a celkovou bezpečnost telekomunikační infrastruktury. **Následující body rozvádějí hlavní dopady geopolitického rizika:**

- Mezinárodní sankce a omezení:- Sankce a omezení uvalené na určité země mohou ovlivnit dodávky technologií a komponent potřebných pro budování a provoz 5G sítí. Například, sankce USA vůči Číně ovlivnily schopnost čínských výrobců jako Huawei dodávat technologie do jiných zemí.

- Politická nestabilita: - Politická nestabilita v některých regionech může vést k nejistotám a narušení dodavatelských řetězců. Investice do infrastruktury v těchto oblastech mohou být riskantní, což může ovlivnit globální dodavatelské řetězce.

- Obavy z kyberšpionáže: - Existují obavy, že určité země mohou využívat technologické společnosti k provádění kyberšpionáže. Například obvinění, že čínské firmy jako Huawei mohou být využívány čínskou vládou ke špionážním účelům, vedla k vyloučení těchto firem z budování 5G sítí v několika zemích.

- Kritická Infrastruktura: - 5G sítě jsou považovány za kritickou infrastrukturu, což znamená, že jejich zabezpečení je klíčové pro národní bezpečnost. Výběr dodavatelů proto musí být prováděn s ohledem na důvěryhodnost a rizika spojená s národní bezpečností.

- Obchodní války - Obchodní války a ekonomické konflikty mezi zeměmi mohou ovlivnit dostupnost a cenu technologií a komponent pro 5G sítě. Například obchodní konflikty mezi USA a Čínou vedly k zvýšení cen některých technologických produktů.

- Technologická závislost - Závislost na technologiích a komponentech z jedné země může představovat riziko. Pokud dojde k politickým konfliktům nebo sankcím, může to výrazně ovlivnit dostupnost potřebných technologií. Diversifikace dodavatelských řetězců je tedy důležitá pro minimalizaci tohoto rizika.

3.3.3 Závislost na klíčových dodavatelích

Silná závislost na několika málo klíčových dodavatelích může znamenat vysoké riziko, pokud by došlo ke kompromitaci jejich produktů, služeb nebo dodavatelských řetězců. Diverzifikace dodavatelů může pomoci zmírnit toto riziko, ale může být logisticky a finančně náročná.

3.3.4 Zvýšené nároky na přezkum dodavatelů

Přezkum a certifikace[5] dodavatelů podle bezpečnostních standardů je základním krokem k zajištění bezpečnosti. To zahrnuje hodnocení bezpečnostních postupů dodavatelů, jejich dodržování průmyslových standardů a způsobů ochrany proti kybernetickým hrozbám.

3.3.5 Zvýšené nároky na kontrolu dodržování smluv a auditování

Kontraktualní opatření[6] a auditování[7] jsou klíčové strategie pro zajištění bezpečnosti a důvěryhodnosti dodavatelského řetězce, zejména v kontextu 5G sítí. Tyto postupy zahrnují formální smluvní dohody, které stanovují specifické požadavky na bezpečnost, a pravidelné audity, které ověřují, že dodavatelé dodržují tyto požadavky. Kontroly kontraktualních opatření a auditování mohou minimalizovat rizika a zajistit, že jejich dodavatelé poskytují bezpečné a spolehlivé služby.

Níže jsou rozvedeny hlavní části kontraktuálních opatření a auditování pro představu konkrétních nároků a změn v rámci kontrol/auditů:

1. Specifikace bezpečnostních požadavků - Smlouvy obsahují konkrétní požadavky na bezpečnostní opatření, které musí dodavatel implementovat. To může zahrnovat šifrování dat, řízení přístupu, bezpečnostní školení zaměstnanců a pravidelné aktualizace softwaru.
2. Dodržování standardů - Dodavatelé jsou povinni dodržovat specifické bezpečnostní standardy a normy (např. ISO 27001, GDPR), které zajišťují, že jejich procesy a systémy splňují požadovanou úroveň bezpečnosti.
3. Práva a povinnosti - Smlouvy jasně definují práva a povinnosti obou stran, včetně povinností dodavatelů v případě bezpečnostního incidentu, odpovědnosti za škody a sankcí za nedodržení smluvních podmínek.
4. Bezpečnostní kontroly - Smlouvy mohou obsahovat ustanovení o pravidelných bezpečnostních kontrolách, které zajistí, že dodavatelé neustále plní stanovené bezpečnostní požadavky.
5. Pravidelné audity - Organizace provádějí pravidelné audity dodavatelů, aby ověřily dodržování smluvních podmínek a bezpečnostních standardů. Audity mohou být plánované nebo neohlášené.
6. Externí a interní audity:- Audity mohou být prováděny interně zaměstnanci organizace nebo externími certifikovanými auditory, kteří poskytují nezávislé hodnocení bezpečnostních opatření dodavatelů.
7. Hodnocení zranitelností - Audity zahrnují identifikaci a hodnocení zranitelností v systémech a procesech dodavatelů. To může zahrnovat penetrační testy, kontrolu dodržování bezpečnostních politik a analýzu bezpečnostních incidentů.
8. Nápravná opatření - Pokud audity odhalí nedostatky nebo zranitelnosti, dodavatelé jsou povinni implementovat nápravná opatření a zlepšení. Organizace mohou stanovit lhůty pro provedení těchto opatření a sledovat jejich plnění.

3.3.6 Tlak na diverzifikaci dodavatelů

Diverzifikace dodavatelů a zajištění, že neexistuje nadměrná závislost na jednom dodavateli, může zvýšit odolnost proti rizikům spojeným s řetězcem dodavatelů. To zahrnuje hledání alternativních dodavatelů pro klíčové komponenty a služby.

3.3.7 Zvýšené nároky na komunikaci

Spolupráce a sdílení informací mezi operátory, dodavateli a vládními orgány může pomoci identifikovat a řešit bezpečnostní hrozby a zranitelnosti v rámci dodavatelského řetězce.

Zabezpečení řetězce dodavatelů v 5G ekosystému je komplexní a vyžaduje proaktivní a koordinovaný přístup. Účinné strategie zahrnují kombinaci technických, organizačních a politických opatření, která zajistí integritu a důvěru ve všechny aspekty 5G infrastruktury a služeb.

[5] Přezkum a certifikace dodavatelů je proces, kterým organizace systematicky hodnotí a ověřují schopnosti a bezpečnostní standardy svých dodavatelů před jejich zapojením do dodavatelského řetězce. Tento proces obvykle zahrnuje formální audity, kontroly a certifikační postupy, které jsou prováděny na základě předem definovaných kritérií a standardů.

.

[6] Kontraktualní opatření zahrnují ustanovení a podmínky v smlouvách mezi organizací a jejími dodavateli, které stanovují bezpečnostní požadavky, standardy a očekávání.

[7] Auditování je proces systematického přezkumu a hodnocení bezpečnostních postupů a opatření dodavatelů, aby se zajistilo, že jsou v souladu s kontraktualními opatřeními.

3.4 Síťové škálování a automatizace s dopady do rozhodování systému

Síťové škálování a automatizace jsou klíčové pro efektivní správu a optimalizaci rozsáhlých a složitých 5G sítí.

3.4.1 Závislost na automatizaci

5G sítě jsou navrženy tak, aby byly vysoce dynamické a flexibilní, což umožňuje operátorům rychle škálovat kapacitu a služby podle aktuální poptávky. Toto škálování je výrazně závislé na automatizaci, která umožňuje sítím přizpůsobovat se změnám v reálném čase.

3.4.2 Hůře rozeznatelná manipulace s daty

Pro automatizaci a optimalizaci sítí se často využívá umělá inteligence (AI) a strojové učení (ML). Tyto technologie pomáhají v predikci zatížení sítě, detekci a reakci na bezpečnostní hrozby, a optimalizaci síťového provozu. Nicméně, závislost na AI a ML přináší i potenciální rizika, jako jsou manipulace s daty, která by mohla ovlivnit rozhodování systému.

3.4.3 Vyšší nároky na vysledování chyb v automatizačních procesech

Automatizace hraje klíčovou roli i v konfiguraci a správě sítě, což zahrnuje nasazování síťových funkcí, zabezpečení a aktualizace softwaru. Zatímco automatizace může výrazně zvýšit efektivitu a snížit lidské chyby, také zvyšuje zranitelnost v případě, že by byly automatizační procesy kompromitovány.

3.4.4 S AI/ML možná manipulace síťových operací a šíření malwaru

Je nutné zajistit, aby algoritmy AI a ML nebyly zneužitelné útočníky pro manipulaci síťových operací nebo pro šíření malwaru. To vyžaduje robustní zabezpečení datových sad, které se pro učení algoritmů používají, a ochranu před útoky, které by mohly ovlivnit jejich chování.

3.4.5 Vyšší nároky na kontrolu automatizované reakce při incidentech

Systémy pro automatizovanou reakci na bezpečnostní incidenty musí být pečlivě navrženy tak, aby rychle a efektivně reagovaly na potenciální hrozby, aniž by přitom narušily provoz sítě nebo způsobily falešné poplachy.

3.4.6 Vyšší nároky na zabezpečení automatizace

Zabezpečení a integrita nástrojů používaných pro automatizaci sítě jsou zásadní. To zahrnuje zajištění, že tyto nástroje nejsou zranitelné vůči kybernetickým útokům a že jejich provoz je chráněn před neoprávněným přístupem.

3.5 Složitost mezinárodních standardů a regulací

Standardy a regulace hrají zásadní roli ve vytváření společného základu pro vývoj, implementaci a bezpečnostní praxi v rámci 5G technologií a zajišťují, že sítě různých operátorů a v různých zemích mohou spolupracovat bezpečně a efektivně.

3.5.1 Rozdíly v regulacích a standardizaci

Rozdíly v národních regulacích a přístupech k standardizaci mohou komplikovat globální nasazení 5G technologií. Zatímco některé země mohou přijímat standardy rychle, jiné mohou mít zpoždění nebo přijmout odlišné regulace, což může vést k fragmentaci a problémům s interoperabilitou.

3.5.2 Bezpečnostní implikace

Jednotné mezinárodní standardy a regulace jsou nezbytné pro zajištění vysoké úrovně bezpečnosti v 5G sítích. To zahrnuje bezpečnostní protokoly pro šifrování, autentizaci, ochranu soukromí a integritu dat. Nedostatek koordinace a jednotnosti ve standardizaci může otevřít dveře potenciálním bezpečnostním slabostem.

3.5.3 Tlak na globální spolupráci

Zesílení globální spolupráce mezi zeměmi, regulátory, a průmyslovými subjekty je klíčové pro vytváření a udržení jednotných mezinárodních standardů. To zahrnuje sdílení osvědčených postupů, společný výzkum a vývoj, a koordinaci politik.

3.5.4 Vyšší nároky na sledování aktualizace standardů

Vzhledem k rychlému vývoji technologií je důležité, aby standardizační organizace pravidelně aktualizovaly a přizpůsobovaly standardy, aby reflektovaly nejnovější poznatky a technologické inovace.

3.5.5 Vyšší nároky na vzdělávání a osvětu

Informování a vzdělávání stakeholderů o významech a dopadech mezinárodních standardů a regulací může podporovat jejich rychlejší a efektivnější implementaci.

3.6 Zvýšené množství osobních a citlivých dat v síti

Ochrana soukromí je zásadním aspektem bezpečnosti 5G sítí. S příchodem 5G technologie a její schopností podporovat exponenciální růst připojených zařízení a aplikací, se výrazně zvyšuje množství osobních a citlivých dat generovaných a přenášených přes síť.

Ochrana soukromí v 5G sítích je mnohostranná výzva, která vyžaduje koordinované úsilí mezi technologickými inovátory, regulátory, a uživateli. Přechod na 5G klade důraz na potřebu robustní ochrany soukromí a bezpečnostních opatření, aby se zajistilo, že technologie slouží veřejnému zájmu a chrání individuální práva.

3.6.1 Masivní zapojení IoT zařízení a více ohrožené soukromí

5G sítě umožňují masivní připojení IoT (internet věcí) zařízení, od chytrých domácích spotřebičů po vozidla a průmyslové senzory. Tyto zařízení shromažďují a sdílejí obrovské množství dat, často včetně osobních informací, což vyvolává obavy týkající se sledování, identifikace a zneužití dat.

3.6.2 Další možnosti úniku dat

S rostoucím počtem připojených zařízení a komplexností sítí se zvyšuje riziko úniků dat. To může zahrnovat jak neúmyslné úniky v důsledku chyb v konfiguraci nebo zranitelností, tak úmyslné útoky s cílem krást osobní data.

3.6.3 Potřeba silnějšího šifrování a anonymizace

Aby bylo možné zajistit ochranu soukromí v 5G sítích, je nezbytné využívat pokročilé metody šifrování a anonymizace dat. Tyto techniky pomáhají zajistit, že i v případě získání dat útočníkem, zůstanou informace chráněny a nečitelné.

3.6.4 Potřeba regulace shromažďování dat a spravedlivého použití

Podniky a organizace využívající 5G sítě by měly dodržovat zásady minimálního shromažďování dat a spravedlivého použití. To znamená shromažďovat pouze ta data, která jsou nezbytně nutná pro poskytnutí služby, a používat data pouze v souladu s účelem, pro který byla shromážděna.

3.6.5 Zvýšené nároky na hodnocení ochrany dat a soukromí

Organizace by měly pravidelně provádět hodnocení rizik souvisejících s ochranou dat a soukromí a ujistit se, že jejich postupy a technologie jsou v souladu s platnými regulacemi, jako je GDPR v Evropské unii.

3.6.6 Budoucí tlak na zapojení technologií pro ochranu dat a soukromí

Vývoj a implementace technologií zaměřených na soukromí, jako jsou techniky homomorfního šifrování nebo diferenciálního soukromí, mohou poskytnout vysokou úroveň ochrany dat při zachování funkcionality aplikací.

3.6.7 Vyšší nároky na vzdělávání uživatelů

Vzdělávání uživatelů a zvyšování povědomí o rizicích a nejlepších postupech pro ochranu osobních dat je klíčové pro posílení celkové bezpečnosti a ochrany soukromí v ekosystému 5G.

4 Zhodnocení potenciálních i možných typů kybernetických útoků Open RAN

Open RAN přináší inovativní přístup k výstavbě telekomunikačních sítí tím, že podporuje větší interoperabilitu a flexibilitu mezi komponentami různých výrobců. To však také vyžaduje inovativní přístup na zhodnocení potenciálních i možných typů kybernetických útoků.

Tato část identifikuje útoky na hlavní části Open RAN, a to na data, zdroje dat a celkovou Open RAN architekturu a uvádí k nim vždy možná protiopatření.

4.1 Útoky na důvěrnost dat

Důvěrnost dat je klíčovou složkou kybernetické bezpečnosti, zahrnující ochranu informací před neoprávněným přístupem a zveřejněním. S útoky na důvěrnost dat v 5G sítích a sítích Open RAN se vyžaduje hlubší pohled na to, jak mohou být data ohrožena a jaké strategie mohou být použity k jejich ochraně. V kontextu 5G a Open RAN sítí existují **specifické kybernetické útoky:**

4.1.1 Odposlech (Eavesdropping)

Odposlech se týká neautorizovaného naslouchání komunikace mezi zařízeními nebo v rámci sítě. V prostředí 5G/Open RAN mohou být odposlechnuty hovory, sledovány textové zprávy, data z aplikací, a dokonce i komunikace mezi síťovými uzly.

Protiopatření:

- Šifrování: Implementace silného šifrování na všech úrovních komunikace (od koncových bodů až po síťové segmenty) může zabránit útočníkům v dešifrování zachycených dat.
- Bezpečné tunelování: Využití VPN (Virtuální Privátní Sítě) a protokolů jako je IPSec pro zabezpečení dat přenášených přes veřejné sítě.

4.1.2 Man-in-the-Middle (MitM) útoky

MitM útoky umožňují útočníkovi vložit se do komunikace mezi dvěma stranami, čímž může odposlouchávat, upravovat nebo vložit zprávy bez vědomí stran. V 5G/Open RAN může být toto zvláště problematické vzhledem k dynamické povaze síťového provozu a komunikace.

Protiopatření:

- Vzájemné ověřování: Zajištění, že obě komunikující strany se mohou navzájem autentizovat před výměnou jakýchkoliv dat, což pomáhá zabránit útočníkům v úspěšném provedení MitM útoků.
- Síťová segmentace: Omezení schopnosti útočníka pohybovat se v rámci sítě a provádět MitM útoky pomocí pečlivého návrhu síťové topologie a izolace kritických systémů.

4.1.3 Útoky na důvěryhodnost z dodavatelského řetězce

Vzhledem k tomu, že Open RAN podporuje větší otevřenost a interoperabilitu mezi různými výrobci a komponenty, může to znamenat zvýšené riziko útoků na důvěrnost dat.

Protiopatření:

- Zajištění důvěrnosti dat v 5G a Open RAN sítích vyžaduje komplexní přístup, jehož součástí je silné šifrování, pečlivé ověřování, síťovou segmentaci a implementaci principů nulové důvěry. Tyto kroky pomáhají chránit citlivé informace a zajistit, že sítě zůstanou odolné proti pokusům o neoprávněný přístup nebo útoky.

4.2 Útoky na integritu dat

Útoky na integritu dat v 5G sítích a sítích Open RAN představují útoky směřující k poškození, manipulaci nebo ztrátě důvěryhodnosti informací. Zajištění integrity dat je zásadní pro funkčnost a bezpečnost celého telekomunikačního ekosystému.

4.2.1 Injection útoky

Injection útoky se odehrávají, když útočník vkládá nebo "injektuje" škodlivá data do systému s cílem provést neoprávněné operace. V kontextu 5G/Open RAN to může zahrnovat vkládání škodlivého kódu do síťové komunikace nebo manipulaci s datovými toky, což vede k narušení služeb nebo k šíření malwaru.

Protiopatření:

- Validace vstupu: Pečlivá kontrola a omezení všech přijímaných dat na povolené typy a formáty může zabránit úspěšnému provedení injection útoků.

- Bezpečnostní protokoly a šifrování: Použití bezpečnostních protokolů a šifrování pro komunikaci mezi uzly a zařízeními chrání integritu přenášených dat.

4.2.2 Spoofing identity

Spoofing útoky se chovají jako falešné představování se za jinou entitu nebo zařízení v síti s cílem získat neoprávněný přístup k datům nebo službám. V prostředí 5G a Open RAN mohou útočníci využít spoofing k získání citlivých informací nebo k narušení síťové komunikace.

Protiopatření:

- Ověřování a autorizace: Zajištění, že každá entita v síti může být jednoznačně identifikována a ověřena před zahájením komunikace, pomáhá zabránit spoofing útokům.

- Síťové politiky a sledování: Vytváření a uplatňování striktních síťových politik, spolu s neustálým monitorováním síťového provozu, umožňuje rychlou detekci a reakci na pokusy o spoofing.

4.2.3 Útoky na integritu z dodavatelského řetězce

Vzhledem k tomu, že Open RAN podporuje větší flexibilitu a integraci různých technologických komponent od různých dodavatelů, mohou vzniknout specifické výzvy pro ochranu integrity dat.

Protiopatření:

- Bezpečnostní certifikace a standardy: Zajištění, že všechny komponenty a zařízení používané v síti Open RAN splňují pevné bezpečnostní standardy a prošly bezpečnostní certifikací.

- Rozšířená detekce a reakce (EDR): Implementace EDR řešení na klíčových uzlech sítě může pomoci v rychlé detekci a reakci na pokusy o manipulaci s daty nebo jiné útoky na integritu.

4.3 Útoky na dostupnost dat

Tyto útoky jsou navrženy tak, aby narušily nebo zcela znemožnily přístup k legitimním službám a datům, což může mít vážné důsledky pro uživatele a poskytovatele služeb. V prostředí 5G a Open RAN, kde se očekává vysoká míra konektivity a spolehlivosti, jsou útoky na dostupnost obzvláště kritické.

4.3.1 DDoS (Distributed Denial of Service) útoky

DDoS útoky jsou jednou z nejznámějších forem útoku na dostupnost, při kterých útočníci přesycují síťové zdroje (např. servery, síťovou infrastrukturu) masivním množstvím nelegitimního provozu, čímž znemožňují přístup pro legitimní uživatele.

Protiopatření:

- Rozložení zátěže a redundantnost: Vytvoření více kopií kritických komponent a distribuce provozu může pomoci absorbovat nárazy DDoS útoků.
- DDoS ochranné služby: Využití specializovaných DDoS ochranných služeb, které dokážou detekovat a mitigovat útoky dříve, než způsobí škody.
- Omezení rychlosti a filtrování provozu: Implementace pravidel pro omezení rychlosti a filtrování podezřelého provozu na síťových hranicích může pomoci minimalizovat dopad DDoS útoků.

4.3.2 Útoky na energetické zdroje

Záměrné vyčerpání nebo rušení energetických zdrojů zařízení v síti, jako jsou vysílače nebo servery, může vést k výpadkům služeb. Tyto útoky mohou být provedeny fyzicky nebo softwarově (např. způsobením přetížení zařízení, které vyžaduje nadměrnou spotřebu energie).

Protiopatření:

- Monitoring a správa energetických zdrojů: Neustálé monitorování spotřeby energie a předvídání potřeb založených na analýze dat může pomoci včas identifikovat neobvyklé vzorce spotřeby.
- Energetická efektivita a redundance: Zlepšení energetické efektivnosti zařízení a zajištění redundance zdrojů mohou pomoci zvládnout pokusy o vyčerpání energie.

4.3.3 Útoky s využitím složitosti architektury Open RAN

Open RAN architektura podporuje rozmanitost dodavatelů a komponent, což může ztížit jednotné řešení pro ochranu před útoky na dostupnost. Větší složitost a potřeba integrace rozličných technologií může také znamenat více potenciálních slabých míst.

Protiopatření:

- Pokročilé monitorování a analýza: Využití pokročilých nástrojů pro monitorování síťového provozu a chování zařízení může pomoci rychle identifikovat a reagovat na útoky.
- Spolupráce a sdílení informací: Spolupráce mezi operátory, dodavateli a bezpečnostními organizacemi ve sdílení informací o hrozbách a nejlepších praktikách může posílit obranu proti útokům na dostupnost.

4.4 Některé další typy útoků na Open RAN

Open RAN přináší také specifické bezpečnostní výzvy, které vyžadují komplexní a vícevrstvé bezpečnostní strategie.

4.4.1 Side-channel útoky

Tyto útoky využívají informace získané z vedlejších kanálů, jako je výkonová spotřeba, elektromagnetické vyzařování nebo dokonce akustické signály, k odhalení citlivých informací o síťovém zařízení nebo provozovaných operacích. Open RAN může být zvláště zranitelný, pokud nejsou hardwarové komponenty pečlivě zabezpečeny.

Protiopatření:

- Fyzická bezpečnost: Ochrana fyzických zařízení před neoprávněným přístupem.
- Izolace a šifrování: Použití izolace úloh a šifrování dat, aby bylo obtížnější získat užitečné informace prostřednictvím side-channel analýzy.

4.4.2 Útoky na rozhraní mezi jednotlivými RAN komponentami

Open RAN s různými výrobci a komponenty může znamenat zvýšené riziko útoků zaměřených na rozhraní a API mezi těmito komponentami.

Protiopatření:

- Pevné API bezpečnostní protokoly: Implementace robustních bezpečnostních kontrol a autentizačních mechanismů pro veškerou komunikaci mezi komponentami.
- Pravidelné bezpečnostní auditování: Kontinuální kontrola a aktualizace bezpečnostních opatření na rozhraních.

4.4.3 Útoky na SDN a NFV

Jelikož Open RAN často využívá SDN a NFV pro zvýšení flexibility a efektivity sítě, stávají se tyto technologie cílem útoků, tzn. útočníci manipulují s virtuálními síťovými funkcemi nebo útočí na SDN řadiče.

Protiopatření:

- Zabezpečení virtualizované vrstvy: Zajištění, že všechny virtuální síťové funkce jsou dobře izolovány a chráněny.
- Silná autentizace a šifrování: Ochrana komunikace mezi SDN komponentami a NFV instancemi.

4.4.4 Insider útoky

Insiderské útoky představují hrozbu ze strany interních osob s legitimním přístupem k síťové infrastruktuře, které mohou zneužít svá oprávnění k provádění škodlivých akcí. Jedná se o tyto příklady dílčích podob útoků:

- Krádež citlivých informací - Zaměstnanec, který má přístup k důvěrným informacím, jako jsou přihlašovací údaje uživatelů, finanční data nebo technické specifikace, může tyto informace zkopírovat a prodat třetím stranám nebo je použít k vlastnímu obohacení.
- Manipulace s konfigurací sítě - Administrátor s přístupem ke konfiguraci sítě může úmyslně změnit nastavení síťových prvků tak, aby způsobil výpadky služeb, snížil výkon nebo zpřístupnil síť útočníkům zvenčí.
- Instalace malwaru - Útočník zevnitř organizace může nainstalovat malware do systémů nebo zařízení v síti, což může vést k získání přístupu k citlivým datům, sledování síťového provozu nebo dokonce úplnému ovládnutí sítě.
- Sabotáž - Nespokojený zaměstnanec může záměrně poškodit hardware, odstranit kritické soubory nebo způsobit jiné formy fyzické nebo logické sabotáže, což může způsobit vážné výpadky služeb nebo ztrátu dat.
- Neoprávněné změny v softwaru - Vývojář nebo technik s přístupem k vývojovým nebo provozním systémům může provést neoprávněné změny v softwarovém kódu nebo nastaveních, což může vést k bezpečnostním zranitelnostem nebo jiným problémům.
- Vytváření zadních vrátek (backdoors) - Útočník zevnitř organizace může v softwaru nebo síťových prvcích vytvořit zadní vrátka, která umožní neoprávněný přístup k systému pro sebe nebo pro další útočníky.
- Zneužití přístupových práv - Zaměstnanec s vysokými oprávněními může zneužít svá práva k přístupu k systémům nebo datům, ke kterým by za normálních okolností neměl mít přístup, a použít tyto informace k osobnímu prospěchu nebo poškodit organizaci.

Protiopatření:

- Pravidelné bezpečnostní audity: Kontrola přístupových práv a sledování aktivit zaměstnanců.
- Princip nejmenších privilegií: Omezení přístupu pouze na nezbytně nutné informace a systémy.
- Bezpečnostní školení: Pravidelné školení zaměstnanců o bezpečnostních postupech a rozpoznávání potenciálních hrozeb.
- Sledování a logování: Implementace systémů pro sledování a logování všech přístupů a aktivit v síti.
- Reakce na incidenty: Vypracování a testování plánů pro reakci na bezpečnostní incidenty.

5 Analýza možností a rizik související se správou identit a přístupů v 5G sítích

S přechodem na 5G technologie dochází k významným změnám v architektuře a fungování sítí, což přináší nové výzvy i možnosti pro Identity and Access Management systémy (IAM). Analýza možností a rizik spojených se správou identit a přístupů se dotýká několika klíčových oblastí, včetně bezpečnosti, soukromí, interoperability, a škálovatelnosti.

Nejprve si uvedeme možnosti a přínosy správy identit a přístupů, které následně vyměníme *za rizika se správou souvisejícími.*

5.1 Vylepšená bezpečnost

Vylepšená bezpečnost v rámci 5G sítí v optice technologii a principů IAM, které sítě využívají k ochraně dat a komunikace, umožňuje uživatelům a zařízením využívat síť s důvěrou v ochranu jejich informací a soukromí.

5.1.1 Pokročilé šifrovací protokoly

5G sítě využívají nejnovější a nejbezpečnější šifrovací standardy, jako je AES (Advanced Encryption Standard) pro šifrování dat přenášených po síti. Tyto protokoly zajišťují, že data jsou chráněna před neoprávněným přístupem během přenosu.

5.1.2 Robustní techniky ověřování

5G sítě zavádějí pokročilé metody ověřování, které přesahují tradiční hesla a PIN kódy. To zahrnuje využití biometrických údajů, jako je otisk prstu, rozpoznání obličeje nebo hlasové ověření, stejně jako dvoufaktorovou autentizaci (2FA) nebo vícefaktorovou autentizaci (MFA) pro zvýšení bezpečnosti při přístupu k síťovým službám.

5.1.3 Bezpečnostní protokoly pro integritu a autentizaci

5G implementuje specifické bezpečnostní protokoly navržené k ochraně integrity a autentizace dat. Tyto protokoly pomáhají zajistit, že data nebyla pozměněna během přenosu a že komunikace probíhá mezi ověřenými stranami.

5.1.4 Izolace a segmentace sítě

5G technologie umožňuje pokročilou segmentaci sítě, což znamená, že různé části sítě mohou být izolovány pro specifické účely nebo aplikace. To umožňuje lepší kontrolu přístupu a zvyšuje bezpečnost tím, že minimalizuje riziko šíření potenciálních hrozeb napříč celou sítí.

5.1.5 Detekce a reakce na hrozby v reálném čase

Díky vysoké propustnosti a nízké latenci 5G sítí mohou bezpečnostní systémy efektivně monitorovat síťový provoz a rychle reagovat na anomálie nebo potenciální bezpečnostní hrozby. To zahrnuje automatizované systémy pro detekci útoků a zranitelností, které mohou okamžitě upozornit na problémy a automaticky implementovat protiopatření.

Zlepšená bezpečnost v 5G sítích tedy není jen o silnějších šifrovacích algoritmech a robustnějších metodách ověřování; zahrnuje komplexní soubor technologií a protokolů navržených k ochraně sítě a jejích uživatelů před širokou škálou kybernetických hrozeb. Tyto bezpečnostní vlastnosti jsou základem pro důvěryhodné využívání 5G technologií v rozmanitých aplikacích, od chytrých domovů a IoT zařízení po kritickou infrastrukturu a podnikové sítě.

5.2 Vysoká škálovatelnost

Vysoká škálovatelnost je jedním z klíčových atributů, které 5G sítě přinášejí do světa telekomunikací, a to má značný dopad na správu identit a přístupů (IAM). Tato vlastnost umožňuje síti podporovat obrovský počet připojených zařízení.

5.2.1 Podpora masivního IoT a mobilních zařízení

Jedním z hlavních cílů 5G technologie je umožnit masivní IoT, od smartphonů a tabletů po rozsáhlé spektrum IoT zařízení, jako jsou senzory, chytrá domácí zařízení, autonomní vozidla a průmyslové stroje, což znamená podporu pro desítky tisíc zařízení připojených k síti na km². To vyžaduje škálovatelné IAM řešení, které může efektivně spravovat identitu a přístupová práva pro obrovský počet zařízení, přičemž zajistí bezpečnost a soukromí.

5.2.2 Dynamická správa

Vysoká škálovatelnost 5G umožňuje dynamickou správu síťových zdrojů a služeb, což znamená, že IAM systémy mohou být adaptivní a flexibilní. To zahrnuje možnost rychle přidávat, aktualizovat nebo odstraňovat identifikátory zařízení a uživatelů v reálném čase, což je zásadní pro zajištění bezpečnosti.

5.2.3 Efektivní segmentace a politiky přístupu

Díky pokročilým schopnostem sítě je možné efektivně segmentovat síť a aplikovat detailní politiky přístupu na základě identit uživatelů nebo zařízení. Tato segmentace umožňuje vytváření virtuálních privátních sítí (VPNs) pro různé typy zařízení nebo skupiny uživatelů, což zvyšuje bezpečnost tím, že izoluje citlivé údaje a operace od ostatních částí sítě.

5.2.4 Automatizace a AI

S rostoucím počtem zařízení se stává zásadní využití automatizace a umělé inteligence (AI) pro správu IAM. 5G sítě s vysokou škálovatelností umožňují nasazení AI a strojového učení pro automatizaci procesů identifikace, autentizace a autorizace. To nejen zefektivňuje správu, ale také pomáhá v předvídání a reagování na bezpečnostní hrozby v reálném čase.

5.2.5 Rozšířená interoperabilita

Vysoká škálovatelnost 5G sítí také podporuje lepší interoperabilitu mezi různými sítěmi a službami, což je klíčové pro správu identit a přístupů napříč různými platformami a poskytovateli. To zahrnuje schopnost spravovat identitu a přístupy pro uživatele a zařízení, které interagují s mnoha různými síťovými službami a aplikacemi, zjednodušuje správu a zlepšuje uživatelskou zkušenost.

Vysoká škálovatelnost 5G sítí tedy otevírá nové horizonty pro IAM řešení, umožňuje efektivní správu rozsáhlého množství zařízení a uživatelů, a zároveň zvyšuje bezpečnost, efektivitu a flexibilitu v dynamickém a propojeném digitálním světě.

5.3 Snížená latence

Snížená latence, kterou nabízí 5G sítě, má značný dopad na autentizační a autorizační procesy. Latence, neboli doba zpoždění, je doba, která uplyne mezi odesláním požadavku z jednoho bodu v síti a přijetím odpovědi. 5G sítě jsou navrženy tak, aby toto zpoždění minimalizovaly, často na několik milisekund nebo méně, což má významný vliv na řadu aplikací a služeb a podporu v rámci správy identity a přístupů.

5.3.1 Rychlejší autentizace a autorizace

Snížená latence znamená, že procesy autentizace a autorizace mohou probíhat mnohem rychleji. To je zvláště důležité v situacích, kde rychlost přístupu je kritická, například při přístupu k zabezpečeným službám, finančním transakcím nebo při použití služeb vyžadujících okamžitou reakci.

5.3.2 Zlepšená uživatelská zkušenost

Rychlejší reakce systému na požadavky uživatelů zlepšuje celkovou uživatelskou zkušenost. Uživatelé očekávají rychlý a plynulý přístup k digitálním službám a aplikacím, a snížená latence 5G to umožňuje. To je obzvláště významné pro aplikace jako jsou streamování videa, cloudové hry, nebo virtuální a rozšířená realita, kde rychlost a okamžitá odezva jsou nezbytné pro kvalitní zážitek.

5.3.3 Vylepšená bezpečnost v reálném čase

Snižování latence umožňuje implementaci bezpečnostních opatření v reálném čase, jako je okamžitá detekce a reakce na bezpečnostní hrozby v podobě rychlého identifikování a blokování neautorizovaných pokusů o přístup.

5.3.4 Podpora pro kritické aplikace

Mnoho kritických aplikací a služeb, jako jsou autonomní vozidla, dálkově řízené operace, nebo systémy nouzové reakce, vyžaduje velmi nízkou latenci pro bezpečné a efektivní fungování. Snížená latence 5G sítí umožňuje spolehlivou komunikaci v reálném čase, která je nezbytná pro tyto aplikace.

5.3.5 Integrace s Edge Computing

Snížená latence 5G je klíčová pro efektivní využití edge computing, kde se zpracování dat a výpočetní úlohy přesouvají blíže ke koncovým uživatelům. Toto uspořádání umožňuje rychlejší zpracování a reakci, což je zásadní pro aplikace vyžadující okamžité zpracování dat, jako je analýza videa v reálném čase nebo interaktivní aplikace.

5.4 Edge Computing

Edge computing odkazuje na architekturu distribuovaného výpočtu, ve které se zpracování dat a výpočetní úlohy provádějí na okraji sítě, což je co nejblíže zdroji dat nebo koncovému uživateli. Toto uspořádání nabízí řadu výhod, které se pozitivně promítají do efektivity, rychlosti a bezpečnosti IAM systémů v 5G prostředí.

5.4.1 Lokalizace datového zpracování

Přesunem zpracování dat blíže ke koncovým uživatelům nebo zařízením edge computing snižuje latenci a zvyšuje rychlost reakce systémů. V kontextu IAM to znamená rychlejší autentizaci a autorizaci uživatelů a zařízení, což je zásadní pro aplikace vyžadující okamžité zpracování nebo pro kontrolu přístupu v reálném čase.

5.4.2 Zvýšená bezpečnost a soukromí

Edge computing umožňuje, že se velká část dat zpracovává lokálně, aniž by musela být přenášena přes centrální servery nebo do cloudu. To minimalizuje riziko úniku dat během přenosu a umožňuje lepší kontrolu nad daty a jejich ochranu. V rámci IAM to znamená, že citlivé informace, jako jsou biometrické údaje pro autentizaci, mohou být zpracovány lokálně, což snižuje riziko kompromitace.

5.4.3 Škálovatelnost a flexibilita

Díky schopnosti zpracovávat data na mnoha různých místech umožňuje edge computing organizacím škálovat své operace. Také umožňuje IAM systémům rychle se adaptovat na rostoucí počet uživatelů a zařízení, zatímco zajišťuje, že výkon a bezpečnostní požadavky jsou stále splněny.

5.4.4 Podpora pro IoT a mobilní zařízení

Edge computing je zásadní pro efektivní správu a bezpečnost IoT zařízení, která jsou často rozptýlena a produkují velké množství dat. Integrace edge computing s 5G sítěmi umožňuje rychlé zpracování a analýzu dat přímo na místě, což usnadňuje autentizaci a autorizaci zařízení, a zároveň minimalizuje zpoždění a zatížení sítě.

5.4.5 Odpověď na hrozby v reálném čase

Kombinace edge computing s nízkou latencí 5G sítí umožňuje bezprecedentní schopnost detekovat a reagovat na bezpečnostní hrozby v reálném čase. Systémy mohou okamžitě identifikovat podezřelé aktivity a přijmout opatření k jejich odvrácení, což zlepšuje celkovou ochranu systému a dat.

Výše uvedenými možnostmi spojenými se správou identit a přístupů v 5G sítích se otevírají nové cesty pro vývoj bezpečnějších, rychlejších a inteligentnějších digitálních služeb a infrastruktury, které mohou lépe reagovat na potřeby moderní digitálně propojené společnosti.

5.5 Složitost sítě

Složitost sítě je **významným rizikem** spojeným s 5G technologiemi, které může mít dalekosáhlé důsledky pro bezpečnost, správu a výkon sítí. Toto riziko je obzvláště relevantní v kontextu správy identit a přístupů (IAM).

5.5.1 Zvýšený počet vstupních bodů pro útočníky

5G sítě podporují masivní množství připojených zařízení, včetně IoT zařízení, což znamená zvýšení potenciálních vstupních bodů pro kybernetické útočníky. S každým připojeným zařízením přichází potenciální slabina, kterou lze zneužít. Správa identit a přístupů musí být proto extrémně robustní a schopná monitorovat a spravovat bezpečnostní rizika pro obrovské množství zařízení.

5.5.2 Složitost konfigurace a správy

S přechodem na 5G se zvyšuje složitost sítě nejen kvůli většímu počtu zařízení, ale také kvůli novým technologiím a architekturám, jako jsou síťové funkce virtualizace (NFV) a software definované sítě (SDN). Tyto technologie v tomto smyslu mohou komplikovat konfiguraci, správu a monitoring, což může vést k lidským chybám nebo přehlédnutí bezpečnostních slabostí.

5.5.3 Nezávislé komponenty a zajišťování interoperability a kompatibility

Integrace 5G s existujícími systémy a technologiemi vyžaduje zajištění interoperability a kompatibility mezi různými síťovými komponentami a službami. Toto úsilí o zajištění hladkého propojení může odhalit nové bezpečnostní slabiny, protože systémy a protokoly, které byly původně navrženy nezávisle, musí nyní spolupracovat.

5.5.4 Složitost zabezpečení end-to-end

5G sítě jsou navrženy s myšlenkou na poskytování end-to-end zabezpečení, což zahrnuje ochranu dat přenášených mezi zařízeními a sítěmi. Složitost takového požadavku vyžaduje komplexní bezpečnostní opatření na různých úrovních sítě, od fyzické vrstvy až po aplikace. Efektivní implementace a správa těchto bezpečnostních opatření je náročná a vyžaduje důkladné plánování a koordinaci.

5.5.5 Náročná správa v oblasti aktualizací a oprav zabezpečení

Vzhledem k rychlému vývoji 5G technologií a aplikací se objevují nové bezpečnostní hrozby a zranitelnosti, které vyžadují průběžné aktualizace a opravy. Správa těchto aktualizací a udržení systémů aktualizovaných a bezpečných v tak složité a dynamicky se měnící síťové infrastruktuře je výzvou.

Celkově složitost 5G sítí přináší významné výzvy pro IAM systémy, což vyžaduje pokročilé řešení a strategie pro zajištění bezpečnosti, správy a výkonu v těchto komplexních prostředích.

5.6 Rozšíření vstupních bodů a vektorů útoku

Rozšíření povrchu útoků **je významným rizikem** spojeným s implementací a provozem 5G sítí. Útok se odkazuje na všechny různé body v systému, které útočník může potenciálně využít k získání neoprávněného přístupu nebo k provádění škodlivých činností. V kontextu 5G sítí a IAM systémů toto rozšíření je svázáno s několika klíčovými pohledy.

5.6.1 Zvýšený počet připojených zařízení

5G sítě umožňují exponenciální nárůst připojených zařízení, zejména v oblasti IoT. Každé zařízení, od chytrých domácích zařízení po průmyslové senzory, může představovat potenciální bod útoku. Správa identit a přístupů pro takový rozsáhlý a diverzifikovaný soubor zařízení je složitá a vyžaduje robustní bezpečnostní řešení.

5.6.2 Složitější síťová infrastruktura

5G technologie zavádí nové architektonické komponenty, jako jsou síťové funkce virtualizace (NFV) a software definované sítě (SDN), což přidává další vrstvy do síťové infrastruktury. Tyto komponenty mohou obsahovat vlastní zranitelnosti nebo mohou být nesprávně nakonfigurovány, čímž se rozšiřuje potenciál útoku

5.6.3 Různorodost a heterogenita sítě

5G sítě integrují různé typy sítí a technologií, včetně LTE, Wi-Fi a nových rádiových přístupových sítí. Tato heterogenita ztěžuje jednotnou ochranu a správu bezpečnostních politik, zvyšuje složitost monitorování a odpovídání na hrozby.

5.6.4 Zvýšená mobilita uživatelů a zařízení

5G sítě podporují vyšší mobilitu uživatelů a zařízení s rychlejším připojením a nižší latencí. Toto umožňuje provozovat nové typy aplikací a služeb, ale také komplikuje sledování a zabezpečení pohyblivých zařízení a datových toků mezi různými sítěmi a geografickými oblastmi.

5.6.5 Rozšířené hrozby a sofistikovanější útoky

S rostoucími možnostmi 5G sítí se zvyšuje i sofistikovanost potenciálních kybernetických útoků. Útočníci mohou využívat pokročilé metody, včetně AI a strojového učení, k identifikaci a využívání slabých míst v síti. 5G sítě se tak setkávají se širokým spektrem útoků, od distribuovaných útoků odmítnutí služby (DDoS) po pokročilé trvalé hrozby (APT).

5.7 Problémy s interoperabilitou

Problémy s interoperabilitou představují **významné riziko**, které může mít dopad na systémy autentizace a autorizace. Interoperabilita se týká schopnosti různých systémů, zařízení a aplikací vzájemně komunikovat a efektivně spolupracovat, což je zásadní pro plynulé a bezpečné fungování rozsáhlých a heterogenních 5G sítí.

5.7.1 Kompatibilita mezi různými technologiemi a standardy

5G sítě podporují technologie včetně starších mobilních sítí (např. 4G LTE), Wi-Fi, nových rádiových přístupových technologií a technologií pro IoT. Zajištění kompatibility a interoperability mezi těmito rozdílnými systémy a standardy je složité a může vést k problémům v autentizaci a autorizaci, pokud nejsou správně nastaveny.

5.7.2 Složitost správy identit a přístupů

Vzhledem k rozmanitosti zařízení a služeb v 5G sítích je správa identit a přístupů (IAM) výzvou. Problémy s interoperabilitou mohou komplikovat správu uživatelských identit, oprávnění a politik přístupu, zvláště když je třeba integrovat systémy od různých výrobců nebo služby běžící na různých platformách.

5.7.3 Pokračující rozšiřování nebo integrace s existujícími sítěmi

5G sítě jsou navrženy tak, aby fungovaly ve spolupráci s existujícími telekomunikačními infrastrukturami a sítěmi. To vyžaduje, aby systémy IAM byly schopné podporovat různé autentizační a autorizační mechanismy používané v těchto sítích, což může způsobit problémy s interoperabilitou a kompatibilitou.

5.7.4 Výzvy v oblasti standardizace a regulace

Jednotná standardizace a regulace jsou klíčové pro zajištění interoperability v 5G sítích. Potenciálně se lze setkat s nedostatky ve shodě nebo se zpožděním ve vývoji a implementaci standardů, které ovlivňují bezpečnost a funkčnost sítí.

5.7.5 Bezpečnostní rizika spojená s interoperabilitou

Mohou se vyskytnout nové bezpečnostní mezery, neboť integrace různých systémů a technologií často vyžaduje kompromisy v oblasti zabezpečení. Například, pokud dva systémy používají odlišné bezpečnostní protokoly, jejich integrace může vést k slabšímu zabezpečení.

Řešení těchto problémů vyžaduje úzkou spolupráci mezi výrobci zařízení, poskytovateli sítí, standardizačními organizacemi a regulačními orgány. Kromě toho je důležité investovat do vývoje flexibilních a modulárních systémů IAM, které mohou být snadno adaptovány na různé technologické platformy a standardy, čímž se minimalizuje dopad problémů s interoperabilitou na bezpečnost a výkon 5G sítí.

5.8 Narušení soukromí

Soukromí je **klíčovou obavou** v kontextu 5G sítí, která může být ovlivněna také způsobem, jakým jsou řízeny identita a přístupy. Zvyšuje se množství generovaných a zpracovávaných osobních dat. Narušení soukromí se odehrává v dalších níže uvedených oblastech.

5.8.1 Masivní sběr dat

5G sítě umožňují sběr, přenos a analýzu obrovského objemu dat z rozmanitých zařízení v reálném čase. Tento sběr dat zahrnuje nejen osobní a citlivé informace, ale také data o lokalitě a chování uživatelů. Pokud nejsou data správně chráněna, může to vést k vážným narušením soukromí.

5.8.2 Rizika související s bezpečností dat

Zvýšený počet zařízení a komplexnost sítě rozšiřují potenciální vstupní body útoku, což zvyšuje riziko úniku nebo zneužití dat. Nedostatečně zabezpečená zařízení nebo komunikační kanály mohou být zranitelné vůči kybernetickým útokům, což ohrožuje soukromí uživatelů.

5.8.3 Nedostatečné šifrování a ochrana dat

I přes pokročilé možnosti šifrování, které 5G nabízí, může být implementace šifrování nekonzistentní napříč různými zařízeními a službami. To může vést k situacím, kdy jsou data přenášena nebo uložena bez adekvátní ochrany, a zvyšuje se tak riziko jejich zneužití.

5.8.4 Problémy s kontrolou a správou dat

Uživatelé mohou mít omezenou kontrolu nad tím, jak jsou jejich data sbírána, zpracovávána a sdílena v rámci 5G sítí. To komplikuje správu soukromí a souhlasu, zejména v souvislosti s mezinárodními a mnohostrannými sítěmi a rozdíly v právních a regulačních požadavcích na ochranu dat.

5.8.5 Technicky složitá anonymizace a minimalizace dat

I při snaze o anonymizaci nebo pseudonymizaci dat mohou být v rámci 5G sítí shromažďována tak detailní a rozsáhlá sada dat, že anonymizace se stává technicky složitou nebo neúčinnou. To zvyšuje riziko identifikace jednotlivců i z velkých a zdánlivě anonymních datových sad.

5.9 Nedostatečné autentizační a autorizační mechanismy

Nedostatečná autentizace a autorizace v kontextu 5G sítí představují **významné riziko**, které může vést k různým bezpečnostním incidentům, včetně neoprávněného přístupu, úniku dat, nebo zneužití služeb. V rámci 5G sítí, které slibují vyšší rychlost, masivní konektivitu a nízkou latenci pro rozmanité aplikace od IoT po kritickou infrastrukturu, jsou robustní systémy autentizace a autorizace klíčové pro zajištění bezpečnosti a důvěryhodnosti nevyhnutelností.

5.9.1 Neoprávněný přístup k síťovým zdrojům a službám

Slabé nebo kompromitované mechanismy autentizace umožňují útočníkům získat přístup k citlivým zdrojům nebo službám, což může vést k úniku dat, zneužití služeb nebo sabotáži operací.

5.9.2 Útoky typu "man-in-the-middle" (MitM)

Nedostatečné autentizační protokoly zvyšují riziko útoků MitM, při kterých útočník odposlouchává nebo manipuluje s komunikací mezi dvěma stranami bez jejich vědomí. To může vést k odcizení citlivých informací, včetně osobních údajů a přihlašovacích údajů.

5.9.3 Spoofing identit

Slabé nebo neefektivní metody autentizace a autorizace mohou usnadnit útočníkům vydávání se za legitimní uživatele nebo zařízení a provádět škodlivé činnosti, jako je šíření malwaru, phishingové útoky nebo zneužití služeb.

5.9.4 Replay útoky

Bez adekvátního zabezpečení, které by zahrnovalo například jednorázové tokeny nebo časové razítko, mohou být autentizační požadavky zachyceny a znovu použity útočníkem k opětovnému získání neoprávněného přístupu.

5.9.5 Zvýšená zátěž a složitost správy

V prostředí s rozmanitými zařízeními a aplikacemi, jaké 5G sítě nabízejí, vyžaduje správa autentizace a autorizace pokročilé řízení identit a přístupových práv. Nedostatečné řešení může zvýšit administrativní zátěž a vést k chybám ve správě, které otevírají nové bezpečnostní mezery.

Opatření proti těmto rizikům vyžaduje komplexní přístup k zabezpečení s použitím silných autentizačních metod (vícefaktorová autentizace (MFA), šifrování, bezpečné tokeny) a dalších pokročilých technik, které zajišťují, že pouze oprávněné uživatele a zařízení mají přístup k síťovým zdrojům a službám. Kromě toho je důležité průběžné monitorování a revize bezpečnostních politik a postupů, aby byly aktuální.

6 Rizika spojená s implementací Open RAN a Open Core

Open RAN a Open Core umožňují flexibilnější a inovativnější přístup k vývoji a správě telekomunikačních sítí. Implementace Open RAN a Open Core architektur do 5G sítí přináší bezpečnostní výzvy a rizika zvláště spojená s integritou datového přenosu.

6.1 Nejasné hranice v rozdělení bezpečnostní zodpovědnosti

Rozdělení bezpečnostní zodpovědnosti v kontextu implementace těchto architektur je klíčovým rizikem, které negativně působí na bezpečnost a integritu datových přenosů v 5G sítích. Riziko se týká nejasností a potenciálních mezer v ochraně, které mohou vzniknout v důsledku víceúrovňové a distribuované povahy těchto architektur.

6.1.1 Zvýšené nároky na koordinaci v dodavatelském řetězci

Pro vysvětlení, v jakých místech je třeba sledovat a řídit riziko, slouží výčet rozdílností níže:

- Modulární a distribuovaná povaha: Open RAN a Open Core architektury umožňují telekomunikačním operátorům a poskytovatelům služeb kombinovat a integrovat komponenty a systémy od různých výrobců. Tato flexibilita vede k větší složitosti v koordinaci bezpečnostních politik a opatření mezi různými dodavateli a systémy.

- Různorodost dodavatelů a technologií: S množstvím dodavatelů a technologií se zvyšuje riziko nekonzistence v bezpečnostních standardech a praktikách. Ne všichni dodavatelé mohou mít stejnou úroveň zabezpečení, což může vytvářet slabá místa v celkové bezpečnostní architektuře.

- Komplexní řízení a aktualizace: Správa bezpečnosti a provádění aktualizací v takto rozmanitém a dynamickém prostředí vyžaduje koordinované a průběžné úsilí. Nejasnosti v zodpovědnosti za aktualizace bezpečnostních záplat a reakci na bezpečnostní incidenty mohou vést k zanedbání nebo opoždění v zavádění kritických bezpečnostních oprav.

6.1.2 Dílčí hrozby spojené s nesprávným rozdělením bezpečnostní zodpovědnosti

- Bezpečnostní mezery: Pokud není jasně určeno, kdo nese zodpovědnost za ochranu konkrétních aspektů síťové infrastruktury, nemusí dílčí oblast řídit nikdo a útočníci toho dokážou využít.

- Koordinace reakce na incidenty: V případě bezpečnostního incidentu může být rychlá a efektivní reakce komplikována nejasnostmi ohledně toho, kdo má incident řešit. Tato zpoždění mohou zhoršit dopady incidentu.

Protiopatření:

- Vytvoření jasných smluvních dohod: Smlouvy a dohody mezi operátory a dodavateli by měly jasně specifikovat rozdělení bezpečnostních zodpovědností a požadavky na bezpečnostní standardy.

- Standardizace a certifikace: Podpora a dodržování standardizovaných bezpečnostních protokolů a pravidel, včetně certifikace komponent a systémů, může pomoci zajistit konzistentní úroveň bezpečnosti napříč celým ekosystémem.

- Spolupráce a sdílení informací: Budování partnerství a kolaborativních sítí mezi operátory, dodavateli a bezpečnostními institucemi pro sdílení informací o hrozbách, zranitelnostech a nejlepších praktikách v oblasti bezpečnosti.

6.2 Rozšíření vstupních bodů a vektorů útoku v kontextu implementace Open RAN a Open Core

6.2.1 Zneužití otevřenosti a dynamiky Open RAN a Open Core

Se zneužitím otevřenosti a dynamiky Open RAN a Open Core se potýkáme ve vazbě na hlavní přednosti těchto architektur, kterými jsou flexibilita a adaptabilita. Body níže specifikují jeho konkrétní aspekty.

- Integrace komponent od různých výrobců: Open RAN a Open Core umožňují operátorům kombinovat hardwarové a softwarové komponenty od různých dodavatelů. Tato rozmanitost může ztížit zajištění konzistentní bezpečnosti napříč všemi prvky sítě, protože každý výrobce může mít jiné bezpečnostní postupy a standardy.

- Větší otevřenost systémů: Architektury podporující otevřené standardy a rozhraní jsou přirozeně náchylnější k zneužití, pokud nejsou náležitě zabezpečeny. Otevřenost usnadňuje interoperabilitu a inovace, ale také umožňuje útočníkům lépe porozumět interním mechanismům systému a potenciálně najít způsoby, jak je kompromitovat.

- Komplexní síťová konfigurace: Dynamické a flexibilní síťové konfigurace, které umožňují Open RAN a Open Core, mohou vést k obtížím při monitorování a ochraně proti bezpečnostním hrozbám. Správná konfigurace a údržba bezpečnostních politik vyžaduje pokročilé nástroje a expertizu.

6.2.2 Dílčí hrozby spojené se zneužitím otevřenosti a dynamiky Open architektur

- Neoprávněný přístup k segmentům sítě: Pokusy o přístup k síťovým segmentům, které by neměly být přístupné danému uživateli nebo zařízení nebo nezvyklé vzorce přihlášení do citlivých oblastí sítě.

- Neobvyklý síťový provoz mezi segmenty: Neobvykle vysoký objem dat přenášený mezi segmenty sítě, které obvykle nekomunikují a pokusy o komunikaci mezi segmenty, které by měly být izolovány.

- Anomálie ve virtuálních strojích a kontejnerech: Nezvyklé změny v konfiguraci nebo stavu virtuálních strojů (VM) nebo kontejnerů a pokusy o přístup nebo manipulaci s hypervisorem nebo správou virtualizace.

- Skryté sítě (tunneling): Detekce tunelování provozu, které může obcházet bezpečnostní politiky nebo segmentaci sítě. Použití neznámých nebo nepovolených protokolů pro skrytí komunikace.

- Neobvyklé změny konfigurace: Neplánované nebo neočekávané změny v konfiguraci sítě nebo virtualizačního prostředí. Změny v pravidlech firewallu nebo směrování, které nejsou schváleny nebo dokumentovány.

- Pokusy o eskalaci oprávnění: Aktivity směřující k získání vyšších oprávnění než má uživatel nebo zařízení přiděleno. Zneužití zranitelností pro získání administrátorských nebo root přístupů.

- Malware a neznámý software: Detekce instalace nebo spouštění neznámého nebo podezřelého softwaru ve virtuálních strojích nebo hostitelských systémech. Aktivita spojená s malwarem, jako je pokus o šíření mezi segmenty sítě nebo exfiltrace dat.

- Nezvyklé monitorovací a ladící aktivity: Použití nástrojů pro sledování nebo ladění, které nejsou běžně používány v daném segmentu sítě nebo prostředí. Neautorizované pokusy o sledování síťového provozu nebo systémových logů.

- Snadnější cílení útočníků: Větší počet rozhraní a komponent znamená více potenciálních vstupních bodů pro útočníky. Každá zranitelnost v jednom z těchto bodů může být využita k narušení integrity datového přenosu nebo k získání neoprávněného přístupu k síťovým zdrojům.

- Složitější detekce a řešení bezpečnostních incidentů: Rozsáhlejší a složitější síťová infrastruktura může ztížit včasnou detekci bezpečnostních incidentů a zpomalit reakci na ně, což zvyšuje riziko škody způsobené útočníky.

Protiopatření:

- Posílení bezpečnostních protokolů (např. SSH, TLS): Implementace pokročilých bezpečnostních protokolů a pravidelné aktualizace zabezpečení pro všechny komponenty sítě, včetně end-point zařízení a síťové infrastruktury. Zajištění, že veškerá správa síťových zařízení a aplikací probíhá přes bezpečné kanály, brání útočníkům v získávání citlivých informací.

- Šifrování dat v klidu a při přenosu: Použití silných šifrovacích algoritmů k ochraně dat uložených v systémech a přenášených přes síť chrání před odposlechem a únikem dat.

- Pokročilé monitorovací a detekční nástroje: Využití sofistikovaných nástrojů pro monitorování sítě a detekci anomálií, které mohou indikovat bezpečnostní hrozby, včetně pokusů o narušení integrity dat. Nepřetržité sledování síťového provozu a detekci anomálií.

- Automatizace reakce na incidenty: Implementace automatizovaných systémů pro reakci na incidenty, které mohou okamžitě reagovat na detekované hrozby, například izolací postižených segmentů nebo vypnutím kompromitovaných VM.

- Izolace kritických sítí a funkcí, segmentace sítí: Vytvoření bezpečnostních zón a použití virtualizace pro oddělení kritických sítových funkcí a služeb od ostatních částí sítě snižuje riziko šíření útoků.

- Zavedení firewallů a systémů pro prevenci průniku (IPS): Chrání hranice mezi segmenty sítě a monitoruje provoz na podezřelé aktivity.

- Školení a osvěta: Zajištění, aby všechny zúčastněné strany byly informovány o potenciálních bezpečnostních rizicích a nejlepších postupech pro jejich minimalizaci.

- Pravidelné audity a testování: Provádění pravidelných auditů a penetračních testů zaměřených na zajištění, že segmentace a virtualizace jsou správně konfigurovány a neobsahují zranitelnosti.

6.3 Nekompatibilita a chyby v konfiguraci

Kompatibilita a konfigurace představují zásadní výzvy v kontextu implementace Open RAN a Open Core architektur do 5G sítí. Týkají se integrace a efektivního fungování různorodých komponent a systémů od mnoha různých dodavatelů. Nejenže musí tyto systémy spolehlivě spolupracovat, ale musí také splňovat přísné bezpečnostní požadavky k ochraně datového přenosu a celkové integritě sítě.

6.3.1 Problematická konfigurace a správa

Složitost implementace a pozdější správy charakterizují následující styčné body:

- Integrace heterogenních systémů: Síťové komponenty a systémy v architekturách Open RAN a Open Core mohou pocházet od mnoha různých dodavatelů, každý s vlastními specifikacemi a protokoly. Zajištění jejich bezproblémové integrace a interoperability může být komplexní a náročné.

- Složitost konfigurace: S větším počtem konfigurovatelných komponent a parametrů se zvyšuje složitost správy a optimalizace sítě. Správná konfigurace je klíčová pro zabezpečení, výkon a spolehlivost sítě, ale také představuje větší prostor pro lidské chyby a konfigurační nedostatky.

- Aktualizace a údržba: Pravidelné aktualizace softwaru a firmwaru jsou nezbytné pro zabezpečení a funkčnost, ale koordinace těchto aktualizací napříč různorodými systémy a dodavateli může být výzvou. Nedostatečná údržba nebo nesprávné aktualizace mohou způsobit bezpečnostní zranitelnosti nebo výpadky služeb.

6.3.2 Dílčí hrozby spojené s problémy v konfiguraci a správy

- Bezpečnostní slabiny: Nesprávná konfigurace nebo nekompatibilita mezi systémovými komponentami může otevřít bezpečnostní mezery, které útočníci mohou využít k získání přístupu k síťovým zdrojům nebo k narušení integrity datového přenosu.

- Výpadky a snížení výkonu: Problémy s kompatibilitou a konfigurací mohou vést k nestabilitě sítě, výpadkům služeb a sníženému výkonu, což ovlivňuje konečné uživatele a může mít negativní dopad na důvěru v operátora.

Protiopatření:

- Podrobné testování a validace: Důkladné testování kompatibility a výkonu před nasazením v reálném prostředí může identifikovat a řešit potenciální problémy s kompatibilitou a konfigurací.

- Automatizace a nástroje pro správu konfigurace: Využití pokročilých nástrojů pro automatizaci konfigurace a správu změn může pomoci minimalizovat lidské chyby a zjednodušit správu komplexních sítí.

- Spolupráce a standardizace: Úzká spolupráce mezi operátory, dodavateli a standardizačními organizacemi může podporovat vytváření a dodržování standardů a protokolů, které usnadňují interoperabilitu a bezpečnou integraci komponent.

- Kontinuální vzdělávání a školení: Investice do vzdělávání a školení technických týmů zvyšují povědomí o nejlepších postupech konfigurace a zabezpečení, což přispívá k robustnější a bezpečnější síťové infrastruktuře.

Překonání výzev spojených s kompatibilitou a konfigurací vyžaduje kombinaci technologických, procesních a lidských faktorů. Klíčem k úspěchu je detailní plánování, pečlivé testování a neustálé zdokonalování procesů a dovedností.

6.4 Neoprávněný přístup, nespolehlivá autentizace

Řízení přístupu a autentizace představují kritické aspekty zabezpečení v kontextu implementace Open RAN a Open Core architektur do 5G sítí. Jsou zásadní pro ochranu proti neoprávněnému přístupu a zajištění, že pouze autorizovaní uživatelé a zařízení mohou komunikovat sítí a přistupovat k citlivým datům. Nedostatky v řízení přístupu a autentizačních mechanismech mohou významně zvýšit riziko narušení integrity datového přenosu a kompromitace celé sítě.

6.4.1 Problémy spojené s řízením přístupu a autentizací

Problémy spojené s řízením přístupu a autentizací nejlépe vystihují jejich hlavní činitelé níže:

- Složitost správy identit: V rozsáhlých a heterogenních sítích, jako jsou ty, které využívají Open RAN a Open Core, je správa identit uživatelů a zařízení značně složitá. Musí být zajištěno, že každý subjekt má přiděleny správné oprávnění a že tyto oprávnění jsou správně aplikovány napříč různými systémy a službami.

- Riziko slabých autentizačních protokolů: Použití zastaralých nebo slabých autentizačních metod může útočníkům usnadnit získání neoprávněného přístupu. V dynamickém prostředí 5G sítí je nezbytné používat silné a vícefaktorové autentizační metody.

- Nekonzistence v politikách přístupu: V mnohovrstvých a modulárních architekturách může být výzvou zajistit konzistenci bezpečnostních politik a pravidel přístupu napříč různými komponentami a dodavateli.

6.4.2 Dílčí hrozby spojené s neoprávněným přístupem či nespolehlivou autentizací

- Kompromitace dat a služeb: Slabiny v autentizaci a řízení přístupu mohou umožnit útočníkům přístup k citlivým datům nebo zneužití síťových služeb, což vede k narušení integrity a důvěrnosti dat.

- Rozšířené bezpečnostní incidenty: Jednou získaný neoprávněný přístup může útočníkům umožnit šíření napříč sítí, což komplikuje detekci a nápravu bezpečnostních incidentů.

Protiopatření:

- Implementace silných autentizačních mechanismů: Použití vícefaktorové autentizace (MFA) a pokročilých šifrovacích technologií zvyšuje bezpečnost při přístupu k síťovým zdrojům a službám.

- Použití silných politik hesel a klíčů: Zavedení silných politik pro vytváření a správu hesel a šifrovacích klíčů chrání před útoky hrubou silou a dalšími metodami prolomení autentizace.

- Centralizovaná správa identit a přístupových práv: Využití centralizovaných systémů pro správu identit (IDM) a správu přístupových práv (IAM) umožňuje efektivnější kontrolu nad tím, kdo má přístup, k jakým zdrojům a za jakých podmínek.

- Konzistentní politiky a pravidla přístupu: Vývoj a udržování konzistentních bezpečnostních politik a pravidel přístupu napříč všemi komponentami sítě a dodavateli zajišťuje, že všechny aspekty sítě jsou adekvátně chráněny.

- Pravidelná revize a audit přístupových práv: Periodické kontroly a auditování přístupových práv zajišťují, že oprávnění jsou stále aktuální a odpovídají potřebám uživatelů a bezpečnostním požadavkům.

Efektivní řízení přístupu a autentizace vyžadují neustálou pozornost a aktualizaci, aby reflektovaly měnící se bezpečnostní hrozby a vývoj technologií.

6.5 Rizika spojená s dodavatelským řetězcem

Rizika spojená s dodavatelským řetězcem představují významnou oblast obav v kontextu implementace Open RAN a Open Core architektur do 5G sítí. Tato rizika vyplývají z rozšířené závislosti na široké síti dodavatelů, kteří poskytují hardwarové komponenty, softwarové aplikace a služby. Vzhledem k tomu, že Open RAN a Open Core podporují větší otevřenost a interoperabilitu, může se síť stát náchylnější k zranitelnostem zavedeným prostřednictvím dodavatelského řetězce, což zahrnuje jak úmyslné, tak neúmyslné bezpečnostní hrozby. Reprezentativní rizika a jejich popis je uveden dále.

- Zranitelnosti a backdoory: Komponenty a software od dodavatelů mohou obsahovat skryté zranitelnosti nebo úmyslně vložené backdoory, které umožňují neoprávněný přístup nebo škodlivé aktivity. Tato rizika jsou zvláště znepokojující, pokud jsou zdroje těchto komponent nejasné nebo nedůvěryhodné.
    - Malware infikované aktualizace: Případ, kdy dodavatel omylem nebo úmyslně vydá aktualizaci softwaru obsahující malware, který může být následně distribuován do celé sítě, což vede k ohrožení dat a služeb.
    - Kompromitované komponenty: Fyzické součástky, jako jsou čipy nebo moduly, mohou obsahovat skryté zranitelnosti nebo škodlivé prvky, které byly zavedeny během výrobního procesu u subdodavatelů.

- Nesoulad s bezpečnostními standardy: Ne všichni dodavatelé mohou dodržovat stejné bezpečnostní standardy nebo mít stejnou úroveň zabezpečení, což může vést k nesouladu v bezpečnostních praktikách a oslabení celkové bezpečnosti sítě.
    - Nedostatečná údržba a podpora: Dodavatel, který nenabízí pravidelné aktualizace a záplaty pro své produkty, může být zdrojem zranitelností, které mohou být zneužity útočníky.

- Riziko narušení dodavatelského řetězce: Útoky na dodavatelský řetězec, kde útočníci kompromitují softwarové produkty nebo aktualizační mechanismy na nějakém bodě dodavatelského řetězce, mohou mít devastující dopad na množství uživatelů a sítí.

- Závislost na jednom dodavateli: Silná závislost na konkrétním dodavateli může zvýšit riziko, pokud tento dodavatel narazí na bezpečnostní problémy, bankrot nebo geopolitická rizika, která by mohla ovlivnit dodávky nebo podporu.

Protiopatření:

- Důkladná kontrola a audit dodavatelů: Pravidelné bezpečnostní audity a kontroly kvality u dodavatelů a jejich subdodavatelů k ověření, že dodržují přísné bezpečnostní standardy.

- Diverzifikace dodavatelů: Snížení závislosti na jednotlivých dodavatelích tím, že se využívají produkty a služby od více dodavatelů, což zvyšuje odolnost proti selhání.

- Průběžné monitorování a aktualizace: Implementace procesů pro průběžné monitorování bezpečnostního stavu používaných komponent a rychlá aplikace bezpečnostních aktualizací a záplat jsou klíčové pro udržení vysoké úrovně bezpečnosti.

- Silné smluvní podmínky: Stanovení jasných bezpečnostních požadavků ve smlouvách s dodavateli a zavedení sankcí za jejich nedodržení.

- Šifrování a autentizace: Použití šifrování a silných autentizačních mechanizmů k ochraně dat přenášených mezi různými komponentami a službami dodávanými různými dodavateli.

- Dodržování standardů a certifikace: Vybírání dodavatelů, kteří dodržují mezinárodně uznávané bezpečnostní standardy a mají certifikace, poskytuje určitou záruku kvality a bezpečnosti jejich produktů a služeb.

- Incidentní plánování a reakce: Vývoj a testování plánů pro reakci na incidenty spojené s dodavatelským řetězcem zajišťuje, že organizace může efektivně reagovat na bezpečnostní hrozby a minimalizovat jejich dopad.

7 Návrh způsobu zajištění dat v 5G sítích

Zajištění integrity a ochrany dat během přenosu v 5G sítích je klíčové pro jejich bezpečné a spolehlivé užívání. Existuje **několik způsobů, jak zajistit, aby data zůstala nedotčena a nezměněna během přenosu.**

7.1 Šifrování dat

Šifrování chrání data během jejich přenosu. Dále se věnujeme bližšímu popisu, jakým způsobem a jaké metody a standardy jsou šifrování dat v 5G sítích využívány.

Šifrování dat je proces, při kterém se původní čitelná data (tzv. plaintext) převádějí do zakódované formy (tzv. ciphertext), která je nečitelná pro každého, kdo nemá příslušný klíč potřebný k dešifrování. Tento proces zajišťuje, že i když jsou data zachycena během přenosu, nemohou být bez klíče přečtena nebo zneužita.

7.1.1 Základní typy šifrování využívané v 5G sítích

- Symetrické šifrování: Tato metoda používá stejný klíč pro šifrování a dešifrování dat. Je rychlá a efektivní pro přenos velkých objemů dat. V 5G sítích se často používá pro šifrování datového toku mezi uživatelským zařízením a sítí. Příkladem algoritmu symetrického šifrování může být AES (Advanced Encryption Standard).

- Asymetrické šifrování: Tato metoda využívá párování klíčů – veřejný klíč pro šifrování a soukromý klíč pro dešifrování. Asymetrické šifrování se obvykle používá pro bezpečný klíčový přenos, autentizaci a digitální podpisy. RSA (Rivest-Shamir-Adleman) je jedním z nejznámějších algoritmů asymetrického šifrování.

7.1.2 Implementace šifrování v 5G

Šifrování lze implementovat na různých úrovních, příklady shrnuje text dále:

- End-to-End šifrování: Tato metoda šifruje data na zdrojovém zařízení a dešifruje je až na cílovém zařízení, čímž minimalizuje riziko neoprávněného přístupu k datům během přenosu skrze různé síťové segmenty.

- Šifrování na úrovni transportní vrstvy: Protokoly jako TLS (Transport Layer Security) jsou používány k zajištění šifrované komunikace mezi klientem a serverem v 5G sítích. TLS je základem pro bezpečný web a je široce používán pro šifrování HTTP spojení.

- Šifrování na úrovni síťové vrstvy: K zajištění bezpečnosti na síťové vrstvě při komunikaci přes IP sítě se využívá nejčastěji protokol IPsec (Internet Protocol Security). IPsec je relevantní pro zabezpečení dat přenášených mezi 5G zařízeními a síťovými prvky.

Hlavními oblastmi, kterých se implementace šifrování dotýká, jsou správa klíčů, řešení výkonnosti a latence sítě a nasazení protokolů a relevantních praktik podle architektury sítě.

- Správa klíčů: Efektivní správa klíčů je zásadní pro zabezpečení šifrované komunikace. V 5G sítích je třeba zajistit, aby byly šifrovací klíče bezpečně distribuovány a obměňovány, aby se předešlo jejich kompromitaci.

- Výkonnost a latence: Zatímco šifrování zvyšuje bezpečnost, může také způsobit zvýšení latence a snížení výkonnosti sítě. Je důležité najít správnou rovnováhu mezi bezpečností a výkonností, aby bylo zajištěno, že zabezpečení neovlivní uživatelskou zkušenost.

- Standardizace a interoperabilita: Vzhledem k rozmanitosti zařízení a technologií využívaných v 5G sítích je nezbytná standardizace šifrovacích protokolů a praktik, aby byla zajištěna jejich interoperabilita a efektivní zabezpečení.

Použitím těchto šifrovacích metod a řešeními výzev spojených se šifrováním mohou 5G sítě poskytnout robustní ochranu dat přenášených mezi zařízeními a síťovými prvky, čímž vzniká garance, že data zůstanou během přenosu nedotčena a nezměněna.

7.2 Kontrola Integrity

Dalším způsobem zajištění integrity dat jsou **integritní kontroly**. Nabízí podrobnější pohled na to, jak lze zajistit, že data nebyla během přenosu změněna. Integritní kontrola je klíčová pro udržení důvěry a bezpečnosti v digitálním prostředí, zvláště v rámci rychlých a rozsáhlých datových přenosů typických pro 5G sítě.

Integritní kontrola je proces ověření, že data nebyla pozměněna od okamžiku svého vytvoření, odeslání či uložení. To se obvykle provádí pomocí kryptografických hash funkcí a digitálních podpisů, které umožňují ověřit autentičnost a integritu dat. Dále uvádíme jednotlivé možnosti s jejich popisem.

7.2.1 Kryptografické hash funkce

- Princip funkce: Hash funkce přijímá vstupní data libovolné délky a generuje z nich pevně daný, jedinečný hash (také nazývaný otisk). Pokud dojde k jakékoli změně v datech, i velmi malé, výsledný hash bude zcela odlišný. To umožňuje snadné ověření integrity dat.

V 5G sítích se hash funkce mohou používat pro ověření integrity sdílených dat mezi zařízeními a síťovými komponenty, což zabraňuje manipulaci s daty během jejich přenosu.

7.2.2 Digitální podpisy

- Princip fungování: Digitální podpis kombinuje hash funkcí vytvořený otisk dat s asymetrickým šifrováním. Odesílatel vytvoří otisk dat, který poté šifruje svým soukromým klíčem, čímž vytvoří digitální podpis. Příjemce může použít veřejný klíč odesílatele k dešifrování podpisu a porovnání otisku s hashem, který si sám vygeneruje z přijatých dat.

Digitální podpisy mohou se aplikují v 5G sítích k zajištění autenticity a integrity zpráv mezi uzly sítě a koncovými zařízeními. To je zásadní pro zabezpečené komunikační protokoly a služby.

7.2.3 Implementace kontrol integrity

Také implementace kontrol integrity se musí zaměřit na určité parametry charakteristik sítě a zvolit si mezi prioritami pro jejich vhodnou konfiguraci a aplikaci:

- Výběr silných hash funkcí: Je důležité vybrat hash funkce, které jsou odolné vůči kolizím (tj. dvě různé sady dat generují stejný hash). SHA-256 je příkladem silné hash funkce, která se často používá pro integritní kontrolu.

- Efektivní správa klíčů: V kontextu digitálních podpisů je klíčová efektivní správa kryptografických klíčů, aby se předešlo jejich kompromitaci. Bezpečná distribuce a obnova klíčů jsou zásadní.

- Výkon a latence: Zajištění integrity dat může zvýšit výpočetní nároky a potenciálně ovlivnit výkon a latenci sítě, což je v 5G sítích kritické. Je třeba najít rovnováhu mezi bezpečností a výkonem.

- Standardizace a kompatibilita: Ve světě 5G je nutné zajistit, aby metody integritní kontroly byly standardizovány a kompatibilní napříč různými zařízeními a sítěmi, což usnadňuje interoperabilitu a zabezpečení.

Implementací těchto metod integritní kontroly lze v 5G sítích efektivně chránit data před neoprávněnou manipulací a zajistit jejich integritu během přenosu. Tyto postupy, spolu s ostatními zabezpečovacími opatřeními, vytvářejí robustní obranný mechanismus pro ochranu dat v dynamickém a rozmanitém prostředí 5G technologií.

7.3 Vzájemná autentizace

Vzájemná autentizace přispívá k zabezpečení komunikace a zabraňuje různým útokům, včetně útoků typu "man-in-the-middle" (MITM). Vzájemná autentizace je proces, při kterém obě strany komunikující přes síť dokážou ověřit identitu druhé strany před zahájením výměny dat. Tento proces je klíčový pro zajištění důvěry a bezpečnosti v digitálních komunikačních kanálech.

Vzájemná autentizace se realizuje pomocí různých metod a protokolů, které umožňují oběma stranám ověřit, že jejich komunikační partner je skutečně tím, za koho se vydává. To se obvykle provádí prostřednictvím kryptografických klíčů, certifikátů, nebo pomocí jednorázových hesel.

7.3.1 Metody vzájemné autentizace v 5G sítích

Rozlišujeme 3 hlavní metody vzájemné autentizace využitelné v 5G sítích:

- Asymetrická kryptografie: Jednou z hlavních metod vzájemné autentizace je použití asymetrické kryptografie, kde každá strana má pár klíčů (veřejný a soukromý klíč). Veřejný klíč je sdílený a slouží k šifrování zpráv, které mohou být dešifrovány pouze odpovídajícím soukromým klíčem. Proces autentizace zahrnuje výměnu a ověření digitálních podpisů, které jsou vytvořeny pomocí soukromých klíčů a mohou být ověřeny veřejnými klíči.

- Certifikáty a PKI (Public Key Infrastructure): Vzájemná autentizace může být také založena na použití digitálních certifikátů, které jsou vydávány a podepisovány důvěryhodnými certifikačními autoritami (CA). Tyto certifikáty ověřují vlastnictví veřejných klíčů a umožňují oběma stranám ověřit identitu druhé strany.

- Autentizační a klíčové dohodovací protokoly: 5G sítě využívají sofistikované autentizační protokoly, jako je EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement), které umožňují bezpečnou vzájemnou autentizaci mezi uživatelským zařízením a síťovými prvky. Obě strany pak mohou bezpečně generovat a sdílet šifrovací klíče, které se používají pro ochranu komunikace.

7.3.2 Implementace vzájemné autentizace

Implementací vzájemné autentizace v 5G sítích lze výrazně zvýšit úroveň bezpečnosti a ochrany dat. Tento proces je základním kamenem pro budování důvěry mezi komunikujícími stranami a je nezbytný pro ochranu proti pokročilým kybernetickým hrozbám. Nasazení vzájemné autentizace determinují následující oblasti:

- Řízení a distribuce klíčů: Efektivní správa klíčů je zásadní pro úspěšnou implementaci vzájemné autentizace. To zahrnuje bezpečné ukládání, obnovu a revokaci klíčů a certifikátů.

- Zabezpečení proti útokům: Vzájemná autentizace musí být navržena tak, aby odolávala pokusům o MITM útoky a další pokusy o obejití autentizačních mechanismů.

- Kompatibilita a interoperabilita: Je důležité zajistit, aby autentizační metody byly kompatibilní s různými zařízeními a sítěmi v rámci 5G ekosystému a podporovaly interoperabilitu mezi různými operátory a službami.

7.4 Network slicing

Koncept "network slicingu" v 5G sítích je klíčová vlastnost, jež umožňuje vytvářet více virtuálních sítí na jedné fyzické síťové infrastruktuře. Každý takový "slice" může být přizpůsoben pro specifické požadavky aplikací, služeb nebo uživatelů, což zahrnuje různé úrovně bezpečnosti. Tato flexibilita je zvláště důležitá, protože 5G sítě slouží rozmanitému spektru aplikací od IoT přes autonomní vozidla až po kritické komunikace

Network slicing je proces, kdy je fyzická síť rozdělena na několik virtuálních sítí (slices), přičemž každá slice je nezávislá a může být individualizována podle specifických potřeb aplikace nebo služby. Tato technologie umožňuje operátorům optimalizovat a efektivně využívat své síťové zdroje.

7.4.1 Implementace network slicingu

Network slicing se implementuje za různými účely ve vazbě na bezpečnostní priority organizace:

- Izolace datových toků: Network slicing umožňuje oddělit datové toky různých uživatelů nebo služeb, což zabraňuje vzájemnému ovlivňování a potenciálním bezpečnostním rizikům. Například, data kritických aplikací mohou být izolována od běžného internetového provozu.

- Specifické bezpečnostní požadavky: Každá slice může být konfigurována s vlastními bezpečnostními politikami a mechanismy, odpovídajícími jejím specifickým potřebám. To umožňuje implementovat různé úrovně zabezpečení v závislosti na citlivosti a požadavcích na ochranu dat konkrétní aplikace nebo služby.

- Dynamické řízení bezpečnosti: Network slicing umožňuje operátorům dynamicky upravovat bezpečnostní politiky a nastavení v reakci na měnící se hrozby a bezpečnostní požadavky s možností rychle reagovat na incidenty, izolovat postižené segmenty sítě a zavádět specifická bezpečnostní opatření.

- Optimalizace výkonu a bezpečnosti: Umožňuje vyvážení mezi výkonem a bezpečností použitím slice specifické pro nízko-latentní aplikace, zatímco jiné slice mohou být optimalizovány pro maximální bezpečnost, například pro přenos citlivých informací.

Implementace network slicingu v 5G sítích vyžaduje pečlivé plánování, správu a sledování, aby bylo zajištěno, že všechny slices splňují své specifikované požadavky a zároveň poskytují robustní ochranu dat. Obdobně jako u ostatní způsobů zajištění dat v 5G sítích se v rámci implementace network slicingu zaměřujeme na správnou konfiguraci a splnění předpokladů úspěšné implementace:

- Správa a orchestrace: Efektivní správa a orchestrace slices jsou klíčové pro zajištění, že každá slice splňuje své bezpečnostní a výkonnostní požadavky. To vyžaduje sofistikované systémy pro sledování a řízení sítě.

- Standardizace a interoperabilita: Pro účinné nasazení network slicingu je nezbytná standardizace protokolů a rozhraní, aby bylo zajištěno, že různé technologie a zařízení mohou spolehlivě a bezpečně spolupracovat.

- Bezpečnostní rizika: Zatímco slicing poskytuje izolaci a může zvýšit bezpečnost, také přináší nové výzvy, jako je potřeba zabezpečit komunikaci mezi slices a správně konfigurovat bezpečnostní politiky pro každou slice.

7.5 Bezpečnostní protokoly a techniky

Zabezpečení dat při jejich přenosu prostřednictvím bezpečnostních protokolů a technik představuje významnou ochranu proti neoprávněnému přístupu, úniku informací a manipulaci s daty. Implementace bezpečnostních protokolů a technik je základem pro zajištění důvěrnosti, integrity a dostupnosti dat v 5G sítích. **Z bezpečnostních protokolů a technik můžeme volit mezi:**

- IPsec (Internet Protocol Security): IPsec je soubor protokolů pro zabezpečení Internet Protocol (IP) komunikace šifrováním a ověřováním na úrovni síťové vrstvy. V 5G sítích může být IPsec použit pro zabezpečení dat mezi síťovými prvky, například mezi 5G bázovými stanicemi a jádrem sítě, zajištěním, že data nemohou být odposlouchávána nebo manipulována během přenosu.

- TLS (Transport Layer Security): TLS je široce používán pro zabezpečení komunikace na transportní vrstvě, chrání data přenášená mezi aplikacemi a servery na internetu. V kontextu 5G sítí může být TLS využit pro zabezpečení komunikace mezi síťovými komponenty nebo pro zabezpečení služeb přistupujících k síti, jako jsou webové aplikace a API.

- DTLS (Datagram Transport Layer Security): DTLS poskytuje podobnou úroveň zabezpečení jako TLS, ale je navržen pro použití s protokoly založenými na datagramech, jako je UDP. Uplatní se pro 5G aplikace vyžadující nízkou latenci, jako jsou hlasové služby nebo IoT, kde je potřeba zabezpečit komunikaci bez výrazného dopadu na výkon.

- PFCP (Packet Forwarding Control Protocol): V 5G sítích se PFCP používá pro nastavení a správu uživatelských datových toků v jádru sítě. I když primárně slouží pro správu toků, bezpečnostní aspekty protokolu, jako je ověřování a autorizace řídících zpráv, jsou důležité pro ochranu síťové infrastruktury.

7.5.1 Implementace bezpečnostních protokolů a technik

Implementací a správným konfigurováním těchto bezpečnostních protokolů a technik mohou 5G sítě poskytnout robustní zabezpečení dat přenášených mezi zařízeními a síťovými komponentami, což je klíčové pro ochranu před neoprávněným přístupem a útoky. Zejména dynamické faktory 5G sítí, které musí být brány v potaz při jejich implementaci, shrnuje text dále:

- Správa klíčů a certifikátů: Efektivní správa klíčů a certifikátů je nezbytná pro zabezpečenou implementaci protokolů jako TLS a IPsec. Výzvou je udržet správu klíčů bezpečnou a současně dostatečně agilní, aby reagovala na změny a obnovu klíčů.

- Výkon a škálovatelnost: Zabezpečení musí být implementováno tak, aby minimalizovalo dopad na výkon a latenci v síti. To je obzvláště důležité v 5G, kde je důraz kladen na podporu aplikací vyžadujících nízkou latenci a vysoké rychlosti přenosu dat.

- Interoperabilita: S rozmanitostí zařízení a technologií v 5G ekosystému je zajištění interoperability mezi různými bezpečnostními protokoly a mechanismy klíčové. Standardizace a dodržování průmyslových standardů jsou nezbytné pro zajištění kompatibility a bezpečné komunikace.

- Neustálý vývoj a aktualizace: Bezpečnostní protokoly a technologie musí být neustále aktualizovány a přizpůsobovány, aby odolávaly nově vznikajícím hrozbám a zranitelnostem. To vyžaduje od operátorů a výrobců zařízení aktivní monitorování bezpečnostního prostředí a rychlou implementaci nezbytných aktualizací a oprav.

7.6 Detekce incidentů a reakce na incidenty

Poslední v této kapitole zmíněný způsob zajištění bezpečnosti dat v 5G síti je **detekce incidentů a reakce na incidenty** (uplatňování bezpečnostních zásad). Detekce a reakce na incidenty se zaměřuje na aktualizace a správu bezpečnostních zásad a postupů jako klíčový prvek pro zajištění, aby data v 5G sítích zůstala nedotčena a nezměněna během přenosu.

V dynamickém prostředí kybernetické bezpečnosti, kde se hrozby neustále vyvíjejí a mění, je monitorování a reakce na incidenty, pravidelná revize a aktualizace bezpečnostních protokolů, softwaru a hardware nezbytná pro udržení robustní obrany.

- Monitorování a reakce na incidenty:

    - Proaktivní monitorování: Kontinuální monitorování síťového provozu a systémových protokolů umožňuje rychlou identifikaci podezřelé aktivity nebo bezpečnostních incidentů. Operátoři tak rychle reagují a minimalizují potenciální škody.
    - Plány reakce na incidenty: Mít připravené a pravidelně aktualizované plány pro reakci na bezpečnostní incidenty je klíčové pro rychlé a efektivní řešení problémů. Plány by měly zahrnovat postupy pro izolaci postižených systémů, vyšetřování incidentů a obnovu poškozených dat nebo služeb.

- Pravidelné aktualizace softwaru a hardware:
    - Záplatování zranitelností: Aktualizace softwaru a firmware zařízení v 5G sítích jsou klíčové pro opravu zranitelností, které by mohly být zneužity útočníky. Pravidelné záplatování zabraňuje exploataci známých slabých míst.
    - Aktualizace bezpečnostních funkcí: Technologický pokrok a nové bezpečnostní techniky mohou poskytnout lepší ochranu nebo efektivnější výkon. Aktualizace mohou zahrnovat nové šifrovací algoritmy, vylepšené mechanismy autentizace a další pokročilé bezpečnostní funkce.

- Dodržování standardů a regulací: Zajištění, že síťové operace a bezpečnostní opatření jsou v souladu s mezinárodními standardy a právními předpisy, je zásadní pro ochranu dat a zajištění důvěry uživatelů. To zahrnuje standardy jako jsou ISO/IEC 27001, GDPR a další specifické normy pro telekomunikace a kybernetickou bezpečnost.

- Správa bezpečnostních zásad:
    - Revize a aktualizace bezpečnostních zásad: Pravidelná revize bezpečnostních politik a postupů zajišťuje, že reflektují aktuální hrozby a nejlepší praktiky. To zahrnuje aktualizace zásad přístupu, zásad šifrování dat, politik sledování a reakce na incidenty.
    - Školení zaměstnanců: Vzdělávání zaměstnanců a uživatelů síťové infrastruktury je zásadní pro zajištění, že jsou si vědomi aktuálních hrozeb a bezpečnostních postupů. Školení může snížit riziko bezpečnostních incidentů způsobených lidským faktorem.

7.6.1 Implementace

Implementací těchto opatření mohou organizace a operátoři 5G sítí efektivně chránit data před neustále se měnícími hrozbami a zajistit, že bezpečnostní opatření zůstávají aktuální a účinná v boji proti potenciálním útokům. Implementace tedy musí v tomto smyslu reagovat, tzn. zejména zvažovat adaptabilitu navržených opatření a posuzovat implementaci v kontextu komplexity:

- Adaptabilita: Síťové prostředí a hrozby se neustále vyvíjejí, což vyžaduje flexibilitu a adaptabilitu v bezpečnostních strategiích a postupech.

- Komplexnost správy: Rozsáhlé a dynamické 5G sítě představují výzvy v komplexnosti správy bezpečnosti, což vyžaduje pokročilé nástroje pro správu bezpečnosti a automatizaci.

8 Prověření a zhodnocení opatření pro ochranu 5G sítí před nepovolenou komunikací

Opatření pro ochranu 5G sítí před nepovolenou komunikací se zahraničními servery/sítěmi jsou klíčová pro zajištění bezpečnosti a integrity telekomunikační infrastruktury. Tato opatření mohou zahrnovat širokou škálu technik a postupů, od sofistikované systémy pro detekci a prevenci až po fyzického zabezpečení hardware.

8.1 Pokročilá detekce hrozeb a systémy prevence

Pokročilá detekce hrozeb a systémy prevence jsou základem pro ochranu 5G sítí před nepovolenou komunikací se zahraničními servery a dalšími bezpečnostními hrozbami. Tyto systémy kombinují několik technologií a metodik **pro identifikaci, analýzu a reakci na potenciální bezpečnostní incidenty v reálném čase.**

8.1.1 Systémy pro detekci a prevenci průniků (IDS/IPS)

Intrusion Detection Systems (IDS) jsou navrženy tak, aby pasivně monitorovaly síťový provoz a identifikovaly podezřelé aktivity nebo známé vzorce útoků. Pokud IDS detekuje potenciální hrozbu, vyvolá upozornění pro další analýzu.

Intrusion Prevention Systems (IPS) jsou krokem dále; nejenže detekují potenciální hrozby, ale jsou také schopny aktivně zasáhnout a zablokovat škodlivý provoz nebo izolovat napadená zařízení od zbytku sítě, čímž zabraňují šíření útoku.

Potenciální hrozby, na které se systémy pro detekci zaměřují a které indikují nepovolenou nebo nežádoucí komunikaci se zahraničními servery, jsou specifické geopoliticky a představují především:

1. Neobvyklý síťový provoz:
    - Anomální šířka pásma: Extrémně vysoké nebo nízké využití šířky pásma, které není běžné pro normální provoz.
    - Neobvyklý objem dat: Neočekávané velké množství přenesených dat, které může indikovat exfiltraci dat nebo DDoS útok.
2. Skenerové a průzkumné aktivity:
    - Port scanning: Pokusy o skenování portů za účelem nalezení otevřených portů a zranitelných služeb.
    - Network mapping: Pokusy o mapování sítě za účelem získání informací o síťové infrastruktuře a zařízení.
3. Podezřelé přihlašovací aktivity:
    - Brute-force útoky: Opakované neúspěšné pokusy o přihlášení, které mohou indikovat pokusy o uhodnutí hesel.
    - Neobvyklé přihlašovací lokace: Pokusy o přihlášení z geografických lokalit, které nejsou běžné pro daného uživatele.
4. Změny v síťové topologii:
    - Nové zařízení v síti: Neočekávané připojení nového zařízení, které může být potenciálně škodlivé.
    - Neautorizované změny konfigurace: Změny v nastavení síťových zařízení, které nebyly schváleny nebo zdokumentovány.
5. Škodlivý síťový provoz:
    - Malware komunikace: Přenosy dat mezi interními zařízeními a známými škodlivými IP adresami nebo doménami.
    - Command and Control (C2) komunikace: Pokusy o komunikaci s C2 servery, které útočníci používají k ovládání kompromitovaných zařízení.
6. Anomálie ve vzorcích provozu:
    - DoS útoky: Nárůst specifických typů provozu, které mohou indikovat Denial-of-Service útok.
    - Opakující se vzorce: Neobvyklé nebo opakující se vzorce provozu, které se liší od běžných provozních zvyklostí.
7. Neoprávněný přístup a eskalace oprávnění:
    - Zneužití oprávnění: Pokusy o přístup k citlivým datům nebo systémům bez odpovídajících oprávnění.

    - Eskalace oprávnění: Pokusy o získání vyšších úrovní oprávnění než je přiděleno.
8. Podezřelé aktivity na aplikační úrovni:
    - SQL injection: Pokusy o injektáž škodlivého SQL kódu do databází.
    - Cross-site scripting (XSS): Pokusy o vložení škodlivého kódu do webových stránek, které mohou být zneužity k útoku na uživatele.

IDS mohou generovat upozornění na podezřelé aktivity a poskytovat podrobnosti pro další analýzu. V kombinaci s Intrusion Prevention Systems (IPS), mohou nejen detekovat, ale také aktivně blokovat škodlivé provozy a izolovat kompromitovaná zařízení. Správci sítě pak mohou využít tyto informace k provedení hloubkové analýzy, potvrzení incidenty a nasazení vhodných opatření na jeho řešení.

8.1.2 Pokročilé analýzy

Přínosy v IDS a IPS systémech rozšiřují **pokročilé analýzy**, které jsou v robustních systémech inkorporovány buď v podobě behaviorální analýzy nebo sandboxingu:

- Behaviorální analýza: Tato technologie využívá strojové učení a umělou inteligenci k analýze normálního chování uživatelů a síťového provozu. Jakékoli odchylky od normálu, které by mohly naznačovat pokus o neautorizovanou komunikaci nebo jiný útok, jsou rychle identifikovány.

- Sandboxing a virtuální analýza: Potenciálně škodlivý kód nebo aplikace jsou spouštěny v izolovaném prostředí ("sandbox"), kde mohou být bezpečně analyzovány bez rizika poškození reálné sítě nebo dat.

8.1.3 Automatizovaná reakce a náprava

Systémy jsou často vybaveny nástroji pro **automatizovanou reakci**, které umožňují rychlé izolování napadených zařízení, zablokování škodlivých IP adres, aktualizaci bezpečnostních pravidel nebo dokonce automatické aplikování záplat na zranitelnosti.

8.1.4 Integrace s ostatními bezpečnostními systémy

V neposlední řadě účinná ochrana 5G sítě vyžaduje integraci IDS/IPS s dalšími bezpečnostními systémy, jako jsou firewally, systémy pro správu bezpečnostních informací a událostí (SIEM), a nástroje pro řízení hrozeb. Tato integrace umožňuje komplexní přehled o bezpečnostním stavu sítě a efektivnější reakci na hrozby.

8.1.5 Neustálé aktualizace a učení se

Aby byly IDS/IPS systémy nezastaraly v dynamickém světě komunikace, musí být pravidelně aktualizovány s nejnovějšími podpisy hrozeb a využívat nejnovější vědecké poznatky v oblasti detekce hrozeb. To zahrnuje průběžné učení se z nově detekovaných útoků a adaptaci na měnící se taktiky útočníků.

Implementace a správná konfigurace těchto systémů vyžaduje odborné znalosti a zkušenosti, jelikož nadměrné nebo nedostatečné využití může vést k falešným poplachům nebo přehlížení skutečných hrozeb. Právě proto je klíčové, aby organizace investovaly nejen do těchto technologií, ale také do odborného výcviku svých bezpečnostních týmů.

8.2 Šifrování dat

Šifrování dat je zásadním prvkem v ochraně komunikace se zahraničními prostředky v 5G sítích, chrání je před odposlechem, úpravami nebo zneužitím třetími stranami. Tato technologie zajišťuje, že informace mohou být dešifrovány a čteny pouze oprávněnými uživateli nebo systémy.

Při implementaci šifrování je důležité vyvážit bezpečnost, výkon a použitelnost. Šifrování může zvýšit zátěž na síťové zdroje a zařízení, což vyžaduje pečlivé plánování a optimalizaci. Je také klíčová pravidelná aktualizace a revize používaných šifrovacích algoritmů a protokolů, aby se předešlo zastarání a potenciálním bezpečnostním zranitelnostem.

Implementace robustního šifrování ve 5G sítích vyžaduje komplexní přístup, zahrnující nejen použití silných šifrovacích algoritmů, ale i správné řízení kryptografických klíčů a neustálou pozornost k bezpečnostním aktualizacím a nejlepším praktikám.

Vycházíme-li z předchozích informací, už nyní víme, že lze aplikovat různé úrovně šifrování. Pro přenos dat a komunikaci ze zahraničí jsou poplatné zejména níže zmiňované techniky.

8.2.1 End-to-End šifrování

End-to-end šifrování je proces, při kterém jsou data šifrována na straně odesílatele a dešifrována pouze na straně příjemce. To znamená, že data zůstávají šifrována během celé cesty přes síť, což brání jakémukoli i zahraničnímu útočníkovi ve čtení nebo manipulaci s daty, i když by se mu podařilo data zachytit.

8.2.2 Šifrování na úrovni sítě

Šifrování na úrovni sítě se týká šifrování dat, která procházejí přes síťovou infrastrukturu, jako jsou routery a přepínače. Toto šifrování je zvláště důležité pro ochranu dat, která jsou přenášena mezi různými částmi sítě, a pomáhá zabezpečit komunikaci mezi zařízeními a síťovými uzly.

8.2.3 Šifrování na úrovni aplikací

Šifrování na úrovni aplikací se zaměřuje na ochranu dat generovaných a spotřebovávaných konkrétními aplikacemi, které jsou nasazovány a jejichž dodavatelé mají obvykle zahraničního vlastníka. To zahrnuje šifrování zpráv, e-mailů, hlasových hovorů a jakýchkoli jiných dat, která aplikace zpracovává. Aplikace mohou používat vlastní šifrovací protokoly nebo využívat šifrování poskytované operačním systémem nebo platformou.

8.2.4 Protokoly, kryptografie a standardy pro šifrování

Klíčovou roli v šifrování zastupují bezpečnostní protokoly, kryptografické prvky a důraz na dodržování standardů pro šifrování. Využívané protokoly a techniky šifrování prezentují následující odstavce.

- Protokoly jako TLS (Transport Layer Security) a jeho předchůdce SSL (Secure Sockets Layer) jsou široce používány pro zabezpečení komunikace mezi webovými servery a prohlížeči. V kontextu 5G se mohou využívat i pro zabezpečení komunikace mezi síťovými komponentami.

- IPsec (Internet Protocol Security) je sada protokolů pro zabezpečení komunikace na síťové vrstvě, což umožňuje autentizaci a šifrování paketů na IP úrovni. To je klíčové pro zabezpečení VPN (Virtual Private Network) a jiných forem komunikace v 5G sítích.

- Správa kryptografických klíčů je zásadní pro účinné šifrování. To zahrnuje generování, distribuci, ukládání, výměnu, používání a odstraňování kryptografických klíčů. Bezpečná správa klíčů je nezbytná pro zabránění neoprávněnému přístupu k šifrovaným datům.

8.3 Segmentace sítě a virtualizace

Segmentace sítě a virtualizace jsou klíčové techniky používané pro zvýšení bezpečnosti a flexibility 5G sítí v komunikaci . Tyto metody umožňují izolovat různé části sítě, čímž se snižuje riziko šíření útoků a zvyšuje se efektivita správy zdrojů.

Segmentace sítě rozděluje síť na menší, spravovatelné segmenty, často nazývané sub-sítě. Tato rozdělení umožňují lepší kontrolu nad tokem dat a přístupem k síťovým zdrojům.

Klíčové aspekty segmentace sítě jsou:

- Izolace provozu: Segmentace odděluje citlivé části sítě (např. databáze s osobními údaji) od ostatních částí, čímž se snižuje riziko, že by útok na jednu část sítě mohl ovlivnit další citlivé části.

- Omezení šíření útoků: V případě bezpečnostního incidentu segmentace brání šíření útoku po celé síti, což usnadňuje izolaci a řešení problému.

- Zpřesnění bezpečnostních pravidel: Umožňuje vytvářet specifická bezpečnostní pravidla pro každý segment, což zlepšuje celkovou bezpečnostní politiku a efektivitu.

Virtualizace v 5G sítích se týká vytváření virtuálních, oddělených sítí na stejné fyzické infrastruktuře. To se často provádí pomocí technologií jako jsou SDN (Software-Defined Networking) a NFV (Network Functions Virtualization).

Klíčové vlastnosti virtualizace jsou:

- Flexibilita a škálovatelnost: Virtualizace umožňuje rychlé nasazování nových služeb a aplikací bez potřeby fyzických změn v síťové infrastruktuře.

- Lepší využití zdrojů: Umožňuje efektivnější využití síťových a výpočetních zdrojů rozdělením a alokací podle aktuálních potřeb.

- Dynamické řízení sítě: Poskytuje nástroje pro dynamické řízení síťového provozu a zdrojů, což zlepšuje výkon a zabezpečení sítě.

8.3.1 Specifika segmentace pro aplikace v 5G sítích

5G technologie umožňuje vznik virtuálních sítí (síťových slice), které mohou být přizpůsobeny pro konkrétní služby nebo aplikace, jako jsou autonomní vozidla, IoT zařízení nebo kritická infrastruktura. Tímto způsobem může být pro každou aplikaci zajištěna optimální úroveň výkonu a zabezpečení.

Implementace segmentace a virtualizace vyžaduje pečlivé plánování a správu, včetně definování přesných bezpečnostních pravidel pro každý segment nebo virtuální síť, pravidelné revize a aktualizace těchto pravidel a monitorování sítě pro identifikaci a reakci na bezpečnostní hrozby. Tyto metody, kombinované s dalšími bezpečnostními opatřeními, vytvářejí robustní rámec pro ochranu 5G sítí před nepovolenou komunikací a dalšími hrozbami.

8.4 Správa identit a přístupová práva

Správa identit a přístupových práv je základním kamenem zabezpečení 5G sítí, který se zaměřuje na ověřování a autorizaci uživatelů a zařízení, aby se zabezpečil přístup pouze k oprávněným entitám. Cílem opatření je prevence neoprávněného přístupu a zneužití síťových zdrojů.

Je důležité koncipovat systémy pro správu identit a přístupových práv jako pružné, snadno spravovatelné a schopné se přizpůsobit rychle se měnícím požadavkům sítě a jejích uživatelů.

Podíváme se nyní na jednotlivé vrstvy tohoto způsobu zabezpečení, které jsou relevantní pro komunikaci se zahraničními servery a jinou technologií.

8.4.1 Centrální správa identit

Centrální správa identit umožňuje centralizovanou správu uživatelských účtů a jejich oprávnění prostřednictvím procesů pro vytváření, správu, deaktivaci a odstraňování účtů. Centrální správa identit usnadňuje sledování a kontrolu přístupu k síťovým zdrojům.

8.4.2 Autentizace a autorizace

Silná autentizace vyžaduje od uživatelů nebo zařízení poskytnutí jednoznačného důkazu své identity, často prostřednictvím vícefaktorové autentizace (MFA), která kombinuje něco, co uživatel zná (heslo), s něčím, co má (bezpečnostní token nebo mobilní telefon), nebo něco, co je (biometrické údaje).

Autorizace pak určuje, k jakým zdrojům nebo službám má autentizovaný uživatel nebo zařízení přístup. To se obvykle řídí politikami založenými na rolích (RBAC) nebo politikami založenými na atributech (ABAC), které definují oprávnění na základě role uživatele nebo specifických atributů.

8.4.3 Správa přístupových práv

Správa přístupových práv zahrnuje monitorování a revizi přístupových práv, aby se zajistilo, že uživatelé a zařízení mají pouze taková oprávnění, která jsou nezbytně nutná pro jejich úkoly (princip minimálních oprávnění). Pravidelné revize pomáhají odhalit a odstranit zastaralá nebo nadbytečná oprávnění.

8.4.4 Identita jako služba (IDaaS)

Identita jako služba (IDaaS) je cloudové řešení, které poskytuje správu identit a přístupových práv jako službu. I jako služba řešení mohou nabídnout pokročilé funkce, včetně jednotného přihlášení (SSO), správy identit založené na cloudu a integrace s mnoha aplikacemi a službami.

8.4.5 Bezpečnostní tokeny a certifikáty

Bezpečnostní tokeny a certifikáty hrají klíčovou roli v autentizaci a šifrování komunikace mezi zařízeními a sítí. Tokeny a certifikáty jsou vydávány důvěryhodnými autoritami a používány pro ověření identity a zabezpečení dat.

8.4.6 Biometrická autentizace

Biometrická autentizace využívá unikátní fyzické nebo behaviorální charakteristiky jednotlivce (např. otisky prstů, rozpoznávání obličeje, hlasové vzory) pro ověření identity. Poskytuje vyšší úroveň zabezpečení než tradiční hesla nebo PINy.

8.5 Pravidelné aktualizace a opravy

Tyto činnosti zajistí, že software a firmware všech zařízení a komponent v síti jsou ochráněny proti známým hrozbám a zranitelnostem. Veřejně známé požadavky na opravy jsou snadným cílem útočníků.

Přínosy pravidelných aktualizací a oprav v rámci komunikace se zahraničím se uskutečňují kontinuálně v jednotlivých částech správy.

- Identifikace a hodnocení zranitelností

Aktivní monitoring a hodnocení zranitelností v síti a zařízeních je prvním krokem. To zahrnuje sledování bezpečnostních bulletinů, varování a doporučení od výrobců hardwaru a softwaru, stejně jako od bezpečnostních organizací a fór.

- Plánování a testování aktualizací

Plánování a testování aktualizací před jejich nasazením je zásadní pro minimalizaci rizika přerušení služeb nebo jiných negativních dopadů na síťovou infrastrukturu. To zahrnuje vytváření testovacích prostředí, která napodobují produkční sítě, aby se ověřila kompatibilita a bezpečnost aktualizací.

- Automatizace procesu aktualizace

Automatizace procesu aktualizací může výrazně zlepšit efektivitu a konzistenci nasazování oprav. Použití nástrojů pro správu konfigurace a automatizaci umožňuje správcům sítě pravidelně a systematicky aplikovat aktualizace napříč celou sítí.

- Zabezpečení distribuce aktualizací

Zabezpečení distribuce aktualizací je klíčové pro zabránění útočníkům v manipulaci s aktualizačními balíčky. To znamená použití šifrování a digitálních podpisů k ověření integrity a pravosti aktualizací.

- Řízení konfigurace

Řízení konfigurace je proces sledování a udržování konzistentních nastavení zařízení a softwaru v síti. Tento proces pomáhá identifikovat neautorizované změny, které by mohly zvýšit zranitelnost sítě.

- Vytváření záloh a plánů obnovy

Zálohování a plány obnovy jsou nezbytné pro rychlou obnovu v případě selhání aktualizace nebo bezpečnostního incidentu. Pravidelné zálohování konfigurací a důležitých dat zajišťuje, že síť může být rychle obnovena do bezpečného stavu.

- Osvěta a školení

Informování o nejlepších postupech, bezpečnostních opatřeních a postupech reakce na incidenty zaručí, že všechny osoby zapojené do správy sítě rozumí důležitosti a postupům pravidelných aktualizací a oprav.

8.6 Monitoring a auditování

Monitoring a auditování jsou zásadní složky bezpečnostní strategie pro 5G sítě, poskytující přehled o aktuálním stavu sítě integrovanou nebo komunikující se zahraničím, identifikaci potenciálních hrozeb a proaktivní reakci na bezpečnostní incidenty. Tyto procesy pomáhají zajišťovat, že veškeré neobvyklé nebo podezřelé aktivity jsou rychle rozpoznány a řešeny.

Odehrává se formou jak samotného monitoringu sítě, tak uplatňováním dalších technik.

8.6.1 Kontinuální monitoring sítě

Kontinuální monitoring zahrnuje neustálé sledování síťového provozu, záznamů, systémových událostí a výkonnostních metrik. Použití pokročilých nástrojů a technik, včetně SIEM (Security Information and Event Management) systémů, umožňuje real-time analýzu dat a rychlou detekci podezřelých nebo anomálních aktivit.

8.6.2 Analýza bezpečnostních událostí

Analýza bezpečnostních událostí pomáhá identifikovat potenciální bezpečnostní incidenty a určit jejich příčiny. To zahrnuje korelaci událostí z různých zdrojů, hodnocení závažnosti a případné klasifikace jako falešná pozitiva. Efektivní analýza vyžaduje kombinaci automatizovaných nástrojů a odborných znalostí.

8.6.3 Proaktivní hledání hrozeb

Proaktivní hledání hrozeb (Threat Hunting) je proces aktivního vyhledávání dosud neidentifikovaných hrozeb v síti. Spočívá v analýze vzorců provozu, anomálií a potenciálně podezřelých chování, které mohou naznačovat skryté útoky nebo kompromitace.

8.6.4 Auditování a dodržování předpisů

Auditování zahrnuje pravidelné na provozu nezávislé kontroly bezpečnostních politik, konfigurací a pravidel pro zajištění jejich správné implementace a účinnosti. Ověřuje se dodržování interních i externích předpisů a standardů, jako jsou GDPR, PCI-DSS, a další relevantní bezpečnostní rámce.

8.6.5 Logování a dokumentace

Logování a dokumentace jsou základem pro efektivní monitoring a auditování. Jejich součástí je ukládání podrobných záznamů o aktivitách v síti, změnách konfigurací, přístupu k systémům a detekovaných incidentech. Tyto záznamy jsou klíčové pro analýzu incidentů, forenzní vyšetřování a dodržování legislativních požadavků.

8.6.6 Vzdělávání a osvěta uživatelů

Vzdělávání a osvěta uživatelů hrají důležitou roli v bezpečnostním monitoringu a auditování tím, že pomáhají uživatelům rozpoznat a nahlásit podezřelé aktivity. Školení zaměstnanců a zvyšování povědomí o bezpečnostních hrozbách a nejlepších postupech může významně snížit riziko incidentů.

8.6.7 Spolupráce a sdílení informací

Spolupráce a sdílení informací mezi organizacemi, bezpečnostními týmy a externími subjekty, jako jsou bezpečnostní fóra a vládní agentury, zlepšuje schopnost odhalit a reagovat na nové hrozby. Výměna informací o hrozbách a osvědčených postupech podporuje kolektivní obranu proti kybernetickým útokům.

Implementace robustního monitoringu a auditování stojí na pokročilých technologiích, kvalifikovaném personálu a efektivních procesech. Tyto prvky společně vytvářejí dynamický obranný systém, který umožňuje rychlou identifikaci a reakci na bezpečnostní hrozby, zvyšuje odolnost 5G sítí a chrání důležité informace a služby.

8.7 Spolupráce s výrobci a mezinárodní spolupráce

Spolupráce s výrobci a mezinárodní spolupráce pomáhá v identifikaci, řešení a v důsledku minimalizaci potenciálních hrozeb a zranitelností.

8.7.1 Spolupráce s výrobci

Spolupráce s výrobci, která multiplikuje opatření na ochranu 5G sítí, dává příležitost posílit jejich účinnost v několika aspektech:

- Sdílení informací o zranitelnostech: Výrobci hardwaru a softwaru mohou sdílet informace o zjištěných zranitelnostech a doporučeních pro jejich opravu nebo zmírnění rizik. Toto sdílení informací umožňuje operátorům 5G sítí rychle reagovat na potenciální hrozby.

- Aktualizace a záplaty: Pravidelné aktualizace a záplaty od výrobců jsou nezbytné pro udržení bezpečnosti sítě. Spolupráce zajišťuje, že tyto aktualizace jsou rychle distribuovány a aplikovány, aby se předešlo zneužití známých zranitelností.

- Bezpečnostní doporučení: Výrobci mohou poskytovat doporučení a osvědčené postupy pro konfiguraci a správu zařízení a systémů. To pomáhá operátorům implementovat robustní bezpečnostní konfigurace a minimalizovat rizika.

- Technická podpora a spolupráce při řešení incidentů: V případě bezpečnostních incidentů mohou výrobci poskytnout technickou podporu a spolupracovat na analýze a řešení problémů, což pomáhá rychle obnovit bezpečný provoz sítě.

8.7.2 Mezinárodní spolupráce

Mezinárodní spolupráce má především preventivní charakter a umožňuje sdílet know-how. Odehrává se obvykle formou:

- Sdílení informací o hrozbách: Mezinárodní spolupráce mezi vládami, bezpečnostními agenturami a průmyslovými organizacemi umožňuje výměnu informací o kybernetických hrozbách a zranitelnostech. To zlepšuje schopnost odhalit a reagovat na globální hrozby.

- Společné normy a politiky: Mezinárodní organizace a standardizační orgány pracují na vývoji společných bezpečnostních standardů a politik pro 5G sítě. Společné normy usnadňují interoperabilitu a zajišťují konzistentní úroveň bezpečnosti napříč různými zeměmi a operátory.

- Spolupráce při řešení přeshraničních kybernetických incidentů: Kybernetické útoky často překračují národní hranice, což vyžaduje koordinovanou mezinárodní reakci. Spolupráce pomáhá v koordinaci reakce na tyto incidenty a posiluje globální kybernetickou obranu.

- Vzdělávání a výměnné programy: Programy pro vzdělávání a výměnu umožňují sdílení znalostí a osvědčených postupů mezi odborníky na kybernetickou bezpečnost z různých zemí. To podporuje budování silnějších a více informovaných bezpečnostních týmů.

Mezinárodní spolupráce vytváří tlak na urychlené řešení výzev spojených s bezpečností 5G sítí globálně. Kromě jiného podporuje sdílení kritických informací, zvyšuje povědomí o hrozbách a zlepšují schopnost reagovat na bezpečnostní incidenty.

8.8 Vzdělávání a osvěta

V dosavadním textu na různých místech zmíněné **vzdělávání a osvěta** si v kontextu zahraničních výzev v 5G sítích zaslouží samostatnou kapitolu. Vzdělávání a osvěta jsou zásadní pro pokrok a zvýšení bezpečnosti 5G sítí, protože lidský faktor hraje klíčovou roli v obraně proti kybernetickým hrozbám. Tento přístup se zaměřuje na informování všech účastníků sítě, od administrátorů až po koncové uživatele, o potenciálních hrozbách, nebo zkušenostech s incidenty, o nejlepších postupech pro zabezpečení a postupech pro reakci na incidenty.

Uskutečňuje se formou vzdělávacích programů pro zaměstnance, testováním zaměstnancům, průběžnou komunikací v organizaci a dalšími technikami.

8.8.1 Vzdělávací programy pro zaměstnance

Pravidelná školení a vzdělávací programy pro zaměstnance jsou zásadní pro udržení vysoké úrovně povědomí o kybernetické bezpečnosti. Tato školení by měla zahrnovat informace o aktuálních hrozbách, metodách sociálního inženýrství, bezpečném zacházení s daty a reakcích na bezpečnostní incidenty.

8.8.2 Simulace útoků a testování

Provedení simulovaných útoků, jako jsou phishingové kampaně, pomáhá testovat, jak dobře zaměstnanci rozpoznávají a reagují na pokusy o zneužití. Tato cvičení pomáhají identifikovat oblasti, kde je třeba zlepšit vzdělávání a osvětu.

8.8.3 Informační materiály a komunikace

Pravidelná komunikace o nejnovějších hrozbách, zranitelnostech a aktualizacích bezpečnostních politik je nezbytná pro udržení informovanosti všech účastníků sítě. Jedná se především o e-mailové bulletiny, interní webové stránky a online fóra pro diskuzi o bezpečnostních otázkách.

8.8.4 Vzdělávání koncových uživatelů

Vzhledem k tomu, že koncoví uživatelé mohou být cílem útoků, jako je phishing nebo malware, je důležité je informovat o rizicích a o tom, jak mohou chránit svá zařízení a data. To zahrnuje vzdělávání o bezpečném prohlížení internetu, používání silných hesel a aktualizaci softwaru.

8.8.5 Role-Based Training

Jedná se o školení zaměřené na konkrétní role. Různé role v organizaci mohou vyžadovat specifické znalosti a dovednosti v oblasti kybernetické bezpečnosti. Například technici a administrátoři potřebují hlubší pochopení bezpečnostních technologií a postupů, zatímco zaměstnanci v kontaktu s klienty musí být schopni rozpoznat a reagovat na hrozby zaměřené na zákazníky.

8.8.6 Spolupráce a sdílení nejlepších praktik (best practices)

Spolupráce mezi organizacemi, sdruženími a vládními agenturami může podporovat sdílení osvědčených postupů, nástrojů a strategií pro zvýšení bezpečnosti 5G sítí. Probíhá formou konferencí, workshopů a coworkingu.

Vzdělávání a osvěta představují nepřetržitý proces a podkladové materiály je nutné pravidelně aktualizovat a přizpůsobovat podle dynamiky výskytu bezpečnostních výzev a zranitelností. Vzdělávací programy a osvětové kampaně přispívají významně k odolnosti 5G sítí tím, že minimálně zvyšují povědomí o aktuálních hrozbách a podporují bezpečnostní kulturu ve všech úrovních organizace.

9 Návrh možných způsobů odhalování negativních jevů v 5G sítích

5G sítě přinášejí vysokou propustnost, nízkou latenci a masivní konektivitu pro Internet věcí (IoT), což otevírá nové možnosti provozu v reálném čase a integrace v aplikacích pro autonomní vozidla, inteligentní města a pokročilé průmyslové automatizace atp. **Odhalování negativních jevů v 5G sítích** je klíčové pro zajištění spolehlivosti, bezpečnosti a celkového výkonu těchto sítí.

9.1 Monitoring a analýza provozu v reálném čase

Monitoring a analýza provozu v reálném čase jsou zásadní pro udržení zdraví, výkonu a bezpečnosti 5G sítí. Tento proces zahrnuje sledování a vyhodnocování datového provozu v síti, aby bylo možné rychle identifikovat a řešit jakékoli potenciální problémy s rychlou odezvou.

Monitoring a analýza provozu v reálném čase tedy poskytují nezbytný základ pro proaktivní správu a ochranu 5G sítí, umožňující operátorům a správcům sítě rychle identifikovat a řešit potenciální problémy dříve než mohou mít významný dopad na služby poskytované koncovým uživatelům.

Odhalování negativních jevů se děje od sběru relevantních dat, v rámci různých technik analýzy a souvisí s integracemi na ostatní systémy, aby ve výsledku nezůstalo na statickém zaznamenání jevu a reakce byla zapojena v reálném čase.

9.1.1 Sběr dat

Pro odhalování negativních jevů hraje stěžejní roli kontinuita **sběru dat** a aktivita nad daty ve smyslu přezkušování latence, rychlosti přenosu a možných ztrát paketů.

- Pasivní monitoring: Neustálé sledování síťového provozu bez zasahování do přenosu dat. Zaměřuje se na analýzu metadat a hlaviček paketů pro získání přehledu o charakteristikách provozu.
- Aktivní testování: Zahrnuje generování a odesílání testovacích paketů skrze síť k měření výkonu, jako jsou latence, rychlost přenosu dat a ztráty paketů.

9.1.2 Analýza dat

Analýza dat je logickým krokem po jejich sběru. Směřuje hlavně k detekci anomálií a identifikaci odlišnosti ve vzorcích v provozu:

- Detekce anomálií: Použití algoritmů pro rozpoznávání odchylek od normálního provozního chování, které mohou signalizovat přetížení sítě, nefunkční hardware nebo softwarové chyby.
- Analýza vzorců: Identifikace specifických vzorců v provozu, které mohou ukazovat na kybernetické útoky, jako jsou DDoS (Distributed Denial of Service) útoky, šíření malwaru nebo pokusy o phishing.

V rámci analýzy se uplatňují různé nástroje a technologie pro hlubokou analýzu provozních dat. Hlavními představiteli jsou:

- Pokročilé analytické platformy: Využití sofistikovaných nástrojů, které kombinují technologie big data a umělé inteligence pro hlubokou analýzu provozních dat a rychlé zjišťování problémů.
- Síťové sondy a senzory: Rozmístění fyzických nebo virtuálních zařízení po celé síti, která shromažďují důležité informace o provozu a zdraví sítě.

9.1.3 Reakce na incidenty

Odhalování negativních jevů v 5G sítích **s reakcí v reálném čase** pracuje se systémy, které využívají automatizované reakce a systém notifikací správcům sítě.

- Automatizované reakce: Implementace systémů, které automaticky reagují na detekované problémy, například přesměrováním provozu, izolací postižených částí sítě nebo uplatněním bezpečnostních pravidel pro mitigaci útoků.

- Oznámení a eskalace: Systémy pro upozornění správců sítě na potenciální problémy a eskalace závažných incidentů pro rychlé řešení.

9.1.4 Integrace s ostatními systémy

Reakci na incidenty výrazně podporují integrace s ostatními systémy a sdílení informací.

Integrace s bezpečnostními nástroji se týká hlavně spolupráce s firewally, systémy pro detekci a prevenci proniknutí (IDS/IPS) a dalšími bezpečnostními mechanismy pro komplexní ochranu sítě.

Integrace s platformami pro sdílení informací o hrozbách (threat intelligence platforms) umožňuje síti reagovat na nově identifikované hrozby a zkracovat čas na jejich odezvu.

9.2 Pokročilé techniky strojového učení a umělé inteligence

Pokročilé techniky strojového učení (LM) a umělé inteligence (AI) hrají klíčovou roli v odhalování a řešení negativních jevů v 5G sítích. LM a AI technologie umožňují síťovým systémům učit se z dat, automaticky identifikovat vzorce chování a predikovat potenciální problémy dříve, než způsobí výpadky nebo bezpečnostní incidenty.

Kontinuální učení a adaptace modelů AI je nezbytná pro zachování jejich efektivity v dynamickém prostředí 5G sítí, kde se vzorce provozu a typy hrozeb neustále vyvíjejí.

LM a AI technologie se uplatňují při detekci anomálií a bezpečnostních hrozeb, prediktivní údržbě a optimalizaci sítě. Čím více jsou tyto technologie integrované s existujícími síťovými a bezpečnostními systémy, tím je reakce na stále sofistikovanější hrozby včasnější a účinnější, případně s nižšími náklady.

9.2.1 Detekce anomálií

Modely strojového učení jsou trénovány na normálních datech o síťovém provozu, aby se naučily rozpoznávat, co je typické chování sítě. Poté mohou efektivně identifikovat anomálie nebo odchylky, které mohou signalizovat technické problémy, přetížení sítě nebo kybernetické útoky.

Hluboké učení, forma strojového učení založená na neuronových sítích je obzvláště užitečná pro analýzu velkých objemů dat v reálném čase, což umožňuje odhalovat složité a subtilní anomálie, které by mohly uniknout tradičním detekčním metodám.

9.2.2 Prediktivní údržba

Prediktivní algoritmy využívají historická a reálná data pro predikci budoucích výpadků nebo potřeb údržby zařízení a infrastruktury. To umožňuje operátorům provádět preventivní opatření, dříve než dojde k problémům, což zvyšuje spolehlivost a dostupnost sítě.

Data z čidel a logů ze zařízení a infrastruktury poskytují cenné informace pro tyto prediktivní modely, protože umožňují detekovat vzorce, které předcházejí poruchám.

9.2.3 Optimalizace sítě

Algoritmy strojového učení mohou automaticky upravovat nastavení sítě pro optimalizaci výkonu a kapacity v reakci na měnící se vzorce provozu a požadavky uživatelů.

Reinforcement learning (učení s posilováním) umožňuje modelům AI "učit se" z vlastních akcí tím, že neustále hodnotí, jak dobře jejich rozhodnutí vedou k dosažení cílů, jako je zvýšení propustnosti nebo snížení latence.

9.2.4 Bezpečnostní hrozby

AI a strojové učení mohou identifikovat a klasifikovat bezpečnostní hrozby v reálném čase, odhalovat nové typy malwaru a automatizovaně implementovat bezpečnostní politiky pro obranu proti těmto hrozbám.

Systémy pro detekci a prevenci proniknutí (IDS/IPS) využívající AI mohou efektivněji rozpoznávat složité útoky, včetně těch, které využívají sofistikované metody obcházení tradičních bezpečnostních opatření.

9.2.5 Integrace na existující síťové a bezpečnostní systémy

Integrace s existujícími síťovými a bezpečnostními systémy přibližuje v reálném čase sdílení dat a informací o hrozbách mezi různými systémy a platformami do systémů pro zajištění koordinované a efektivní reakce na problémy.

9.3 Network slicing a izolace zdrojů problémů

Network slicing, neboli síťové segmentace je hlavní technologie v architektuře 5G, která umožňuje operátorům rozdělit jednu fyzickou síť na několik virtuálních síťových segmentů (slices). Každý slice může být optimalizován pro specifické potřeby různých typů služeb, aplikací nebo zákaznických skupin. Tento přístup umožňuje efektivnější využití zdrojů sítě a zajišťuje, že různé typy služeb mohou koexistovat na stejné fyzické infrastruktuře bez vzájemného negativního ovlivnění.

Network slicing posiluje způsoby odhalování negativních jevů spíše ve smyslu urychlení reakce na tyto jevy, zejména pak oddělením problematické nebo zasažené oblasti od ostatní síťové architektury. Děje se tak prostřednictvím izolace, přidělováním, aplikováním flexibility včetně té na úrovni garancí určitých parametrů provozu.

9.3.1 Izolace a zabezpečení

- Izolace zdrojů problémů: Network slicing umožňuje izolovat problémy v jednom slice, čímž se zabrání šíření problémů do ostatních slices. Například, pokud dojde k přetížení v slice určeném pro IoT zařízení, nebude to mít vliv na slice pro kritické komunikace, jako jsou služby nouzového volání.

- Zvýšená bezpečnost: Každý slice může mít svá vlastní bezpečnostní pravidla a konfigurace, což umožňuje lepší ochranu před kybernetickými hrozbami a usnadňuje dodržování regulatorních a compliance požadavků.

9.3.2 Efektivní využití zdrojů

- Dynamické přidělování zdrojů: Network slicing využívá výhody v dynamickém přidělování síťových zdrojů podle aktuálních potřeb jednotlivých slices. Týká se šířky pásma, výpočetní kapacity a úložiště, což zvyšuje efektivitu využití zdrojů a umožňuje rychle reagovat na měnící se požadavky služeb.

- Optimalizace pro specifické aplikace: Různé aplikace a služby mají různé požadavky na síťovou infrastrukturu. Například, aplikace vyžadující nízkou latenci, jako jsou autonomní vozidla nebo průmyslová automatizace, mohou být umístěny do slice s prioritou pro nízkou latenci, zatímco jiné služby, které potřebují vysokou propustnost, mohou být umístěny do jiného slice.

9.3.3 Flexibilita a škálovatelnost

- Rychlá reakce na měnící se požadavky: Network slicing umožňuje operátorům rychle reagovat na měnící se tržní požadavky nebo požadavky konkrétních zákazníků tím, že mohou vytvářet nebo upravovat slices podle potřeby.

- Škálovatelnost: Tato technologie umožňuje síti růst a přizpůsobovat se bez nutnosti významných změn ve fyzické infrastruktuře, což zjednodušuje nasazování nových služeb a rozšiřování stávajících.

9.3.4 Zlepšení kvality služeb (QoS)

- Garance kvality služeb: Každý slice může mít garantované parametry kvality služeb, což zajišťuje, že aplikace a služby běžící v rámci tohoto slice budou mít potřebnou šířku pásma, latenci a jiné síťové parametry.

- Přizpůsobení služeb zákazníkům: Operátoři mohou nabízet zákazníkům přizpůsobené síťové služby s garantovanými výkonovými parametry, což zvyšuje spokojenost zákazníků a umožňuje diferenciaci produktů.

Network slicing v 5G sítích tedy přináší revoluční změnu v způsobu, jakým jsou síťové zdroje alokovány a spravovány, a nabízí silný nástroj pro zajištění vysokého výkonu, bezpečnosti a efektivity sítě při současném uspokojování různorodých potřeb uživatelů a aplikací.

9.4 Bezpečnostní protokoly a šifrování

Tyto technologie nejen zajišťují bezpečnost komunikace mezi zařízeními a sítí, ale také chrání integritu a soukromí dat. Vzhledem k rozsáhlému využití 5G sítí, od mobilních telefonů přes IoT zařízení až po kritickou infrastrukturu, je zabezpečení dat a komunikace klíčové pro prevenci úniků dat, kybernetických útoků a jiných bezpečnostních hrozeb.

9.4.1 Zabezpečení na různých úrovních

Bezpečnostními protokoly a šifrování je spíše technikálie, zabraňuje negativním jevům, než aby přímo vedly k jeho odhalení. Vhodné zabezpečení se odvíjí podle úrovní, na kterých je aplikováno.

- Šifrování na úrovni datového toku: Každý datový tok mezi zařízením a síťovým uzlem je šifrován, což zajišťuje, že data zůstanou soukromá a nedostupná pro neoprávněné strany. Toto šifrování se vztahuje na všechny typy dat, včetně hlasové komunikace a datového přenosu.

- Bezpečnostní protokoly pro ověřování: Protokoly jako EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement) jsou používány pro ověřování zařízení a uživatelů v síti, což zabraňuje neautorizovanému přístupu.

Šifrování, bezpečnostní protokoly, autentizace a dodržování standardů mají za úkol spíše preventivní ochranu nebo patřičnou reakci na negativní jevy, ale nelze je v procesu možných způsobů odhalování negativních jevů opomenout, neboť minimálně data ze šifrovacích algoritmů a pokusů obejít systémy šifrování a ochrany indikují negativní jevy. Zopakujeme si tedy jednoduchým výčtem, jak nám šifrovací techniky a další bezpečnostní správa techniky poslouží.

9.4.2 Šifrovací algoritmy

- Moderní šifrovací algoritmy: 5G sítě využívají pokročilé šifrovací algoritmy, jako je AES (Advanced Encryption Standard), který poskytuje vysokou úroveň bezpečnosti. Tyto algoritmy jsou pravidelně aktualizovány a posilovány, aby odolávaly pokročilým dešifrovacím a kybernetickým útokům.

- Veřejné klíče a soukromé klíče: Systémy šifrování založené na veřejných a soukromých klíčích umožňují bezpečnou výměnu klíčů mezi komunikujícími stranami bez nutnosti předávat klíč přes nezabezpečené kanály.

9.4.3 Integrita dat a autentizace

- Protokoly pro zajištění integrity dat: Kromě šifrování dat, 5G sítě implementují protokoly jako IPsec (Internet Protocol Security) pro zajištění integrity dat a autentizace na internetové vrstvě, což zabraňuje manipulaci s daty během jejich přenosu.

- Autentizace zpráv: Digitální podpisy a certifikáty jsou používány pro ověřování zpráv a transakcí, což zajišťuje, že data pocházejí od legitimního zdroje a nebyla pozměněna.

9.4.4 End-to-end šifrování

- Šifrování od koncového zařízení k síťovému uzlu: End-to-end šifrování zajišťuje, že data jsou šifrována od zdroje až po cíl, což zabraňuje odposlechu a manipulaci s daty během přenosu skrze různé síťové segmenty.

- Výzvy pro implementaci: Přestože end-to-end šifrování poskytuje významnou úroveň bezpečnosti, jeho implementace může být komplexní vzhledem k potřebě správy klíčů a kompatibility mezi různými zařízeními a službami.

9.4.5 Soulad s regulacemi a standardy

- Dodržování mezinárodních standardů: 5G sítě musí splňovat mezinárodní bezpečnostní standardy a regulace, jako jsou ty stanovené Mezinárodní telekomunikační unií (ITU) a 3rd Generation Partnership Project (3GPP).

- Průběžná aktualizace a hodnocení: Bezpečnostní protokoly a šifrovací mechanismy musí být pravidelně revidovány a aktualizovány, aby odrážely nejnovější vývoj v oblasti bezpečnostních hrozeb a technologií.

9.5 Penetrační testování a simulace útoků

Penetrační testování a simulace útoků jsou hlavními nástroji pro identifikaci slabých míst v 5G síťové infrastruktuře a ověřování efektivity implementovaných bezpečnostních opatření. Tyto techniky představují proaktivní přístup k odhalování negativních jevů, simulují potenciální útočné scénáře a pomáhají identifikovat a řešit zranitelnosti dříve, než je zneužijí skuteční útočníci.

Jednotlivé úkoly penetračního testování případně simulace útoků lze charakterizovat níže:

- Identifikace zranitelností: Cílem je identifikovat slabá místa v síťové infrastruktuře, konfiguraci, softwaru a protokolech, které by mohly být využity útočníky.

- Simulace skutečných útočných scénářů: Testování zahrnuje simulaci široké škály útoků, včetně DDoS útoků, útoků na základě zranitelností v softwaru, phishingu a dalších kybernetických hrozeb.

- Ověření efektivity bezpečnostních opatření: Testy pomáhají ověřit, jak efektivně existující bezpečnostní opatření a protokoly chrání síť před potenciálními útoky.

9.5.1 Skenování zranitelností a penetrační testování v 5G sítích

Skenování zranitelností a penetrační testování jsou techniky používané k identifikaci a řešení bezpečnostních hrozeb v 5G sítích. Obě metody mají své specifické postupy a nástroje, které se vzájemně doplňují a společně poskytují komplexní přehled o bezpečnostním stavu sítě.

Cílem **skenování zranitelností** je rychlé a automatizované odhalení potenciálních bezpečnostních slabin v síťové infrastruktuře, zařízeních a aplikacích. Skenování zranitelností se provádí pravidelně, aby bylo zajištěno, že nově objevené zranitelnosti jsou rychle identifikovány a řešeny.

Navíc výhodou skenování zranitelností je, že může být prováděno pravidelně s minimálním manuálním zásahem, dokáže pokrýt velké množství zařízení a aplikací za krátkou dobu a je efektivní při odhalování známých zranitelností, které mají odpovídající bezpečnostní záplaty nebo řešení.

Proces skenování zranitelností má tyto fáze:
- Sběr informací: Identifikace síťových aktiv, služeb a aplikací, které mají být skenovány.
- Skenování pomocí nástrojů: Použití specializovaných skenerů zranitelností, jako jsou Nessus, OpenVAS nebo Qualys, k provádění automatizovaných kontrol na základě databází známých zranitelností.
- Analýza výsledků: Vyhodnocení výsledků skenování k identifikaci konkrétních zranitelností, jejich závažnosti a potenciálního dopadu na síť.
- Nápravná opatření: Doporučení a implementace opatření k odstranění identifikovaných zranitelností, jako je aplikace bezpečnostních záplat nebo změna konfigurace.

Oproti tomu penetrační testování simuluje reálné kybernetické útoky s cílem identifikovat zranitelnosti, které by mohly být zneužity útočníky. Testování nejen odhaluje zranitelnosti, ale také ověřuje, jak mohou být skutečně zneužity a jaký dopad by měly na bezpečnost a provoz sítě.

Hlavní výhody penetračního testování je, že poskytuje realistický pohled na bezpečnostní stav sítě tím, že simuluje skutečné útoky. Dále je penetrační testování schopné odhalit složitější zranitelnosti, které nemusí být zachyceny automatizovaným skenováním a ověřit účinnost bezpečnostních opatření.

Proces penetračního testování je složitější a komplexnější a představuje širší spektrum aktivit při jeho nasazování:
- Plánování a rozsah: Definování cílů a rozsahu testování, včetně určení, které systémy a aplikace budou testovány.
- Sběr informací: Shromažďování informací o cílové síti a systémech, včetně mapování sítě, identifikace aktivních služeb a zjišťování verzí softwaru.
- Identifikace zranitelností: Použití nástrojů a manuálních technik k identifikaci potenciálních zranitelností.
- Exploatace zranitelností: Pokusy o využití identifikovaných zranitelností k získání přístupu nebo zneužití systému, což simuluje reálné útočné techniky.
- Post-exploatační aktivity: Analýza možností dalšího pohybu po síti a získání přístupu k dalším systémům nebo datům.
- Analýza a reportování: Dokumentace provedených kroků, identifikovaných zranitelností a doporučení pro jejich řešení.
- Oprava a ověření: Implementace doporučených opatření a následné ověření, že zranitelnosti byly účinně odstraněny.

9.5.2 Význam odhalování negativních jevů pro 5G sítě

Negativní jevy v 5G sítích, jakožto komplexním prostředí a jejich odhalování čelí v důsledku sofistikovanějších technik útoků a deklarované inovativnosti poptávce, která nesmí být zklamáním počínaje běžnými uživateli sítě po ty z oblasti autonomních technologií a průmyslových automatizací. Týká se především:

- Zajištění bezpečnosti kritické infrastruktury: Vzhledem k tomu, že 5G sítě budou sloužit jako základ pro kritickou infrastrukturu a služby, je nezbytné zajistit jejich maximální možnou bezpečnost.
- Ochrany proti složitým a vývojovým hrozbám.
- Podpory důvěry a spolehlivosti: Provozovatelé 5G sítí musí zajistit, aby jejich sítě byly důvěryhodné a odolné vůči útokům, což je klíčové pro podporu obchodních a osobních aplikací.

9.6 Spolupráce a sdílení informací o hrozbách

Spolupráce a sdílení informací o hrozbách mezi operátory, výrobci zařízení a vládními agenturami je dalším způsobem, jak odhalovat negativní jevy 5G sítí. Vzhledem k rychlému vývoji a sofistikovanosti těchto hrozeb je nezbytné, aby všichni zúčastnění aktéři v ekosystému 5G sítí spolupracovali a sdíleli relevantní informace, což umožňuje rychlou reakci a zajištění ochrany.

Vytvořením sdílených databází hrozeb, mezinárodní a sektorovou spoluprací a dynamickou aktualizací bezpečnostních opatření rozšiřují všichni účastníci způsoby, jak včas identifikovat a odhalovat bezpečnostní hrozby.

9.6.1 Vytvoření sdílených databází hrozeb

Pro identifikaci a sdílení negativních jevů slouží databáze buď jako centralizované platformy nebo jako databáze signatur malware a indikátorů kompromitace:

- Centralizované platformy pro sdílení informací: Vytvoření společných platforem, jako jsou informační střediska pro sdílení hrozeb (Threat Intelligence Sharing Platforms), umožňuje sběr, analýzu a distribuci informací o hrozbách mezi zúčastněnými stranami.
- Databáze signatur malware a indikátorů kompromitace (IoC): Sdílení těchto informací pomáhá organizacím rychle identifikovat a reagovat na nově objevené negativní jevy.

9.6.2 Mezinárodní a sektorová spolupráce

Ke spolupráci v oblasti detekce negativních jevů se využívá obecně globální síť pro výměnu informací (mezi státy, mezinárodními organizacemi a sektory) anebo působí specializované skupiny (ISACs), které spolupracují ve specifickém sektoru a sdílí si relevantní informace v rámci svého oboru podnikání.

Úlohu podpůrných nástrojů po detekci negativních jevů a jejich sdílení plní pak zejména dynamická aktualizace bezpečnostních opatření, společné normy a protokoly a v neposlední řadě společný vývoj a výzkum.

- Dynamická aktualizace bezpečnostních opatření – Systémy mohou být nastaveny tak, aby automaticky přijímaly aktualizace bezpečnostních signatur a pravidel na základě sdílených informací.
- Společné normy a protokoly - Používání standardizovaných formátů, jako je STIX (Structured Threat Information eXpression) a TAXII (Trusted Automated Exchange of Indicator Information), usnadňuje interoperabilitu a efektivitu výměny informací o hrozbách.
- Výzkum a vývoj - Spolupráce podporuje výzkum a vývoj v oblasti pokročilých obranných technologií a strategií pro boj proti kybernetickým hrozbám.

10 Schopnosti 5G sítí vybudovaných v prostředí Open RAN odolávat DDoS útokům

Prověření a zhodnocení schopnosti 5G sítí vybudovaných v prostředí Open RAN **odolávat distribuovaným útokům odepření služby (DDoS**) je komplexní úkol. 5G sítě a Open RAN přinášejí nové přístupy a technologie do oblasti mobilních komunikací, které mají potenciál zvýšit flexibilitu, snížit náklady a podpořit inovace.

10.1 Architektura Open RAN

Open RAN, neboli Otevřená Rádiová Přístupová Síť je iniciativa zaměřená na standardizaci a otevření rozhraní a implementací v rádiových přístupových sítích. Tento přístup umožňuje operátorům kombinovat a používat hardware a software od různých výrobců, což vede k větší flexibilitě, snížení závislosti na jednom dodavateli a potenciálně nižším nákladům.

Klíčové výhody architektury Open RAN tedy spočívají ve:

- Flexibilitě a inovacích: Otevřené rozhraní umožňují snazší integraci nových technologií a služeb, což může zrychlit inovace.
- Snížení nákladů: Možnost vybírat mezi různými dodavateli může vést k cenové konkurenci a snížení nákladů pro operátory.
- Odolnosti a spolehlivosti: Diversifikace dodavatelů a komponent může zvýšit odolnost sítě proti výpadkům a útokům, protože neúspěch jednoho komponentu nevede nutně k selhání celé sítě.

Na opačnou stranu misky vah náleží ale **nedokonalosti s architekturou Open RAN spojené**:

- Složitost a integrace: Integrace komponent od různých výrobců přináší složitost, což může ztížit zabezpečení a správu sítě.
- Rozhraní a standardy: Otevřené rozhraní vyžadují pečlivé zabezpečení, aby se zabránilo zneužití. Standardizace je klíčová, ale může také představovat výzvu v rychle se vyvíjejícím prostředí.
- Dodavatelský řetězec: Rozšíření dodavatelského řetězce zvyšuje riziko zranitelností a útoků spojených s dodavatelským řetězcem.

10.2 Bezpečnostní rámec 5G sítí

5G technologie přináší významná zlepšení ve výkonu, kapacitě a efektivitě, ale také naráží na nové bezpečnostní jevy. **Bezpečnostní rámec 5G** je navržen tak, aby řešil tyto výzvy prostřednictvím zejména rozšířeného šifrování, zlepšování ochrany identity uživatelů a zařízení, a pokročilých mechanismů pro integritu a ochranu dat.

10.2.1 Integrace s Open RAN:

Bezpečnostní rámec 5G musí být pečlivě integrován s Open RAN architekturou, aby se zajistilo, že všechny otevřené a interoperabilní komponenty plně respektují a využívají bezpečnostní opatření definovaná pro 5G.

Týká se především zabezpečení rozhraní mezi různými částmi sítě, ochrany proti útokům na dodavatelský řetězec, a implementace pokročilých detekčních a reakčních mechanismů proti DDoS útokům.

10.3 Specifika DDoS útoků v kontextu 5G a Open RAN

5G a Open RAN sítě mají schopnost reagovat na specifika distribuovaných útoků odepření služby (DDoS) ze své podstaty nebo na úrovni inkorporovaných ochranných opatření. Nejprve si **shrneme specifika DDoS úkolů v 5G**:

- Vysoké rychlosti a nízká latence 5G: 5G sítě jsou navrženy pro podporu vysokých rychlostí datového přenosu a nízké latence. Tyto vlastnosti mohou být zneužity při DDoS útocích, jelikož útočníci mohou generovat větší objem škodlivého provozu v kratším časovém úseku, což zvyšuje potenciální dopad útoku na cílové služby a infrastrukturu.

- Distribuovaná a heterogenní povaha Open RAN: Open RAN architektura podporuje integraci komponent a řešení od různých výrobců, což může vést k rozšířenému a distribuovanému modelu sítě. Zatímco toto může přinést výhody z hlediska flexibility a odolnosti, také to může zkomplikovat detekci a mitigaci DDoS útoků, protože útok může být distribuován přes různé části sítě a zdroje.

- Exploatace síťových funkcí a protokolů: 5G a Open RAN zavádějí nové síťové funkce a protokoly, které mohou být potenciálně zneužity pro provádění DDoS útoků. Například, pokud útočníci získají kontrolu nad dostatečným počtem zařízení připojených k síti 5G, mohou tyto zařízení využít pro generování škodlivého provozu směřujícího na specifické cíle.

- Složitost správy a monitorování: Integrace a správa heterogenních síťových komponent v prostředí Open RAN může být náročná, což ztěžuje kontinuální monitorování a rychlou reakci na potenciální DDoS útoky.

- Bezpečnostní mezery a zranitelnosti: Možné bezpečnostní mezery mezi různými komponentami a dodavateli mohou poskytnout útočníkům vstupní body pro zahájení DDoS útoků.

- Zajištění interoperability a bezpečnosti: Udržení interoperability mezi různými komponentami a zároveň zajištění vysoké úrovně bezpečnosti je klíčovou výzvou, která vyžaduje pečlivé plánování a implementaci bezpečnostních protokolů.

10.3.1 Ochranná opatření a mitigace

Zvládnutí DDoS útoků v prostředí 5G a Open RAN vyžaduje technologická opatření, procesní zabezpečení a meziorganizační spolupráci. Zajištění odolnosti proti těmto útokům je neustálým procesem, který musí reflektovat neustále se vyvíjející kybernetické hrozby. Děje se konkrétně za působení:

- Rozšířeného monitorování a detekce: Implementace nástrojů pro monitorování síťového provozu a detekci anomálií je zásadní pro identifikaci a reakci na DDoS útoky v jejich počátečních fázích.

- Pokročilé detekce a analýza: Využití pokročilých technologií pro detekci útoků, jako jsou umělá inteligence (AI) a strojové učení (ML), umožňuje rychlé rozpoznání abnormálního provozu a potenciálních DDoS útoků. Tyto systémy se neustále učí z nových dat a dokážou přizpůsobit své reakce na měnící se vzorce útoků.

- Network slicingu a izolace útoků: Network slicing, klíčová vlastnost 5G sítí, umožňuje operátorům vytvářet izolované virtuální sítě (slices) s vlastními zabezpečenými a optimalizovanými prostředky. V případě DDoS útoku může být útok izolován do specifického slice, čímž se minimalizuje jeho dopad na ostatní části sítě.

- Dynamického řízení přístupu a filtrace provozu: Dynamická kontrola přístupu a inteligentní filtrace provozu na základě behaviorálních vzorců a reputace IP adres může pomoci identifikovat a blokovat škodlivý provoz ještě předtím, než dosáhne kritických komponent sítě.

- Zabezpečením Multi-Vendor správy: V nejednotném dodavatelském prostředí Open RAN je zásadní zajistit, že všechny komponenty a služby od různých výrobců splňují stejné vysoké bezpečnostní standardy. To zahrnuje pečlivý výběr dodavatelů, pravidelné bezpečnostní audity a testování kompatibility a zabezpečení mezi různými systémy.

- Škálovatelné a průběžné ochrany: Ochrana proti DDoS útokům musí být škálovatelná, aby dokázala absorbovat a zpracovat velké objemy škodlivého provozu. To zahrnuje využití cloudových služeb pro distribuci zátěže a absorpci útoků, stejně jako průběžnou aktualizaci ochranných systémů.

- Kooperace a sdílení Informací: Spolupráce mezi telekomunikačními operátory, dodavateli technologií, bezpečnostními firmami a vládními agenturami je klíčová pro výměnu informací o hrozbách, nejnovějších taktikách útočníků a efektivních metodách obrany. Sdílení informací pomáhá vytvářet silnější obranný štít proti DDoS útokům a zlepšuje celkovou kybernetickou odolnost.

- Edukačních programů a osvěty: Informovanost a vzdělávání zaměstnanců o bezpečnostních hrozbách a nejlepších postupech pro jejich prevenci jsou zásadní pro posílení první linie obrany. Edukace může zahrnovat školení o bezpečnostních protokolech, rozpoznávání potenciálních hrozeb a správné reakci na incidenty

10.4 Standardy a nejlepší praxe (best practices)

Význam mezinárodních standardů a nejlepších praktik pro ochranu 5G sítí a infrastruktur postavených na principu Open RAN před distribuovanými útoky odepření služby (DDoS) postupně roste. Tyto standardy a praktiky jsou zásadní pro vytvoření spolehlivého, bezpečného a odolného telekomunikačního ekosystému zejména z pohledu společného uplatňování a společného jazyka.

10.4.1 Mezinárodní standardy a bezpečnostní doporučení

V rámci 5G sítí a Open RAN se před DDoS se dají standardy a doporučení jednoduše jako preventivní prvek před implementací a v průběhu bezpečnostní správy. V této oblasti působí organizace nebo uskupení jakými jsou:

- 3GPP (3rd Generation Partnership Project): Tato organizace vytváří standardy, které pokrývají celou šíři mobilních telekomunikací, včetně 5G. 3GPP specifikace adresují různé aspekty bezpečnosti sítě, od zabezpečení rádiového přenosu po bezpečnostní architekturu sítě. Pro ochranu před DDoS útoky, 3GPP standardy zahrnují mechanismy pro identifikaci a autentizaci uživatelů a zařízení, šifrování dat a integritu signalizace.

- ITU (International Telecommunication Union): ITU, agentura OSN pro informační a komunikační technologie, publikuje standardy známé jako ITU-T doporučení. Tyto dokumenty se věnují širokému spektru ICT témat, včetně bezpečnostních aspektů telekomunikačních sítí. ITU-T X.série doporučení pokrývají kybernetickou bezpečnost a ochranu osobních údajů, což je relevantní pro obranu proti DDoS útokům.

- GSMA (Global System for Mobile Communications Association): GSMA, asociace zastupující zájmy mobilních operátorů po celém světě, vyvíjí pokyny a best-practice dokumenty, které pomáhají členům implementovat bezpečnostní opatření v souladu s nejnovějšími standardy a technologiemi. To zahrnuje bezpečnostní pokyny pro 5G sítě a doporučení pro ochranu proti DDoS a jiným kybernetickým hrozbám.

Z pohledu výstupů ze standardů a bezpečnostních doporučení, i když se jedná o písemný projev, který musí být transformován do konkrétní realizace, pokrývají zásadní oblasti ochrany proti DDos útokům tato dílčí doporučení:

- Sdílení informací o hrozbách: Efektivní obrana proti DDoS útokům vyžaduje aktuální informace o potenciálních hrozbách a útočných metodách. Organizace by měly podporovat sdílení těchto informací mezi sebou a s vládními bezpečnostními agenturami.

- Pravidelné bezpečnostní audity a testování: Pro identifikaci slabých míst v síťové infrastruktuře a ověření účinnosti implementovaných bezpečnostních opatření je nezbytné pravidelně provádět bezpečnostní audity a penetrační testování.

- Implementace robustních bezpečnostních protokolů: Zabezpečení komunikace mezi různými komponentami sítě a ochrana proti neautorizovanému přístupu je klíčová. To zahrnuje využití silného šifrování, autentizace a integritní kontroly.

- Odpovídající reakční plány na incidenty: Vytvoření a udržování aktuálních plánů pro reakci na bezpečnostní incidenty, včetně DDoS útoků, je zásadní pro rychlou a efektivní reakci. Tyto plány by měly zahrnovat postupy pro izolaci útoků, komunikaci s relevantními stranami a obnovu služeb.

- Vzdělávání a osvěta: Udržování vysoké úrovně povědomí o bezpečnosti mezi zaměstnanci a zákazníky pomáhá snižovat rizika spojená s kybernetickými hrozbami. To zahrnuje školení o bezpečnostních praktikách, rozpoznávání phishingových pokusů a bezpečném zacházení s daty.

10.5 Testování a validace

Testování a validaci schopnosti 5G sítí a infrastruktur Open RAN odolávat distribuovaným útokům odepření služby (DDoS) slouží pro identifikaci potenciálních slabých míst v síti a ověření účinnosti implementovaných bezpečnostních opatření.

Prvním krokem je vypracování detailního plánu testování, který zahrnuje cíle, rozsah, metodiky, použité nástroje a kritéria úspěchu. Je důležité zvolit přístup, který pokryje všechny klíčové aspekty sítě a zabezpečení, včetně rádiového přístupu, jádra sítě, aplikací a služeb.

Následně se použijí specializované nástroje a frameworky pro generování DDoS útoků tak, aby byly simulovány různé typy útoků (např. volumetrické, protokolové, aplikativní) a testuje se, jak síť reaguje a odolává těmto útokům.

Analýza dat získaných během testů vyžaduje pokročilé nástroje schopné zpracovat velké objemy informací a identifikovat anomálie. Tyto nástroje mohou využívat AI a ML pro detekci nových nebo neobvyklých vzorců útoků.

Důležitým výstupem testování je posouzení výkonnosti sítě pod zátěží a schopnost systému udržet služby dostupné během útoku. Hodnotí se také čas reakce na útok a efektivita automatických i manuálních opatření pro mitigaci útoků.

Závěry a doporučení získané během testovacích a validačních činností by měly být dokumentovány (klíčová rizika, navrhovaná zlepšení a plány pro implementaci nápravných opatření) a sdíleny s relevantními týmy a vedením.

Ještě poznámka závěrem, tak jako kybernetické hrozby se neustále vyvíjejí, testování a validace musí být kontinuální proces, zejména v části revize testovacích scénářů a bezpečnostních opatření. Musí potvrdit v každém okamžiku vysokou účinnost i proti novým sofistikovanějším hrozbám. Zároveň testování by nemělo být zaměřeno pouze na technické aspekty, ale mělo by zahrnovat i procesy, politiky a lidský faktor.

11 Návrh způsobu zajištění dostupnosti 5G sítí i při jejím vysokém zatížení

Zajištění dostupnosti 5G sítí i při jejich vysokém zatížení je klíčovou výzvou pro operátory a technologické společnosti a tuto úlohu plní jak **pokročilé technologie pro správu sítě, tak technologie network slicingu, cloud a edge computing**, rozšiřování kapacit a sdílení zdrojů, či samotná a stále aplikovaná optimalizace a aktualizace softwaru.

11.1 Pokročilé technologie pro správu sítě

Pokročilé technologie pro správu sítě hrají klíčovou roli v zajištění dostupnosti a efektivity 5G sítí, zejména v dobách jejich vysokého zatížení. Tyto technologie zahrnují řadu metod a nástrojů, které umožňují operátorům lépe monitorovat, analyzovat a spravovat sítě.

11.1.1 Prediktivní analýza a machine learning

Prediktivní analýza využívá historická data o využití sítě k předvídání budoucího zatížení a potenciálních problémů. Operátoři pak přizpůsobují alokaci zdrojů a kapacity dříve, než dojde k problémům.

Machine learning a umělá inteligence mohou automaticky analyzovat obrovské objemy dat v reálném čase a identifikovat vzorce, které by mohly naznačovat vznik problémů nebo šanci pro optimalizaci výkonu sítě.

11.1.2 Automatizace správy sítě

Automatizované nástroje pro správu sítě mohou automaticky implementovat změny konfigurace, aktualizace softwaru a optimalizace sítě bez nutnosti manuálního zásahu, což zvyšuje efektivitu a snižuje možnost lidských chyb.

Self-organizing networks (SON) jsou schopny samy se optimalizovat, konfigurovat a léčit. Automaticky se koriguje vysílací výkon a kapacity na základě aktuálních potřeb uživatelů a síťových podmínek

11.1.3 Dynamické alokování zdrojů

Flexibilní alokace zdrojů umožňuje sítím dynamicky přerozdělovat kapacitu a zdroje podle aktuálního zatížení a potřeb uživatelů. To pomáhá zajišťovat, že kritické služby mají vždy prioritu a s ní spojenou dostatečnou kapacitu a že celkové využití sítě je co nejefektivnější.

11.1.4 Pokročilý monitoring a diagnostika

Systémy pro pokročilý monitoring shromažďují a analyzují data o výkonu, zatížení, kvalitě služeb a bezpečnosti sítě v reálném čase, což umožňuje rychlé odhalení a řešení problémů.

Diagnostické nástroje mohou identifikovat příčiny problémů, od výpadků služeb po zpomalení sítě, a pomoci při rychlé obnově normálního stavu.

Implementací těchto pokročilých technologií a přístupů mohou operátoři nejen zlepšit dostupnost a spolehlivost 5G sítí, ale také zvýšit celkovou spokojenost uživatelů díky lepší kvalitě a konzistenci služeb.

11.2 Využití technologie Network slicing

Jak již bylo několikrát popsáno, **network slicing** umožňuje operátorům vytvářet několik virtuálních sítí slices na téže fyzické infrastruktuře. Každá z těchto virtuálních sítí je izolovaná a může být optimalizována pro konkrétní typ služby nebo sadu

požadavků. Tato flexibilita umožňuje operátorům efektivněji řídit zdroje a poskytovat služby přizpůsobené specifickým potřebám uživatelů nebo aplikací.

11.2.1 Optimalizace pro různé typy služeb

Každý slice může být specificky konfigurován pro různé účely, jako jsou masová IoT (Internet věcí) zařízení, kritické komunikace (např. pro nouzové služby nebo autonomní vozidla), nebo vysokorychlostní mobilní internet pro koncové uživatele. Optimalizace se pak odehrává podle specifických požadavků na latenci, propustnost, spolehlivost a mobilitu.

11.2.2 Efektivní využití zdrojů

Díky izolaci a specifické konfiguraci každého slice je možné efektivněji alokovat a spravovat zdroje sítě. Pak kritické aplikace mají vždy dostatečné zdroje i v časech vysokého zatížení, zatímco méně kritické služby mohou být flexibilně řízeny podle dostupných kapacit.

11.2.3 Zajištění kvality služeb (QoS) a spolehlivosti

Network slicing umožňuje operátorům definovat a dodržovat SLA (Service Level Agreements) pro různé typy služeb. Tato schopnost pracuje tak, že všechny aplikace a služby fungují s předvídatelnou kvalitou a spolehlivostí, což je zásadní pro kritické aplikace vyžadující nízkou latenci a vysokou dostupnost.

11.2.4 Rychlá reakce na měnící se požadavky

Vzhledem k dynamické povaze network slicing mohou operátoři rychle reagovat na měnící se požadavky trhu nebo na specifické události, které vyžadují okamžité zvýšení kapacity nebo zdrojů pro určité služby. To umožňuje sítím být velmi flexibilní a adaptabilní.

11.2.5 Zvýšení bezpečnosti

Izolace mezi slices znamená, že potenciální bezpečnostní hrozby s vlivem na jednu virtuální síť nemají přímý vliv na ostatní slices. Takové oddělení zvyšuje celkovou bezpečnost sítě a snižuje riziko šíření hrozeb.

11.3 Rozšíření kapacity pomocí Small Cells

Rozšíření kapacity a pokrytí 5G sítí pomocí **technologie Small Cells** podporuje zajištění dostupnosti sítě i při jejím vysokém zatížení, zejména v hustě osídlených oblastech nebo místech, kde je zvýšená poptávka po mobilních datových službách. Small Cells jsou malé, nízko výkonné vysílače, které doplňují tradiční makro buňky a umožňují operátorům poskytovat pokrytí a kapacitu v konkrétních oblastech.

11.3.1 Podpora pro vysokorychlostní přenosy dat

Small Cells umožňují uživatelům využívat vysokorychlostní internetové připojení díky blízkosti vysílače, což vede k nižší latenci a vyšším rychlostem přenosu dat.

11.3.2 Efektivnější využití spektra

Díky menšímu pokrytí každé Small Cell a jejich koncentraci v oblastech s vysokou poptávkou mohou operátoři efektivněji využívat dostupné spektrum a provozovat více současných přenosů v dané oblasti bez vzájemného rušení.

11.3.3 Flexibilní a nákladově efektivní rozšíření sítě

Instalace Small Cells je obvykle méně nákladná a méně invazivní než výstavba nových makro buněk. Mohou být umístěny na stávající infrastrukturu, jako jsou budovy, veřejné lampy nebo telefonní sloupy, což umožňuje rychlejší a flexibilnější rozšíření sítě.

11.3.4 Snížení zatížení makro buněk

Rozložením zatížení mezi makro buňky a Small Cells mohou operátoři optimalizovat celkové využití sítě. To pomáhá udržet vysokou úroveň služeb i v peakových časech tím, že se snižuje zatížení na jednotlivých makro buňkách.

Je třeba zmínit, že implementace Small Cells se potýká s řešením zejména otázek potřeby zajištění povolení pro instalaci, rušení signálu mezi buňkami a integrací s existující síťovou infrastrukturou.

11.4 Dynamic Spectrum Sharing (DSS)

Dynamic Spectrum Sharing (DSS) je inovativní technologie, která umožňuje operátorům mobilních sítí efektivně využívat stávající spektrum pro současné nasazení sítí různých generací, jako jsou 4G LTE a 5G. DSS usnadňuje přechod od 4G k 5G a umožňuje operátorům nabídnout služby 5G bez nutnosti získávat nová spektrální pásma nebo vyřazovat stávající služby 4G.

11.4.1 Flexibilní využití spektra

DSS umožňuje, aby se stejný frekvenční pás dynamicky sdílel mezi různými generacemi sítí. V závislosti na aktuální poptávce uživatelů a dostupnosti zařízení může systém v reálném čase přizpůsobovat alokaci spektra mezi 4G a 5G sítěmi.

11.4.2 Optimalizace nákladů a efektivity

Tato technologie umožňuje operátorům rychle rozšířit pokrytí 5G sítí bez nutnosti velkých počátečních investic do nového spektra nebo infrastruktury. DSS snižuje náklady na nasazení 5G sítí a zároveň maximalizuje využití stávajícího spektra.

11.4.3 Zajištění plynulého přechodu mezi generacemi sítí

S DSS mohou operátoři poskytovat služby 5G tam, kde je to možné, zatímco stále udržují a podporují existující služby 4G. To zajišťuje, že uživatelé s 4G zařízeními nebudou vyloučeni a zároveň mohou uživatelé s 5G zařízeními těžit z vyšších rychlostí a nižší latence.

11.4.4 Dynamická a efektivní správa zatížení

DSS umožňuje operátorům dynamicky řídit zatížení mezi 4G a 5G sítěmi, což je zvláště užitečné v obdobích vysokého zatížení. To zajišťuje efektivnější využití dostupných zdrojů a zlepšuje celkový výkon sítě.

11.4.5 Podpora různých scénářů využití

DSS není omezena pouze na specifické frekvenční pásy nebo geografické oblasti, což umožňuje operátorům implementovat technologii v různých prostředích a pro různé scénáře využití, od hustě osídlených městských oblastí po rozlehlé venkovské regiony.

11.5 Využití cloudových a edge computing technologií

Cloudové a edge computing technologie se jako poslední z inovativních technologií používají v 5G sítích pro zajištění dostupnosti a vysokého výkonu služeb i při vysokém zatížení. Tyto technologie pracují s decentralizací zpracování dat a aplikací, což přináší data a výpočetní zdroje blíže ke koncovým uživatelům.

11.5.1 Snížení latence

Edge computing zpracovává data přímo na okraji sítě, blízko uživatelů nebo IoT zařízení. Tím se výrazně snižuje latence, což je kritické pro aplikace, které mají prioritu v provozu v reálném čase, jako jsou autonomní vozidla, průmyslová automatizace, telemedicína a virtuální/augmentovaná realita.

11.5.2 Odlehčení centrálních cloudových serverů

Distribuce zpracování dat a úložiště mezi edge servery snižuje zatížení centrálních datových center. S tím je synergicky spojeno efektivnější využití zdrojů a pokles potřeby přenosu velkých objemů dat přes celou síť, což zvyšuje celkovou efektivitu sítě.

11.5.3 Zvýšení spolehlivosti a dostupnosti služeb

Edge computing může zvýšit spolehlivost sítě tím, že umožňuje kontinuitu služeb i v případě výpadků nebo problémů v centrálních datových centrech. Lokální zpracování dat znamená, že aplikace mohou pokračovat ve fungování i při přerušení spojení s hlavním cloudem.

11.5.4 Efektivní využití šířky pásma

Přesunutím zpracování dat blíže ke zdroji se snižuje potřeba přenosu velkých objemů dat přes sítě a uvolňuje se tak šířka pásma pro jiné aplikace a služby. To je zvláště důležité v obdobích vysokého zatížení, kdy je šířka pásma cenným zdrojem.

11.5.5 Podpora pro IoT a rozšířené aplikace

Edge computing se svými vlastnostmi je zásadní pro rozvoj Internetu věcí (IoT), kde množství dat generovaných senzory a zařízeními vyžaduje rychlé zpracování a rychlé rozhodování či interakci v reálném čase.

11.5.6 Zabezpečení a soukromí

Zpracováním dat na okraji sítě, blíže k jejich zdroji, může edge computing také zvýšit zabezpečení a ochranu soukromí tím, že citlivá data nemusí opustit lokální síť nebo geografickou oblast.

Z dosavadních zkušeností je zřejmé, že Implementace cloudových a edge computing technologií vyžaduje zejména investice do nové infrastruktury.

11.6 Optimalizace a aktualizace softwaru

Optimalizace a aktualizace softwaru sítě je známou a dlouho aplikovanou aktivitou pro zajištění vysoké dostupnosti, spolehlivosti a výkonu 5G sítí. Procesy představují pravidelné aktualizace softwarových komponent sítě, vylepšení algoritmů řízení sítě a úpravy konfigurace za účelem maximalizace efektivity a kvality služeb.

11.6.1 Zvýšení efektivity sítě

Aktualizace softwaru a optimalizace konfigurace mohou zlepšit algoritmy pro směrování dat, řízení přístupu k síti a alokaci zdrojů, což vede k efektivnějšímu využití dostupného spektra a síťových zdrojů. Výsledkem jsou rychlejší data a lepší kvalita hlasových služeb pro uživatele.

11.6.2 Zlepšení spolehlivosti a odolnosti sítě

Pravidelné aktualizace softwaru mohou odstraňovat chyby, zlepšovat bezpečnostní protokoly a zvyšovat odolnost sítě proti výpadkům a útokům. Síť tak zůstane dostupná a spolehlivá i v náročných podmínkách.

11.6.3 Podpora nových technologií a služeb

Rozvoj 5G sítí neustále přináší nové aplikace a služby, jako jsou IoT, autonomní vozidla, telemedicína a rozšířená/virtuální realita. Optimalizace a aktualizace softwaru umožňují sítím zapojit tyto nové technologie tím, že rozšiřují jejich schopnosti a zlepšují výkon.

11.6.4 Adaptace na měnící se vzorce poptávky

Dynamické upravování síťové konfigurace a kapacity podle aktuálního zatížení a vzorců poptávky může zlepšit zkušenosti uživatelů a zároveň zvýšit celkovou efektivitu sítě. Výhodou je rychlá adaptace na výkyvy v populačním růstu, případně velké události nebo katastrofy.

11.6.5 Minimalizace provozních nákladů

Efektivnější využití zdrojů a zlepšení automatizace prostřednictvím softwarových aktualizací snižuje provozní náklady organizace. Synergicky vedou SW aktualizace k redukci počtu manuálních zásahů a automatizace rutinních úloh umožňuje operátorům ušetřit čas a zdroje.

Pravidelné aktualizace a optimalizací jsou také spjaty s potřebou pečlivého plánování a testování jejich nasazení, tzn. zejména testování kompatibility nových softwarových verzí s existujícím hardwarovým a softwarovým prostředím.

11.7 Zajištění redundance a odolnosti sítě

Zajištění redundance a odolnosti sítě je představuje řadu technických a organizačních opatření, která pomáhají minimalizovat dopad potenciálních problémů a zajistit nepřetržitou dostupnost služeb.

11.7.1 Redundance hardwaru a diverzifikace cest

Fyzické nasazení více komponent hardwaru, jako jsou servery, switche, a routery, v různých částech sítě funguje tak, že v případě selhání jednoho prvku může jeho funkci okamžitě převzít jiný.

Odolnost sítě proti výpadkům zprostředkuje použití více možných cest pro data mezi kritickými body a tedy data přesměrovat v případě problémů na jedné trase.

11.7.2 Software-Defined Networking (SDN) a Network Functions Virtualization (NFV)

SDN a NFV umožňují flexibilní a dynamickou rekonfiguraci sítě prostřednictvím softwaru. Tyto technologie podporují rychlé přizpůsobení síťové infrastruktury a služeb v reálném čase, což pomáhá udržovat kontinuitu služeb i při hardwarových nebo softwarových problémech.

11.7.3 Geografická diverzifikace

Rozmístění datových center a klíčových síťových prvků v různých geografických oblastech může pomoci minimalizovat riziko výpadků způsobených lokálními negativními jevy (výpadky elektrické energie) nebo dokonce místními katastrofami.

11.7.4 Automatizované zálohování a obnova

Pravidelné zálohování konfigurací, softwaru a kritických dat zajišťuje, že v případě selhání lze systémy rychle obnovit do posledního stabilního stavu.

Automatizace procesů obnovy zvyšuje schopnost rychle reagovat na problémy a minimalizovat dobu výpadku služeb

11.7.5 Monitorování a diagnostika v reálném čase

Pokročilé monitorovací a diagnostické nástroje umožňují nepřetržité sledování stavu sítě a rychlou identifikaci a řešení problémů nedostupnosti sítě.

Také včasné zjištění a řešení problémů pomáhá předcházet rozsáhlým výpadkům.

11.7.6 Plánování proti výpadkům a katastrofám

Vytvoření a pravidelné testování plánů pro obnovu po výpadcích a katastrofách je nezbytné pro připravenost na různé scénáře, od technických selhání po přírodní katastrofy. Zaškolení personálu a pravidelné cvičení je podpůrným faktorem pro to, aby tým byl připraven rychle a efektivně reagovat na incidenty.

12 Návrh systému pro pravidelné auditování a monitorování bezpečnostních opatření v 5G sítích

Návrh systému pro **pravidelné auditování a monitorování bezpečnostních opatření** v 5G sítích je důležitým krokem pro zajištění bezpečnosti a odolnosti 5G sítí proti různým sofistikovaným hrozbám a útokům. Začíná vždy identifikací aktiv a rizik a jejich hodnocením.

12.1 Identifikace a hodnocení aktiv a rizik

Tento proces pomáhá organizacím pochopit, co musí chránit, a jaké hrozby by mohly ohrozit jejich aktiva. Odvíjí se od mapování aktiv auditorem.

12.1.1 Mapování aktiv

Mapování aktiv má za úkol katalogizovat identifikovaná aktiva, následně je zhodnotit a na závěr stanovit vlastníka každého aktiva:

- Katalogizace Aktiv: Vytvoření úplného seznamu všech komponent sítě, včetně fyzických zařízení (např. servery, switche, základnové stanice), softwaru (operační systémy, aplikace), dat (uživatelská data, konfigurační data) a služeb (připojení k internetu, cloudové služby).
- Klasifikace Aktiv: Rozdělení aktiv do kategorií na základě jejich důležitosti a citlivosti. To zahrnuje určení, která data jsou osobní, která mají finanční hodnotu, a která jsou kritická pro operace.
- Zodpovědnost za Aktiva: Přiřazení zodpovědných osob nebo týmů ke každému aktivu pro zajištění správy, bezpečnosti a aktualizací.

12.1.2 Analýza rizik

Analýza rizik je proces, který je znám z několika jiných podkladů, zde tedy uvádíme v krátkosti hlavní kroky procesu:

- Identifikace Hrozeb: Analýza potenciálních vnějších a vnitřních hrozeb pro sítě 5G, jako jsou kybernetické útoky, fyzické poškození infrastruktury, chyby v softwaru nebo ztráta dat.
- Hodnocení Zranitelností: Určení slabých míst v bezpečnosti, které by mohly být využity hrozbami. To zahrnuje zastaralý software, nedostatky v konfiguraci a slabá místa v protokolech a šifrování.
- Dopad a Pravděpodobnost: Hodnocení potenciálního dopadu každé hrozby na organizaci a pravděpodobnost jejího výskytu. To pomáhá určit, které hrozby představují největší riziko.
- Prioritizace Rizik: Na základě hodnocení dopadu a pravděpodobnosti se rizika řadí podle priority, což umožňuje organizaci zaměřit se na nejvýznamnější hrozby

12.1.3 Plán řízení rizik

Poté co jsou zřejmá a ohodnocená rizika v 5G sítích dané organizace nezbývá nic jiného než společně s jejich vlastníky a řešitel podle dané priority rozhodnout o **plánu jejich řízení. Děje se tak prostřednictvím**:

- Mitigační Strategie - Vývoj strategií pro snížení rizik, včetně technických řešení (např. zesílení zabezpečení, aktualizace a záplaty) a organizačních opatření (např. zlepšení procesů, školení zaměstnanců).
- Plánovaná Opatření - Vytvoření konkrétního plánu pro implementaci mitigace a prevence rizik, včetně časového harmonogramu a přidělení zdrojů.
- Monitorování a Revize - Pravidelné hodnocení a aktualizace analýzy rizik a plánu řízení rizik, aby se zohlednily nově vznikající hrozby a změny v síti nebo organizaci.

Identifikace a hodnocení aktiva a rizik jsou klíčové pro vytvoření efektivní strategie bezpečnosti 5G. Poskytují základ pro všechny další bezpečnostní aktivity, umožňují organizaci lépe se připravit na potenciální hrozby a zvýšit odolnost své 5G sítě

12.2 Implementace preventivních opatření

Implementace preventivních opatření se zaměřuje na předcházení bezpečnostním incidentům prostřednictvím různých technik a metod.

Používá se zejména zabezpečení koncových bodů, šifrování dat a síťová segmentace.

- Opatření zabezpečení koncových bodů:
  - Antivirus a antimalware: Instalace a pravidelná aktualizace antivirového a antimalwarového softwaru na všech koncových zařízeních v síti, aby se předešlo škodlivým útokům.
  - Správa záplat a aktualizací: Zavedení procesu pro pravidelné záplatování a aktualizaci operačních systémů a aplikací na koncových zařízeních, aby se opravily známé zranitelnosti.
  - Správa přístupu: Implementace silných politik ověřování a autorizace, včetně vícefaktorové autentizace, pro omezení přístupu k síťovým zdrojům pouze oprávněným uživatelům.
- Opatření šifrování dat:
  - Šifrování v klidu: Použití silného šifrování pro uložená data, aby byla chráněna před neoprávněným přístupem v případě ztráty nebo krádeže zařízení.
  - Šifrování v pohybu: Zajištění, že veškerá data přenášená mezi zařízeními a přes veřejné sítě jsou šifrována, což brání jejich odposlouchávání nebo manipulaci.
  - Správa klíčů: Zavedení robustního systému pro správu šifrovacích klíčů, včetně jejich bezpečného ukládání, rotace a vymazávání.
- Opatření síťové segmentace:
  - Definování segmentů: Rozdělení sítě na logické segmenty na základě funkce, úrovně citlivosti dat nebo úrovně bezpečnosti. To umožňuje lepší kontrolu přístupu a omezuje šíření útoků v síti.
  - Izolace kritických systémů: Zajištění, že kritické systémy a data jsou izolovány v bezpečných segmentech, což ztěžuje potenciálním útočníkům přístup.
  - Pravidla pro přístup mezi segmenty: Nastavení striktních pravidel pro řízení komunikace mezi segmenty, včetně firewallů a pravidel pro přenos dat, aby se minimalizovalo riziko přeshraničního šíření útoků.
- Další bezpečnostní opatření:
  - Detekce a prevence proniknutí (IDS/IPS): Implementace systémů pro detekci a prevenci proniknutí, které neustále monitorují síťový provoz a vyhledávají známé vzory útoků nebo podezřelé chování.
  - Bezpečnostní politiky a postupy: Vypracování a provádění jasně definovaných bezpečnostních politik a postupů, které pokrývají všechny aspekty zabezpečení sítě a jsou pravidelně aktualizovány.

- Fyzické zabezpečení: Zabezpečení fyzických zařízení a infrastruktury, které jsou součástí 5G sítě, proti neoprávněnému přístupu, krádeži nebo poškození.

12.3 Pravidelné auditování a monitorování

Pravidelné auditování a monitorování je sledováním síťového provozu, detekce potenciálních hrozeb a slabých míst, a provádění pravidelných kontrol pro identifikaci a řešení bezpečnostních problémů. Příklady podezřelých aktivit, které umí auditování a monitoring postihnout pro ilustraci uvádíme níže:

1. Neobvyklý síťový provoz
   - Velký objem přenosu dat: Nárůst přenosu dat na neobvyklých portech nebo mezi nezvyklými IP adresami může indikovat pokus o data exfiltraci.
   - Neobvyklý čas přenosu: Síťový provoz během neobvyklých časů (např. v noci nebo o víkendech) může být znakem pokusu o útok mimo běžnou pracovní dobu, kdy je pravděpodobné, že síť je méně monitorována.
2. . Anomální chování uživatelů
   - Neobvyklé přihlášení: Pokusy o přihlášení z geografických lokalit, ze kterých se uživatel běžně nepřihlašuje, nebo opakované neúspěšné pokusy o přihlášení mohou indikovat pokus o brute-force útok.
   - Změna vzorců používání: Uživatelské aktivity, které jsou neobvyklé ve srovnání s běžným vzorcem chování daného uživatele, mohou být znakem kompromitovaného účtu.
3. Podezřelé přístupy a modifikace
   - Neoprávněný přístup: Pokusy o přístup k systémům, aplikacím nebo datům, ke kterým uživatel běžně nemá oprávnění, mohou indikovat zneužití přístupových práv.
   - Neobvyklé změny konfigurací: Neočekávané změny konfigurací síťových zařízení, serverů nebo bezpečnostních nastavení mohou být znakem pokusu o kompromitaci systému.
4. Malware a útoky
   - Detekce malwaru: Aktivita, která odpovídá známým vzorům chování malwaru, jako je neobvyklý zápis na disk, pokusy o přístup k systémovým souborům, nebo neobvyklá komunikace s externími servery.
   - DDoS útoky: Náhlý a výrazný nárůst síťového provozu, který způsobuje zpomalení nebo nedostupnost služeb, může být znakem útoku typu Distributed Denial of Service.
5. Neznámé nebo podezřelé zařízení v síti
   - Nová zařízení: Detekce nových zařízení připojených k síti, která nebyla předem schválena nebo známá, může indikovat pokus o neautorizovaný přístup.
   - Zařízení se známými zranitelnostmi: Identifikace zařízení v síti, která obsahují známé zranitelnosti a mohou být cílem útoků.
6. Pokusy o obcházení bezpečnostních opatření
   - Změny ve firewall pravidlech: Neautorizované změny v pravidlech firewallu, které mohou umožnit nežádoucí přístup do sítě.
   - Pokusy o vypnutí bezpečnostních nástrojů: Akce zaměřené na deaktivaci nebo obcházení bezpečnostních systémů, jako jsou antiviry, IDS/IPS nebo SIEM.

Pravidelné auditování a monitorování podpírají automatizované nástroje pro sledování sítě.

12.3.1 Automatizované nástroje pro sledování sítě

Nyní si vyjmenujeme nástroje pro sledování sítě, které jsou známé a v 5G sítích upotřebitelné:

- Implementace SIEM systémů (Security Information and Event Management): Tyto systémy shromažďují a analyzují logy a události z různých zdrojů v síti v reálném čase, aby identifikovaly podezřelé aktivity nebo bezpečnostní incidenty.

- Nástroje pro detekci a prevenci proniknutí (IDS/IPS): Systémy pro detekci a prevenci proniknutí monitorují síťový provoz a vyhledávají známé vzory útoků nebo anomální chování, které by mohlo naznačovat bezpečnostní hrozbu.

- Monitorování zranitelností: Použití nástrojů pro pravidelné skenování sítě a jejích komponent za účelem identifikace nově objevených zranitelností, které by mohly být zneužity útočníky.

12.3.2 Pravidelné bezpečnostní audity

Podle zaměření auditů se bezpečnostní audity rozdělují na:

- Externí bezpečnostní auditování: Pravidelné provádění bezpečnostních auditů externími odborníky, kteří mohou poskytnout nezávislý pohled na bezpečnostní stav sítě a odhalit slabá místa, na která může být interní tým zvyklý.

- Testování proniknutí: Simulace útoků na síť za účelem testování odolnosti proti reálným hrozbám a identifikace slabých míst v bezpečnostních opatřeních.

- Revize politik a postupů: Periodická revize a aktualizace bezpečnostních politik a postupů, aby odpovídaly aktuálnímu bezpečnostnímu prostředí a hrozbám.

Výsledek hodnocení v rámci auditování a monitorování sítě vede následně k aplikaci určité úrovně aktualizací nebo záplatování, případně se stává součástí programu vzdělávání, a to doplněním dalších bezpečnostních hrozeb a učení se správným reakcím a postupům vůči nim.

- Aktualizace a záplatování může mít několik funkčních částí v kontextu 5G sítí. Jsou jimi:
    - Správa záplat: Implementace procesu pro pravidelné záplatování softwaru a firmware na všech zařízeních v síti, včetně routerů, switchů, základnových stanic a koncových bodů.
    - Aktualizace bezpečnostních nástrojů: Zajištění, že všechny bezpečnostní nástroje a systémy jsou neustále aktualizovány, aby efektivně chránily síť proti nejnovějším hrozbám.
    - Záznamy a dokumentace: Vedení podrobných záznamů o všech provedených aktualizacích a záplatách, včetně data instalace a verzí, pro usnadnění sledování a auditování.

12.4 Reakce na incidenty a obnova

Zaměření se na **reakci na incidenty a obnovu** po nich, jsou klíčové aspekty zajištění odolnosti 5G sítí proti bezpečnostním hrozbám. Tato fáze vyžaduje pečlivé plánování a přípravu, aby byla organizace schopna rychle a efektivně reagovat na bezpečnostní incidenty a minimalizovat jejich dopad.

Reakce na incidenty začíná sestavením plánu, jak na vybrané skupiny nebo konkrétní významné typy incidentů reagovat. Pro případnou obnovu po incidentu se hodí mít nastavené zálohování, které dokáže navrátit situaci navrátit do bodu před incidentem. Podpůrným faktorem reakce na incidenty je pak dostatečná a včasná komunikace. **V textu dále poskytujeme ve zkratce výčet hlavních oblastí, kudy se jednotlivé aktivity ubírají jak obecně, tak poplatně řešení v 5G sítích.**

12.4.1 Plán reakce na incidenty

- Vypracování plánu reakce na incidenty: Vytvoření detailního plánu, který popisuje postupy a kroky k provedení v případě bezpečnostního incidentu. Plán by měl obsahovat definici incidentu, komunikační strategie, role a odpovědnosti týmu pro reakci na incidenty, a postupy pro eskalaci.

- Tým pro reakci na incidenty (Incident Response Team - IRT): Sestavení specializovaného týmu, který má na starosti řízení bezpečnostních incidentů. Tým by měl mít jasné role, včetně manažerů incidentů, analytiků bezpečnosti, právních poradců a komunikačních specialistů.

- Školení a cvičení: Pravidelná školení a simulační cvičení pro tým pro reakci na incidenty, aby byli členové týmu dobře připraveni a znali své úkoly v případě skutečného incidentu.

12.4.2 Zálohování a obnova dat

- Strategie zálohování: Vytvoření a provádění strategie zálohování dat, která zahrnuje pravidelné zálohování kritických dat a systémů. Je důležité mít více kopií záloh na různých místech, včetně off-site lokací, pro zvýšení odolnosti proti fyzickým katastrofám nebo kybernetickým útokům.

- Plán obnovy po katastrofě (Disaster Recovery Plan - DRP): Vypracování plánu, který popisuje postupy pro obnovu operací a dat po bezpečnostním incidentu nebo katastrofě. Plán by měl zahrnovat prioritizaci systémů a aplikací pro obnovu a testování obnovovacích procedur.

- Testování obnovy: Pravidelné testování schopnosti organizace obnovit systémy a data z záloh. Testování pomáhá identifikovat potenciální problémy v procesu obnovy a umožňuje jejich opravu před skutečným incidentem.

12.4.3 Komunikace během incidentů

- Plán komunikace: Vypracování plánu komunikace, který specifikuje, jak a kdy komunikovat s interními a externími stranami během bezpečnostního incidentu. To zahrnuje určení, kdo má oprávnění mluvit jménem organizace a jaké informace budou sdíleny s médii, zákazníky a regulačními orgány.

- Transparentnost a důvěra: Udržování transparentnosti během řízení incidentu může pomoci zachovat důvěru zákazníků a partnerů. Je důležité komunikovat jasně a pravidelně aktualizovat všechny zúčastněné strany o vývoji situace a přijatých opatřeních.

12.4.4 Kroky po incidentu

- Analýza po incidentu: Po řešení incidentu provést důkladnou analýzu toho, co se stalo, jak bylo s incidentem zacházeno a jaké kroky byly provedeny k jeho řešení. Cílem je identifikovat slabá místa v bezpečnostních opatřeních a procesech a zjistit lekce, které lze použít pro zlepšení.

- Zpráva o incidentu: Vypracování podrobné zprávy o incidentu, včetně popisu incidentu, analýzy příčin, přehledu reakce na incident a doporučení pro budoucí zlepšení.

12.5 Školení a osvěta

Vzdělávání a osvěta pomáhají zajistit, že všichni zaměstnanci a uživatelé sítě rozumí bezpečnostním rizikům a znají nejlepší praktiky pro jejich minimalizaci.

Školení a osvěta se uplatňuje v různých skupinách uživatelů, tj. zaměstnanců, odborníků a veřejnosti. Protože zde bylo již na více místech textu zopakováno, předkládáme **představení hlavního směřování vzdělávání a osvěty jen v krátkých bodech.**

12.5.1 Vzdělávání zaměstnanců

- Pravidelné školení a workshopy: Organizace by měly poskytovat pravidelné školení o kybernetické bezpečnosti, které pokrývá aktuální hrozby, bezpečnostní politiky společnosti, a postupy pro zajištění bezpečnosti dat a sítě. Školení by mělo být přizpůsobeno různým úrovním zaměstnanců, od technického personálu až po vedení.

- Simulace kybernetických útoků a phishingových kampaní: Provedení simulovaných útoků nebo phishingových kampaní může pomoci zaměstnancům lépe pochopit, jak tyto hrozby vypadají a jak na ně reagovat, což výrazně zvyšuje jejich schopnost detekovat a zabránit skutečným útokům.

- Zapojení do bezpečnostní kultury: Vytvoření silné bezpečnostní kultury ve společnosti, kde bezpečnost je vnímána jako společná zodpovědnost, může výrazně přispět k zabezpečení 5G sítí.

12.5.2 Osvěta veřejnosti

- Informační kampaně pro uživatele: Spuštění informačních kampaní, které osvětlují uživatele o rizicích spojených s používáním 5G sítí a o tom, jak mohou chránit svá data a zařízení. Tyto kampaně by mohly zahrnovat tipy na bezpečné používání internetu, význam aktualizací softwaru a důležitost silných hesel.

- Využití sociálních médií a webových stránek: Pro šíření osvětových materiálů lze efektivně využít sociální média a webové stránky. Tím se informace dostanou k širší veřejnosti a mohou zvýšit povědomí o bezpečnostních hrozbách a o tom, jak se jim bránit.

- Partnerské programy s vzdělávacími institucemi: Spolupráce se školami, univerzitami a dalšími vzdělávacími institucemi může pomoci rozšířit osvětu o kybernetické bezpečnosti mezi mladšími generacemi. Toto může zahrnovat hostování workshopy, přednášky a soutěže v oblasti kybernetické bezpečnosti.

12.6 Spolupráce a sdílení informací

Efektivní spolupráce a otevřená výměna informací mezi různými organizacemi, vládními agenturami a průmyslovými skupinami umožňují rychleji identifikovat hrozby, reagovat na incidenty a šířit osvětu o nejlepších bezpečnostních praktikách. Spolupráce a sdílení informací je zásadní pro zlepšování bezpečnosti 5G sítí na globální úrovni. Sjednocením sil a znalostí různých aktérů lze efektivněji čelit kybernetickým hrozbám a podporovat bezpečný vývoj a využívání 5G technologií. **Spolupráce a sdílení informací se uskutečňuje na různých úrovních, jejich příklady jsou:**

- Partnerské bezpečnostní sítě: Vytváření a udržování partnerství mezi organizacemi ve stejném průmyslu nebo sektorům pro sdílení informací o hrozbách, zranitelnostech a incidentech. Tyto sítě mohou zahrnovat soukromé společnosti, neziskové organizace a vládní instituce.

- Bezpečnostní fóra a sdružení: Účast na bezpečnostních fórech a sdruženích poskytuje platformu pro výměnu poznatků a zkušeností v oblasti kybernetické bezpečnosti. Organizace mohou těžit z přístupu k široké škále zdrojů, včetně průzkumů, analýz a nástrojů pro detekci hrozeb.

- Národní a mezinárodní iniciativy: Spolupráce s národními a mezinárodními vládními agenturami na iniciativách zaměřených na zlepšení kybernetické bezpečnosti. To může zahrnovat účast na národních centrech pro kybernetickou bezpečnost, sdílení informací o hrozbách a spolupráci na vývoji bezpečnostních standardů a politik.

- Vládní programy pro sdílení informací: Zapojení do programů, které podporují sdílení informací mezi veřejným a soukromým sektorem. Tyto programy často nabízejí cenné informace o aktuálních hrozbách a pomáhají koordinovat reakci na incidenty.

- Konference a semináře: Aktivní účast na konferencích a seminářích o kybernetické bezpečnosti umožňuje odborníkům sdílet své znalosti, objevy a nejlepší praktiky s širší komunitou. Toto může zahrnovat prezentace, workshopy a panelové diskuse.

- Odborné publikace a výzkum: Přispívání do odborných časopisů, blogů a online fór může pomoci šířit povědomí o nových hrozbách, technologiích a metodách obrany. Sdílení výzkumných výsledků a case studies podporuje společné učení a inovace v oblasti bezpečnosti.

- Sdílené databáze hrozeb a zranitelností: Využití online databází a repozitářů, které poskytují informace o známých kybernetických hrozbách, zranitelnostech a jejich řešeních. Přístup k těmto informacím může organizacím pomoci rychle identifikovat a řešit potenciální slabá místa.

- Společné analytické nástroje: Použití nástrojů a platforem, které umožňují sdílení a analýzu dat o bezpečnostních incidentech v reálném čase, může zlepšit schopnost organizací reagovat na nově objevené hrozby.

13 Návrh způsobu zajištění okamžité reakce na možné bezpečnostní incidenty

Zajištění okamžité reakce na možné bezpečnostní incidenty vyžaduje dobře promyšlený plán, který zahrnuje předem definované postupy, komunikaci, nástroje a tým.

13.1 Vytvoření incident response týmu (IRT)

Vytvoření incident response týmu (IRT) zodpovědně **vyžaduje podrobnější pohled na jeho strukturu, sestavení, školení a role.**

13.1.1 Struktura týmu

Struktura týmu, který řeší bezpečnostní incidenty, musí být pokrytá klíčovými těmito rolemi, minimálně v tomto rozsahu:

- Vedoucí týmu: Zkušený leader, který má přehled o bezpečnostních postupech a dokáže efektivně řídit reakci na incidenty.
- Techničtí experti: Specializovaní IT bezpečnostní odborníci zaměření na analýzu malwaru, forenzní analýzu, systémovou a síťovou bezpečnost.
- Právníci se specializací na kybernetické právo a regulační požadavky, kteří mohou poskytnout poradenství v oblasti právních a compliance aspektů incidentů.
- Odborníci na komunikaci, kteří připravují a koordinují veškerou externí a interní komunikaci související s incidentem.
- Zástupci obchodních a operačních jednotek: Zástupci klíčových obchodních a provozních oddělení, kteří pomáhají posoudit dopad incidentu na podnikání a koordinují opatření k minimalizaci tohoto dopadu.

13.1.2 Sestavení týmu

Při výběru členů IRT je důležité hledat jedince s odpovídajícími dovednostmi, zkušenostmi a schopností práce pod tlakem.

Dále je třeba se ujistit, že tým zahrnuje odborníky z různých relevantních oblastí, aby mohl pokrýt všechny aspekty reakce na incidenty.

13.1.3 Role a odpovědnosti

Každý člen týmu by měl mít jasně definované role a odpovědnosti, které se nemohou překrývat s odpovědnostmi v jiné roli. Členovi týmu musí být známé primární úkoly během incidentu a základní principy a postupy komunikace.

13.1.4 Připravenost a dostupnost

Zajištění okamžité reakce na bezpečnostní incident není možné tam, kde členové týmu nejsou schopni reagovat na incidenty kdykoliv (může vyžadovat zavedení směn nebo pohotovostních systémů).

Procesy komunikace a eskalace musí být vždy řádně zdokumentovány pro další použití.

13.1.5 Hodnocení a zlepšování výkonu týmu

Po incidentu není zanedbatelné posouzení výkonu týmu. Efektivní pro vylepšení reakční schopnosti týmu jsou při tom cvičení anebo zapojení týmu do reakce na reálné incidenty. I možnost otevřené zpětné vazby, kde členové týmu mohou sdílet nápady na vylepšení procesů a metod reakce na incidenty, vedou ke zlepšování reakce na možné bezpečnostní incidenty.

13.2 Identifikace a hodnocení incidentů

Identifikace a hodnocení incidentů podporuje účinnou reakci na bezpečnostní incidenty. Zahrnuje procesy a nástroje pro detekci incidentů, jejich kategorizaci, prioritizaci a správné řešení.

13.2.1 Detekce incidentů

Implementací a pravidelnou aktualizací sofistikovaných nástrojů pro monitorování a detekci, jako jsou systémy pro detekci a prevenci průniku (IDS/IPS), systémy pro správu bezpečnostních informací a událostí (SIEM), antivirové programy a nástroje pro analýzu provozu, získá proces okamžité informace pro reakci na možné incidenty.

Další technikou, která významně ovlivňuje systém detekce incidentů je logování a auditování. Systémy, které uchovávají podrobné logy, mohou být dále použity pro identifikaci a analýzu incidentů.

Detekce incidentů funguje mnohem lépe, pokud nastavená komunikace podporuje kulturu bezpečnosti mezi zaměstnanci a má vytvořený jednoduchý proces pro hlášení podezřelé činnosti nebo bezpečnostních incidentů.

13.2.2 Hodnocení incidentů

Hodnocení incidentů se uskutečňuje prostřednictvím na sebe navazujících kroků. Začíná jejich klasifikací a prioritizací, následně je incident podroben analýze a poté je předán na relevantní řešitele, případně jsou obeznámeni účastníci incidentu a jiné zájmové skupiny. Náležitosti jednotlivých úloh jsou shrnuty:

- Klasifikace a prioritizace: Vytvořte systém pro klasifikaci incidentů podle jejich závažnosti a potenciálního dopadu na organizaci. Tento systém by měl umožnit rychlou prioritizaci incidentů, aby byly nejdříve řešeny ty nejzávažnější.

- První analýza: Po detekci incidentu proveďte rychlou první analýzu, abyste získali představu o rozsahu, typu útoku, zasažených systémech a potenciálním dopadu.

- Proces eskalace: Zavedení jasných pravidel pro eskalaci incidentů zajistí, že informace o incidentech dosáhnou správných lidí včetně IRT, managementu a případně externích odborníků pro rychlou a efektivní reakci.

13.2.3 Komunikace v průběhu incidentu

Předem připravené komunikační protokoly urychlují řešení incidentu. Určují, kdo, kdy a jak bude informován o incidentu, včetně interních týmů, vedení společnosti a případně i externích stran.

Komunikace do okamžiku vyřešení incidentu, je kontinuální proces, vyžaduje průběžné informace o stavu řešení incidentu pro všechny zainteresované strany tak, aby byly informovány o pokroku a přijímaných opatřeních.

13.2.4 Dokumentace a záznamy

Dokumentace a záznamy o incidentu napomáhají efektivnímu způsobu zajištění okamžité reakce na možný incident. Je ji potřeba evidovat minimálně na úrovni záznamu všech detekovaných incidentů, včetně popisu incidentu, reakce, zjištěných skutečností, přijatých opatření a výsledků analýz. Dokumentace incidentů je zásadní pro pochopení hrozeb, lekce získané a zlepšení bezpečnostních postupů.

Po řešení každého incidentu se doporučuje provést důkladnou analýzu, aby byly identifikovány hlavní příčiny vzniku incidentu, vyhodnotil se celkový výkon týmu a byla navržena potřebná zlepšení v procesech a bezpečnostních opatřeních.

13.3 Komunikační plán

I když bývá tato kapitola umisťována na závěr, pro správu incidentů je **komunikační plán** zásadním nástrojem při jejich rychlém řešení. Komunikační plán zajišťuje, že všechny zúčastněné strany jsou známy a kontaktovány s požadavkem na řešení a jsou informovány o situaci a podniknutých opatřeních. Dobře promyšlený komunikační plán pomáhá zachovat důvěru a minimalizovat poškození pověsti organizace.

Plánování komunikace obsahuje části jako je vytvoření komunikačních protokolů, stanovení komunikačních kanálů, určení týmu a dalšímu zlepšování slouží pak testování případně přezkum komunikačního plánu. Následuje bodové shrnutí relevantních úkolů těchto částí:

13.3.1 Vytvoření komunikačních protokolů

1. Předdefinované šablony: Spočívá ve vypracování šablon pro komunikaci v různých situacích, které mohou být rychle přizpůsobeny konkrétním incidentům. Šablony by měly zahrnovat interní oznámení, oznámení pro zákazníky, tiskové zprávy a FAQ pro rychlé odpovědi na otázky.

2. Identifikace klíčových zpráv: Určením klíčové zprávy, kterou je potřeba sdělit pro různé typy incidentů se ušetří čas, Klíčová zpráva obsahuje informace o tom, co bylo postiženo, jaké kroky byly podniknuty a jaké další kroky plánujete.

13.3.2 Stanovení komunikačních kanálů

3. Interní komunikace: Pokud budou dopředu zvoleny vhodné kanály pro interní komunikaci, jako jsou e-maily, intranet, SMS, týmové chatovací platformy nebo speciální zasedací místnosti, budou všichni zaměstnanci zvyklí na tuto komunikaci reagovat a reagovat včas.

4. Externí komunikace: Vymezením, jaké kanály budou použity pro komunikaci s externími stranami, včetně tiskových konferencí, sociálních médií, webových stránek a přímé komunikace s postiženými zákazníky nebo partnery, předchází organizace reputačnímu riziku.

13.3.3 Určení týmu pro komunikaci

5. Rozdělení rolí: Je třeba stanovit, kdo bude mít na starosti komunikaci v průběhu incidentu. Roli může zastávat tiskový mluvčí, tým pro sociální média, kontaktní osoby pro zákazníky a techničtí experti pro podrobnější informace.

6. Školení týmu: Komunikační tým musí být dobře školen v krizové komunikaci a rozumět technickými informacím pro různé typy incidentů.

7. Konzultace s právními poradci: Před zveřejněním jakýchkoli informací musí existovat ujištění, že komunikace je v souladu s právními a regulačními požadavky, včetně ochrany osobních údajů a obchodních tajemství.

13.3.4 Plánování komunikace

8. Pravidelné aktualizace: Plán obsahuje termíny a určení v jakých fázích incidentu budou poskytovány aktualizace napříč všemi kanály.

9. Odpovědi na otázky: Otázky od zaměstnanců, zákazníků, médií a veřejnosti musí být zodpovězeny včas, proto nelze podceňovat přípravu a případné schválení nejčastějších odpovědí zodpovědnými osobami.

13.3.5 Testování a přezkum komunikačního plánu

10. Simulace a cvičení: Pravidelné testování komunikačního plánu prostřednictvím simulací a cvičení usnadní zjistit jeho slabiny a zajistí, že všechny zúčastněné strany jsou připraveny rychle a efektivně komunikovat v reálných situacích.

11. Zpětná vazba a aktualizace: Sběr zpětné vazbu po cvičeních i skutečných incidentech slouží k průběžnému vylepšování komunikačních protokolů a postupů.

13.4 Reakce a zmírnění dopadu bezpečnostního incidentu

Po identifikace a hodnocení incidentů musí nastat **reakce ke zmírnění dopadu bezpečnostního incidentů**. Představuje konkrétní akci podniknutou k řešení bezpečnostního incidentu. Začíná izolací hrozby, pokračuje hlubší analýzou incidentu, která vede k odstranění hrozby a obnovení postižených systémů.

13.4.1 Izolace a omezení škod

V prvním kroku se řešitelé incidentu maximálně snaží odstínit ostatní části sítě od incidentu za účelem minimalizace škod a shromáždit důkazy o historii před incidentem i během jeho průběhu:

- Izolace postižených systémů: Postižené systémy je potřeba izolovat od zbytku sítě, aby se zabránilo dalšímu šíření hrozby. Děje se tak např. odpojením od internetu a vypnutím zařízení.

- Zajištění důkazů: Před zahájením procesu čištění se doporučuje zdokumentovat stav systému, zejména pak shromáždit všechny relevantní logy a důkazy pro forenzní analýzu a právní účely.

13.4.2 Analýza incidentu

Po odstínění zásadních vlivů incidentů pokračuje tým analýzou incidentu. Zaměří se na:

- Identifikaci zdroje a metody útoku s využitím informací a forenzních nástrojů k určení, jak byl útok proveden a které zranitelnosti byly využity.

- Odhad dopadu, tzn. stanoví se rozsah dopadu incidentu na data, systémy a operace organizace, včetně zjištění, jaká data byla ovlivněna nebo ztracena.

13.4.3 Odstranění hrozby a obnova

S informací z analýzy incidentu začíná práce na odstranění hrozby, resp. činnosti, které mají za cíl komplexně napravit stav a navrátit data, systémy a operace do bezvadného stavu a vrátit síť do provozu. Uskuteční se to prostřednictvím:

- Odstranění malwaru a záplatováním: Provede se důkladné čištění postižených systémů, včetně odstranění všech stop malwaru a nasazením nejnovějších bezpečnostních záplat na zranitelné software.

- Obnovení záloh: Pokud byla data poškozena nebo ztracena, použijí se nedávné zálohy k obnovení systémů a dat do stavu před incidentem a zkontroluje se jejich náběh.

- Postupná obnova: Obnoví se provoz postižených systémů a zajistí se kontrolované a postupné standardní chování systémů, aby bylo zajištěno, že nejsou opomenuty žádné skryté hrozby.

- Ověření integrity systémů a dat: Před plným obnovením provozu se musí ověřit, že systémy jsou čisté od jakéhokoli malwaru a data nebyla kompromitována.

13.4.4 Komunikace během reakce

Tým pravidelně poskytuje informace dalším interním týmům, vedení a případně postiženým stranám o stavu reakce a obnovy. Snaží se řídit komunikaci transparentním způsobem, aby byla zachována důvěra zákazníků a partnerů v organizaci.

13.4.5 Revize bezpečnostních postupů

Další části se věnují návazným krokům po obnově systémů a dat. Jsou jimi provedení důkladné analýzy, co se stalo, proč k incidentu došlo a aktualizace bezpečnostních opatření. To představuje výsledky analýzy promítnout do úpravy bezpečnostních politik, postupů a případně jiného nastavení nástrojů, aby byla zvýšena odolnost organizace proti budoucím hrozbám.

13.4.6 Testování a školení

Preventivně působí a zmírňují dopady bezpečnostních incidentů zejména dvě aktivity, a to testování obnovení a reakce a školení zaměstnanců. Pravidelně testy plánů obnovy po havárii a reakce na incidenty vedou k ujištění, že postupy jsou efektivní a že personál je řádně připraven. Školení zaměstnanců o bezpečnostních hrozbách a správných postupech slouží k minimalizaci rizik a efektivní reakci na incidenty.

13.5 Analýza a zotavení

Analýza a zotavení po incidentu, je závěrečnou fází procesu reakce na bezpečnostní incidenty. Tato fáze cílí na podrobné vyhodnocení incidentu, zjištění jeho příčin, obnovu normálního provozu a implementaci opatření k zabránění budoucím incidentům.

13.5.1 Podrobná analýza a zpráva incidentu

Nyní má tým prostor a zdroje k podrobnějšímu zkoumání incidentu a novému zvážení, zda v rámci řešení incidentu nebyly některé jeho parametry přehlédnuty. Napomáhá tomu:

- Forenzní analýza: Forenzní analýza umožní porozumění do hloubky tomu, jak k incidentu došlo, které systémy byly ovlivněny, a způsobu útoku. Analýza pomáhá identifikovat slabá místa a příčiny incidentu.

- Shrnutí událostí: Jedná se o záznam nastalých událostí chronologicky a reakcí týmů, které se během incidentu odehrály.

- Dokumentace zjištění: Tým sestaví podrobnou zprávu o incidentu, včetně popisu incidentu, analýzy, odezvy, dopadu na organizaci a doporučení pro budoucí prevenci.

- Sdílení s klíčovými stakeholdery (vedením společnosti, bezpečnostními týmy a případně i externími regulátory nebo zúčastněnými stranami) napomáhá informovanosti uvnitř organizace a prohlubuje důvěru v organizaci.

13.5.2 Zlepšení bezpečnostních opatření

Organizace by po každém kritickém bezpečnostním incidentu měla zvážit zvýšení odolnosti systémů. Lze ji zajistit posílením ochrany kritických systémů a dat pomocí lepších bezpečnostních nástrojů, šifrování a autentizačních procesů.

13.5.3 Revize a testování plánů reakce na incidenty

Poslední úkoly, které zlepší budoucí okamžitou reakci na bezpečnostní incident se dotýkají revize plánů reakce a aktualizaci pravidelných školení a cvičení. Konkrétněji:

- Revize plánů reakce: Na základě zkušeností a lekcí získaných z incidentu se reviduje a aktualizují plány reakce na incidenty a procesy obnovy po havárii.

- Pravidelná školení a cvičení: Organizace pravidelných školení a simulační cvičení pro zaměstnance a reakční týmy vede k udržování postupů a plánů aktuálními.

13.5.4 Zpětná vazba a kontinuální zlepšování

Z pohledu analýzy a zotavení se po bezpečnostním incidentu nás ještě čeká poslední krok a tím je práce na zpětné vazbě a další zlepšování. Pravidelné vyhodnocování efektivitu implementovaných bezpečnostních opatření, jejich úprava a podpora prostředí, ve kterém mohou zaměstnanci a management poskytovat zpětnou vazbu na bezpečnostní postupy a reakci na incidenty jsou těmi úlohami, které zamezují stagnaci v procesu obrany proti bezpečnostním incidentům.

13.6 Zlepšování a prevence

Již dříve jsme uváděli, jak aktualizace a úpravy bezpečnostních opatření a další návazné činnosti bezprostředně po zotavení se z incidentu působí **na zlepšování reakcí a prevenci vzniku dalších bezpečnostních incidentů**. Abychom se neopakovali, dovolíme si pozastavit si vyzdvihnout 3 aktivity, které musí mít podporu vedení organizace a které internímu týmu poskytují ujištění, že bezpečnostní hrozby nejsou v organizací na druhé koleji a činnost týmu je vnímána jako důležitá. Jsou investice do bezpečnostních technologií/zdrojů, spolupráce a sdílení informací, v neposlední řadě pak realizace pravidelných bezpečnostních auditů

Organizace by měla posilovat technologicky, tzn. investovat do nejnovějších bezpečnostních technologií a nástrojů, jako jsou pokročilé systémy pro detekci a prevenci průniku, šifrování dat a multi-faktorová autentizace. Bezpečnostní systémy a opatření musí organizace rozvíjet s dostatečnými zdroji, tzn. vlastnit a alokovat dostatečné finanční a lidské zdroje pro podporu bezpečnostních iniciativ a reakčních aktivit.

Účast v komunitách a zapojení se do partnerství pro sdílení informací o kybernetických hrozbách dokáže pomoci organizaci včas identifikovat a reagovat na nové hrozby.

13.7 Dodržování právních a regulačních předpisů

Posledním prvkem v systému reakce na bezpečnostní incident, který si nyní detailněji rozvedeme, **je řízené dodržování právních a regulačních předpisů**. Všechny kroky podniknuté před, během a po incidentu musí být v souladu s příslušnými právními a regulačními požadavky, což na jednu stranu představuje kroky ochrany osobních údajů, obchodních tajemství a dalších citlivých informací, stejně jako dodržování specifických průmyslových a národních bezpečnostních standardů, na druhou stranu prezentují organizaci v lepším světle přinejmenším jako důvěryhodnou a spolehlivou.

Tím, že organizace proaktivně začleňuje právní požadavky do svých plánů a postupů, minimalizuje právní rizika a zlepšuje schopnost organizace chránit citlivé informace a udržovat důvěru zúčastněných stran.

13.7.1 Porozumění platným předpisům

Porozumění platným předpisům je klíčovou prerekvizitou jejich dodržování. Identifikace pouze relevantních a průběžný monitoring zajistí, že organizace zná svoje právní hranice pro prezentaci navenek:

- Identifikace relevantních předpisů, tedy zjištění, které právní a regulační požadavky se vztahují k organizaci, včetně GDPR a dalších specifických průmyslových standardů.

- Průběžné monitorování změn je sledováním změn v právních a regulačních požadavcích, které by mohly ovlivnit postupy organizace při reakci na incidenty.

13.7.2 Začlenění právních požadavků do reakčních plánů

Platné předpisy musí být tyto inkorpovány do patřičných dokumentů jako organizace uvnitř, tak do písemných závazků s třetími stranami. Bezpečnostní politiky a postupy reakce na incidenty musí navíc tedy obsahovat kroky potřebné k dodržení právních a regulačních požadavků, stejně tak smlouvy s dodavateli a partnery se neobejdou bez zapracování klauzulí o bezpečnosti dat a dodržování předpisů.

13.7.3 Odpovědnost za hlášení incidentů a zajištění ochrany

V rámci platných předpisů a zejména pak ustanovení týkajících se povinností a sankčních ujednání musí být stanovené odpovědné osoby za včasné hlášení incidentů relevantním regulačním orgánům a dotčeným stranám, jak vyžadují příslušné právní předpisy. V zájmu souladu s právními požadavky nelze opomenout vypracování strategie pro komunikaci s dotčenými stranami, včetně zákazníků a veřejnosti.

Zajištění ochrany osobních údajů s sebou nese potřebu implementace opatření k ochraně osobních údajů, jako je šifrování a politika minimální nezbytnosti při zpracování osobních údajů a nastavení procesů tak, aby odpovědné osoby poskytly adekvátní službu dle požadavků subjektů údajů, jako je přístup k údajům, oprava nebo výmaz.

13.7.4 Revize a audit

Provádění pravidelných auditů bezpečnostních a reakčních plánů podpoří více interní snahy o dodržování aktuálních právních a regulačních požadavků. Součástí prověřování bývá existence dokumentace a evidenci podrobných záznamů o bezpečnostních incidentech, reakcích a rozhodnutích. Ulehčí se tím přezkum dodržování předpisů a bude sloužit jako důkaz v případě právního šetření auditory či jinými nezávislými institucemi.

13.7.5 Školení a osvěta

Všechny zaměstnance, zejména ty, kteří se podílejí na zpracování osobních a citlivých údajů, se doporučuje pravidelně školit v oblasti právních a regulačních požadavků souvisejících s ochranou údajů a reakcí na incidenty.

14 Prověření možností ohrožení zálohování a obnovy dat v 5G sítích

Při prověřování možností ohrožení zálohování a obnovy dat v 5G sítích je důležité zaměřit se na několik klíčových aspektů, které mohou být zranitelné nebo mohou představovat bezpečnostní rizika. 5G sítě přinášejí pokročilé technologie a vysoké rychlosti přenosu dat.

14.1 Zabezpečení síťové infrastruktury

Síťová infrastruktura 5G je komplexní a rozsáhlá, provozuje nejen tradiční velké vysílací stanice, ale i velké množství malých buněk (small cells) umístěných na různých místech, jako jsou sloupy veřejného osvětlení, budovy a další struktury. Toto rozšíření zvyšuje expozici sítě potenciálním útokům.

Zabezpečení musí tuto složitost respektovat a nesmí přehlížet nebo se spoléhat, že lze vybranou úroveň bezpečnosti zajistit zastaralými prostředky anebo podceňovat zdrojů bezpečnosti alokované.

Prověření ohrožení zálohování a obnovy dat podléhá jak fyzická bezpečnosti, kybernetická bezpečnost, tak konkrétní techniky segmentace a izolace v 5G sítích.

14.1.1 Fyzická bezpečnost

Úkoly fyzické bezpečnosti spočívají v:

- Ochraně small cells a dalších zařízení: Zajištění, aby byly malé buňky a další kritická infrastruktura fyzicky chráněny před neoprávněným přístupem, vandalismem nebo sabotáží.
- Monitorování a reakce: Implementace systémů pro monitorování fyzického přístupu a rychlá reakce na jakékoliv narušení bezpečnosti.

14.1.2 Kybernetická bezpečnost

Současné cíle implementace kybernetické bezpečnosti pro zálohování a obnovu dat se zaměřují na:

- Zabezpečení síťového přenosu – tzn. použitím pokročilých technik šifrování pro ochranu dat přenášených mezi malými buňkami a jádrem sítě proti odposlechu a manipulaci.
- Ochranu před DDoS útoky – zejména implementací řešení pro rozpoznání a zmírnění distribuovaných útoků odmítnutí služby (DDoS), které by mohly zaměřit síťovou infrastrukturu a narušit její fungování.
- Aktualizaci a správu zranitelností – za účelem opravy zranitelností se nasazují pravidelně aktualizace softwaru a firmware zařízení v síti tak, aby infrastruktura je chráněna nejnovějšími bezpečnostními opravami.

14.1.3 Segmentace a izolace

Obdobně jako v procesu reakce na bezpečnostní incidenty musí být u prvků a technologií zálohování a obnovy navržena segmentace a izolace. Uskutečňuje se prostřednictvím:

- Network slicing: Využití techniky network slicingu pro izolaci různých typů provozu a služeb v rámci 5G sítě, čímž se omezuje šíření potenciálních útoků a zjednodušuje správa bezpečnosti.
- Správa přístupu a identit: Použití pokročilých systémů pro správu identit a přístupových práv k omezení přístupu k síťovým zdrojům pouze na autorizované uživatele a zařízení.

14.1.4 Detekce a reakce na incidenty

I systém zálohování a obnovy mohou být cílem útoku. Platí pro ně totéž, co pro ostatní prvky, zařízení a systémy 5G sítí, tj. musí být monitorovány a podrobeny analýze bezpečnosti a tyto částí musí být zahrnuty do plánu reakce na incidenty.

14.2 Edge computing

Edge computing v kontextu 5G sítí odkrývá důležité aspekty zálohování a obnovy dat. Implementace robustních řešení pro zálohování a obnovu dat na edge zařízeních zajišťuje, že kritická data nebudou ztracena ani v případě fyzického poškození nebo kybernetických útoků.

Edge computing přenáší zpracování dat a výpočetní úlohy blíže k místu jejich vzniku, tedy na okraj sítě, což může přinést významné výhody v podobě nižší latence a snížení zatížení centrálních datových center. Toto rozložení však zároveň představuje **specifické bezpečnostní výzvy**.

14.2.1 Rozšíření vstupních bodů a vektorů útoku

Edge servery jsou často umístěny v méně zabezpečených a obtížněji přístupných lokacích, což zvyšuje riziko fyzických útoků, krádeže nebo poškození.

Také větší počet edge zařízení znamená více bodů, které je potřeba chránit před kybernetickými útoky, včetně malwaru, ransomwaru a útoků na odmítnutí služby (DDoS).

14.2.2 Správa a konfigurace

Vzhledem k velkému množství edge zařízení je automatizace nutnou podmínkou pro efektivní správu bezpečnostních politik, aktualizací a konfigurací. Stejně tak udržení konzistentní úrovně zabezpečení napříč všemi edge zařízeními a servery je náročné, ale nezbytné pro ochranu celé sítě.

14.2.3 Autentizace a přístup

Pro edge computing v kontextu 5G sítí platí multiplikované pravidlo spolehlivé autentizace a řízených přístupů. Dá se zabezpečit:

- Robustní autentizací: Zajištění, že všechny komunikace a přístupy k edge zařízením jsou řádně autentizovány, je zásadní pro prevenci neautorizovaného přístupu.
- Správou identit: Efektivní a spolehlivá správa identit a přístupových práv pro uživatele a zařízení, která komunikují s edge servery, determinuje významnou měrou zabezpečení sítě.

14.2.4 Data a jejich ochrana

Data uložená na edge zařízeních, stejně jako data přenášená mezi edge zařízeními a centrálním datovým centrem, musí být v zájmu bezpečného přenosu vždy šifrována.

14.2.5 Monitorování a detekce

Monitoring a detekce edge zařízení musí splňovat vysoké nároky na bezpečnost, tak aby nebyla ohroženo zálohování a obnova dat. Vyžaduje použití pokročilé technologie monitorování, která dokáže kontinuálně monitorovat a analyzovat provoz na edge zařízeních, a tím pomoci včas odhalit potenciální bezpečnostní hrozby a anomálie.

Rychlá a efektivní reakce na bezpečnostní incidenty, včetně izolace postižených zařízení, je zásadní systémovým činitelem z pohledu obnovy dat v prostoru edge computingu.

14.2.6 Kompatibilita a integrace

Edge computing by měl být navržen a implementován s ohledem na integraci s existujícími bezpečnostními systémy a politikami organizace a bezpečnostní řešení musí být flexibilní a schopná adaptace na nové technologie a standardy, které edge computing přináší.

14.3 Sdílení spektra a network slicing

Na **sdílení spektra a network slicing** se pohlíží jako na dva klíčové koncepty 5G technologie, které přinášejí významné výhody v oblasti efektivity a personalizace služeb.

14.3.1 Sdílení spektra

Sdílení spektra umožňuje různým operátorům nebo službám využívat stejný kus rádiového spektra, což maximalizuje efektivitu jeho využití. Tento přístup však vyžaduje pokročilé řízení a koordinaci, aby nedocházelo ke kolizím nebo rušení mezi službami s dopadem na integritu a dostupnost komunikace.

V zájmu zálohování a obnovy je nutné implementovat sofistikované metody pro detekci a prevenci neautorizovaného využití spektra, včetně monitorování spektra a automatického řešení konfliktů.

14.3.2 Network slicing

Network slicing umožňuje vytváření virtuálně izolovaných sítí na téže fyzické infrastruktuře. Každá slice je optimalizována pro konkrétní typ služby nebo sadu požadavků, což umožňuje operátorům flexibilně a efektivně rozdělovat síťové zdroje

Zajištění striktní izolace mezi jednotlivými sítěmi je klíčové pro ochranu dat a služeb v každé slice a minimalizuje tak ohrožení zálohování a obnovy dat. Naopak jakékoli selhání v izolaci může vést k úniku dat nebo k přeshraničním útokům.

Každá slice může mít odlišné bezpečnostní a provozní požadavky, což vyžaduje komplexní systém pro správu a vynucování politik, který zvládne různorodost a dynamiku 5G prostředí.

V prostředí s mnoha slicemi je vyšší riziko cílených útoků na konkrétní služby a tedy také nároky na systémy zálohování a proces obnovy. Je nutné mít pokročilé systémy pro detekci hrozeb, které mohou identifikovat a izolovat útoky specifické pro jednotlivé slices, a zároveň minimalizovat dopad na ostatní služby.

14.3.3 Řešení a strategie

V oblasti sdílení spektra/network slicingu se s cílem předcházet a minimalizovat ohrožení záloh a obnovy dat uplatňují řešení a strategie **v níže uvedeném rozsahu**:

- Pokročilé šifrování a autentizace: Zabezpečení dat a komunikace mezi slices a uvnitř sdíleného spektra vyžaduje silné šifrování a robustní mechanismy autentizace.
- Dynamické řízení spektra: Využití pokročilých algoritmů pro dynamické řízení a alokaci spektra může pomoci minimalizovat riziko rušení a neoprávněného přístupu.
- Flexibilní politiky bezpečnosti: Vytváření a pružná správa bezpečnostních politik umožní rychle reagovat na měnící se požadavky a hrozby v dynamickém prostředí 5G sítí.
- Monitorování a analýza v reálném čase: Kontinuální monitorování a analýza provozu v reálném čase umožní rychlou detekci a řešení bezpečnostních incidentů.

Sdílení spektra a network slicingu v 5G sítích umožňují operátorům a uživatelům využívat plný potenciál 5G technologie, aniž by byli vystaveni nepřijatelným rizikům ohrožení záloh a obnovy dat.

14.4 Autentizace a šifrování

Autentizace a šifrování v kontextu 5G sítí, odhaluje zásadní oblasti, kde pokročilé metody zabezpečení hrají klíčovou roli ve zvyšování bezpečnosti a ochrany dat. 5G technologie přináší inovace, které vyžadují revizi a posílení existujících bezpečnostních protokolů, a to zejména v oblastech autentizace a šifrování.

14.4.1 Posílení autentizace

V 5G sítích je autentizace nezbytná pro ověření identit uživatelů, zařízení a síťových služeb. Pokročilé autentizační mechanismy zajišťují, že komunikace a přístup k datům jsou chráněny před neoprávněnými pokusy. **V 5G sítích se tak děje zejména prostřednictvím:**

- Vícefaktorové autentizace (MFA), tj. kombinace několika nezávislých faktorů pro zvýšení bezpečnosti při přístupu k síťovým službám.

- Unified Identity Managementu (UIM): Centralizovaná správa identit zajišťuje konzistentní a bezpečnou autentizaci napříč různými službami a aplikacemi v 5G ekosystému.

- Simulované autentizace a klíčová dohody (AKA): Protokoly pro bezpečnou autentizaci a výměnu šifrovacích klíčů mezi uživateli a sítí, které jsou odolné proti různým útokům, včetně odposlechu a spoofingu.

14.4.2 Posílení šifrování

Šifrování hraje zásadní roli v ochraně integrity a soukromí dat přenášených nebo uložených v 5G sítích. Díky pokročilým šifrovacím algoritmům mohou být informace chráněny před neoprávněným přístupem, manipulací a odposlechem. **Využívá se:**

- End-to-end šifrování (E2EE): Zajišťuje, že data jsou šifrována na zdrojovém zařízení a dešifrována pouze na cílovém zařízení, což zabraňuje odposlechu během přenosu skrze síť.

- Šifrování na úrovni síťové vrstvy: Poskytuje další úroveň ochrany pro data v přenosu, zajišťující, že veškerá data přenášená mezi zařízeními a síťovou infrastrukturou jsou chráněna.

- Dynamická správa šifrovacích klíčů: Použití protokolů pro dynamickou výměnu a obnovu šifrovacích klíčů zvyšuje bezpečnost tím, že zabraňuje dlouhodobému využití jednoho klíče, který by mohl být kompromitován.

14.4.3 Řešení a strategie

Přestože pokročilé metody autentizace a šifrování poskytují silný základ pro zabezpečení 5G sítí, musí být v zájmu ochrany záloh a obnovy dat implementovány níže uvedená řešení, či uplatňovány strategie:

- Správa klíčů a identit: Efektivní a bezpečná správa šifrovacích klíčů a identit vyžaduje robustní infrastrukturu a politiky, které mohou zvládnout velké množství zařízení v 5G sítích.

- Výkonnost vs. bezpečnost: Zajištění vysokého výkonu při zachování silného šifrování a autentizace je výzvou, zvláště v prostředích s vysokými požadavky na latenci a propustnost.

- Standardizace a kompatibilita: Rozvoj a implementace globálně akceptovaných bezpečnostních standardů je klíčový pro interoperabilitu a bezpečnost mezi různými operátory a zařízeními v globálním měřítku 5G sítí.

14.5 Rizika specifická pro výrobce

Závislosti na technologiích a zařízeních od konkrétních výrobců ve světě 5G sítí představují také velký problém ve smyslu ohrožení zálohování a obnovy dat . Jedná se o hrozby z pozice existence samotného dodavatelského řetězce, tak v důsledku různé úrovně držení standardizace a zajištění interoperability.

Rizika dodavatelského řetězce lze charakterizovat následovně:

- Závislost na omezeném počtu dodavatelů pro klíčové komponenty 5G infrastruktury zvyšuje riziko, že problémy u jednoho dodavatele, jako jsou bezpečnostní chyby nebo výpadky výroby, mohou mít vážný dopad na celou síť.

- Existuje obava, že zařízení a software od některých výrobců mohou obsahovat zadní vrátka nebo jiné zranitelnosti, které by mohly být zneužity pro špionáž, sabotáž nebo jiné škodlivé činnosti.

Z pohledu nedodržení standardizace a nezajištění interoperabilita je třeba vnímat tato rizika:

- Různí výrobci mohou implementovat standardy 5G různými způsoby, což může vést k problémům s interoperabilitou mezi zařízeními a systémy různých výrobců.

- Různé přístupy výrobců k aktualizacím softwaru a hardwaru mohou ovlivnit bezpečnost a dlouhodobou udržitelnost zařízení v síti.

14.5.1 Řešení a strategie

Rozšíření opatření, který jsou aplikována na úrovni technologie obdobně splní svůj účel v dodavatelském řetězce. Operátor 5G sítě při omezování ohrožení má možnost výběru nebo aplikace z výčtu uvedených řešení:

1. Diverzifikace dodavatelů a výrobců může snížit rizika spojená s nadměrnou závislostí na jediném dodavateli a zvýšit odolnost sítě.

2. Podpora a používání otevřených standardů a protokolů může zlepšit interoperabilitu mezi zařízeními různých výrobců a snížit závislost na proprietárních řešeních.

3. Nezávislé bezpečnostní auditování a certifikace zařízení a softwaru mohou pomoci identifikovat a odstranit potenciální zranitelnosti nebo zadní vrátka.

4. Implementace systémů pro průběžné monitorování bezpečnostního stavu zařízení a pravidelné aktualizace softwaru a firmware zařízení pro řešení známých zranitelností.

Další a ne často zmiňovanou strategií je zapojení organizace do podpory inovací a konkurenceschopnosti. Pokud organizace věnuje prostor podpoře startupů a inovací, může to mezi dodavateli vést k větší diverzifikaci a odolnosti dodavatelského řetězce. Dalším místem, kde se vyplatí sledovat situaci nebo investovat zdroje je výzkum a vývoj. Investice do výzkumu a vývoje nových technologií a bezpečnostních řešení mohou zapojit organizaci do komunity, která poskytne organizaci řešení napřed a vysoce inovativní.

14.6 Rychlost a objem dat

Rizika, spojená s rychlostí a objemem dat v 5G sítích, která mohou ovlivnit schopnost monitorování a analýzy provozu pro zajištění bezpečnosti, jsou velmi významná. Pátá generace mobilních sítí přináší bezprecedentní rychlosti a kapacity, což umožňuje podporu nových aplikací a služeb, od internetu věcí (IoT) po virtuální a rozšířenou realitu. Tyto inovace však rovněž přinášejí nové výzvy v oblasti bezpečnosti a ochrany soukromí.

14.6.1 Zvýšené objemy dat

Enormní množství dat generovaných a přenášených v 5G sítích vyžaduje pokročilé technologie pro jejich zpracování a analýzu v reálném čase, což je nezbytné pro identifikaci potenciálních bezpečnostních hrozeb.

14.6.2 Rychlost přenosu dat

Vysoké rychlosti přenosu dat mohou ztížit včasnou identifikaci a reakci na bezpečnostní hrozby, především když tradiční bezpečnostní mechanismy nemusí být dostatečně rychlé.

14.6.3 Využití umělé inteligence a strojového učení

Automatizovaná analýza dat může poskytovat výhodu s využitím AI a strojového učení pro automatizované rozpoznávání vzorů a anomálií v datech a v masivních objemech dat produkovaných v 5G sítích, ale vyžaduje pečlivé navržení a průběžné sledování těchto nástrojů.

Umělá inteligence dokáže posílit procesy s rychlými a masivními objemy dat formou implementace prediktivních bezpečnostních systémů založených na AI, které mohou předpovídat potenciální hrozby a zranitelnosti na základě analýzy trendů a chování v síti.

14.6.4 Pokročilé šifrování a bezpečnostní protokoly

Využití pokročilých šifrovacích technik a bezpečnostních protokolů, které mohou efektivně pracovat i v prostředí s vysokými rychlostmi dat a velkými objemy, je klíčové v eliminaci ohrožení dat. .

14.6.5 Distribuované bezpečnostní architektury

Implementace NFV a SDN může poskytnout flexibilnější a dynamické řízení síťových zdrojů a bezpečnostních politik, což umožňuje rychlejší adaptaci na měnící se situace spojené s přenosy dat a jejich ohrožením. Také zpracování dat blíže k jejich zdroji může snížit latenci a zatížení centrálních systémů, a z pohledu ohrožení zálohování a obnovy dat vytváří prostor k cílenému použití edge computingu (v místě vzniku dat).

14.6.6 Aktualizace

A na závěr, zajištění, že všechny systémy a aplikace jsou pravidelně aktualizovány, přispívá do celého systému řízení bezpečnost a reakci na incidenty, přičemž významnou měrou eliminuje ohrožení samotných dat či jejich zálohování nebo obnovy.

15 Přehled podpory Open RAN a Open Core v jiných technologicky vyspělých zemích

U problematiky využívání zařízení Open RAN a Open Core v technologicky vyspělých zemích je důležité nejprve pochopit základní principy a motivace tohoto směru v telekomunikacích. **Open RAN a Open Core jsou iniciativy zaměřené na zvýšení interoperability a otevřenosti v síťových architekturách, což zvyšuje jejich konkurenceschopnost, podporuje inovace a flexibilitu při budování a provozování telekomunikačních sítí.**

Přechod k architekturám Open RAN a Open Core představuje zásadní proměnu v telekomunikačním průmyslu. Tento přístup vychází z ideje, že otevřené, standardizované rozhraní a protokoly umožní telekomunikačním operátorům snadněji integrovat a využívat zařízení a služby od různých výrobců. Hlavní motivací za touto transformací je posílení konkurenceschopnosti, zvýšení efektivity vývoje a nasazení nových technologií, jako je 5G a vznik dalších budoucích sítí, a zároveň snížení závislosti na jednotlivých dodavatelích. Tím se otevírá prostor pro nové hráče na trhu, podporuje se inovace a zajišťuje se lepší adaptabilita sítí na měnící se požadavky a technologie. **Tato iniciativa rovněž přináší výzvy, včetně zajištění bezpečnosti, spolehlivosti a kompatibility v rozmanitějším a dynamickém ekosystému**. Pro zajištění úspěšné implementace těchto principů je klíčová spolupráce mezi státními institucemi, telekomunikačními operátory, výrobci zařízení a akademickým sektorem, aby se podpořily otevřené standardy, zajistila interoperabilita a adresovaly bezpečnostní rizika.

15.1 Otevřenost a interoperabilita

Otevřenost a interoperabilita v kontextu Open RAN a Open Core představují základní kameny, na nichž jsou tyto iniciativy postaveny. Tyto principy nejenže podporují technologický pokrok a inovace v telekomunikačním průmyslu, ale také přinášejí širší ekonomické a sociální přínosy.

15.1.1 Otevřenost

Otevřenost se odkazuje na používání otevřených standardů a specifikací, které jsou veřejně dostupné a podporují širokou spolupráci mezi různými subjekty v průmyslu. To umožňuje telekomunikačním operátorům a dodavatelům vyvíjet a nabízet produkty a služby, které jsou vzájemně kompatibilní, bez ohledu na to, kdo je vyrobil. Otevřenost znamená transparentnost v procesu vývoje a standardizace, což vede k větší důvěře mezi uživateli a poskytovateli.

15.1.2 Interoperabilita

Interoperabilita je schopnost různých systémů, zařízení, aplikací nebo služeb spolupracovat a efektivně si vyměňovat informace a využívat je, aniž by bylo nutné provádět zásadní změny nebo specifické adaptace. V prostředí Open RAN a Open Core to znamená, že zařízení a softwarové komponenty od různých výrobců mohou spolehlivě fungovat společně v jedné síti, což operátorům umožňuje flexibilně kombinovat a porovnávat různé technologické řešení, aby dosáhli optimálního výkonu a efektivity.

15.1.3 Motivace za otevřeností a interoperabilitou

Z výše uvedeného textu sice hlavní prvky motivace vyplývají, ale shrneme si je následovně:

- Zvýšení konkurence: Otevírání trhů pro nové dodavatele snižuje závislost na jednotlivých velkých dodavatelích a podporuje konkurenceschopnost, což vede k lepším cenám a inovativním řešením.
- Inovační potenciál: Snižuje bariéry pro vstup nových hráčů a umožňuje rychlejší adopci nových technologií, což napomáhá rychlejšímu vývoji a nasazení inovativních služeb a aplikací.

- Flexibilita a odolnost sítí: Umožňuje operátorům flexibilně upravovat a rozšiřovat své sítě podle aktuálních potřeb a poptávky, zatímco zajišťuje vysokou úroveň odolnosti a spolehlivosti.

- Globální standardizace: Podpora otevřených standardů přispívá k harmonizaci technických řešení na mezinárodní úrovni, což usnadňuje globální spolupráci a rozvoj telekomunikační infrastruktury.

Otevřenost a interoperabilita iniciují výstavbu odolných, flexibilních a inovativních telekomunikačních sítě, připravených čelit výzvám budoucnosti s ohledem na požadovanou rychlost a objemy dat.

15.2 Flexibilita a inovace

Flexibilita a inovace jsou klíčové principy, které řídí adopci a vývoj technologií Open RAN a Open Core v telekomunikačním průmyslu. Tyto principy nejenže umožňují rychlou adaptaci na měnící se technologické a tržní požadavky, ale také podporují tvorbu a implementaci nových služeb a funkcí, které reagují na potřeby uživatelů.

V důsledku flexibility vznikají sítě s těmito vlastnostmi:

- Modulární a rozšiřitelné architektury: Open RAN a Open Core nabízejí modulární přístup k budování sítí, kde různé komponenty mohou být vyvíjeny, testovány a nasazovány nezávisle jedna na druhé. Toto umožňuje operátorům snadněji upgradovat nebo přizpůsobit své sítě novým technologiím a standardům bez nutnosti kompletního přepracování stávající infrastruktury.

- Architektury rychle adaptované na tržní změny: Flexibilní architektury usnadňují rychlé nasazení nových technologií a služeb, což operátorům umožňuje lépe reagovat na měnící se požadavky trhu a uživatelské preference.

Inovace zaručují sítě, jejichž hlavní charakteristiky lze spatřovat v:

- Podpoře pro vývoj nových služeb: Otevřené a interoperabilní platformy poskytují ideální základnu pro inovaci, umožňují vývojářům a podnikům experimentovat s novými aplikacemi a službami, jako jsou IoT (Internet věcí), edge computing, virtuální a rozšířená realita, které vyžadují vysokou propustnost, nízkou latenci a vysokou spolehlivost.

- Zvýšení konkurenční dynamiky: Přístup ke společným otevřeným standardům a rozhraním snižuje bariéry pro vstup nových hráčů na trh a podporuje větší konkurenci. To stimuluje inovace, protože firmy se snaží diferencovat své produkty a služby, aby lépe vyhovovaly potřebám zákazníků.

15.2.1 Motivace za flexibilitou a inovací

Důvody, proč flexibilita a inovace v 5G sítích, funguje jsou zejména ekonomické. Flexibilita a modularita sítí mohou výrazně snížit kapitálové a provozní náklady (CAPEX a OPEX) tím, že umožní efektivnější využití zdrojů a snadnější upgrade technologií.

S ekonomickou efektivitou souvisí schopnost rychle a efektivně nasazovat nové služby a funkce. Ta může zlepšit uživatelský zážitek a zvýšit uživatelskou spokojenost a loajalitu.

Flexibilní a inovativní infrastruktura je klíčová pro podporu budoucích technologií, jako jsou 6G a další pokročilé digitální služby, které budou vyžadovat ještě vyšší úroveň adaptability a výkonu.

15.3 Konkurence a snížení nákladů

Konkurence a snížení nákladů stojí za adopcí technologií Open RAN a Open Core a mají klíčový význam pro transformaci telekomunikačního průmyslu. Tyto principy nejenže napomáhají vytváření zdravého a dynamického tržního prostředí, ale také přinášejí významné ekonomické výhody jak pro operátory, tak pro koncové uživatele.

15.3.1 Konkurence

Open RAN a Open Core rozšiřují možnosti pro nové dodavatele, aby vstoupili na trh s telekomunikačními zařízeními a službami. To zvyšuje konkurenci mezi dodavateli a přináší další inovace, lepší kvalitu služeb a nižší ceny. Konkurence podněcuje dodavatele k vytváření unikátních a inovativních řešení, aby se odlišili od konkurence. To přináší operátorům a koncovým uživatelům širší výběr a přístup k pokročilým technologiím.

Zvýšená konkurence také přispívá k dynamice trhu a stimuluje růst a rozvoj celého sektoru, což je v zájmu všech zúčastněných stran.

15.3.2 Snížení nákladů

Díky možnosti výběru mezi širším spektrem dodavatelů a řešeními mohou operátoři optimalizovat své investice a dosáhnout vyšší efektivity při budování a provozování svých sítí.

Pokles cen zařízení a služeb redukuje jak kapitálové výdaje (CAPEX), tak provozní výdaje (OPEX) a to se promítá do celkové cenové struktury služeb pro koncové uživatele.

Flexibilita a škálovatelnost sítí také ovlivňuje jednání operátorů, umožňuje jim s jinými prostředky reagovat na měnící se poptávku a potřeby trhu bez nutnosti rozsáhlých investic do nové infrastruktury.

15.3.3 Motivace za konkurencí a snížením nákladů

Konkurence je hnací silou inovací, která napomáhá růstu a rozvoji telekomunikačního průmyslu, což přináší prospěch všem zúčastněným stranám.

Přitom snížení nákladů a větší konkurenceschopnost mohou vést k širší dostupnosti telekomunikačních služeb, což umožňuje většímu počtu uživatelů využívat pokročilé digitální technologie.

Konkurence a snížení nákladů zajistí tedy širší dostupnost a přístupnost služeb, a podporu inovačního ekosystému, který reaguje na potřeby trhu a společnosti.

15.4 Evropská unie

Evropská unie (EU) představuje významný příklad, který aktivně podporuje vývoj a adopci Open RAN a Open Core technologií jako součást širší strategie pro digitalizaci a zajištění technologické suverenity. EU klade důraz na inovace, bezpečnost, konkurenceschopnost a udržitelnost v telekomunikačním sektoru.

Evropská unie podporuje výzkum, stanovuje regulační rámec a zaměřuje se na podporu inovací a ekosystému. Příklady jednotlivých opatření a aktivit uvádíme jako výčet dále.

15.4.1 Financování a podpora výzkumu

- Programy financování: EU poskytuje významné financování pro výzkum a vývoj v oblasti telekomunikací prostřednictvím různých programů, jako je Horizont 2020 a jeho nástupce Horizont Evropa. Tyto programy podporují projekty zaměřené na inovace v Open RAN, kyberbezpečnost, cloudové výpočty a další klíčové oblasti.

- 5G Public Private Partnership (5G PPP): Toto partnerství mezi EU a telekomunikačním průmyslem podporuje výzkum, vývoj a nasazení sítí 5G, včetně projektů souvisejících s Open RAN. Cílem je posílit evropské vedení v 5G technologiích a připravit cestu pro budoucí generace sítí.

15.4.2 Regulační rámec a standardizace

- Podpora otevřených standardů: EU aktivně podporuje vývoj a adopci mezinárodních standardů, které jsou klíčové pro interoperabilitu a bezpečnost v sítích Open RAN. Opírá se o úzkou spolupráci s mezinárodními standardizačními organizacemi a podporu evropských firem v těchto procesech.

- Bezpečnostní iniciativy: Bezpečnost je pro EU klíčovou prioritou, a proto byly zavedeny iniciativy, jako je Cybersecurity Act, které stanovují rámec pro zajištění bezpečnosti sítí a informačních systémů, včetně těch založených na Open RAN.

15.4.3 Podpora inovací a ekosystému

- Inovační huby a spolupráce: EU podporuje vznik inovačních center a sítí excelence, které propojují univerzity, výzkumné instituce, start-upy a průmyslové partnery. Cílem je stimulovat vývoj a komercializaci nových technologií v oblasti Open RAN.

- Zelená agenda a udržitelnost: EU integruje principy udržitelnosti do své podpory pro telekomunikační technologie, včetně Open RAN, jako součást širšího úsilí o dosažení klimatické neutrality do roku 2050. Open RAN technologie mohou přispět k efektivnějšímu využívání energetických zdrojů a snížení emisí CO2.

15.4.4 Mezinárodní spolupráce

EU se snaží o spolupráci s mezinárodními partnery na podpoře otevřených technologií a standardů, což zahrnuje dialog a partnerství s jinými regiony a zeměmi na podporu globální interoperability a bezpečnosti telekomunikačních sítí.

Evropská unie tedy přistupuje k podpoře Open RAN a Open Core technologií komplexně, s důrazem na inovace, bezpečnost, udržitelnost a mezinárodní spolupráci. Tím EU směřuje k posílení své technologické suverenity a konkurenceschopnosti, zajištění bezpečných a udržitelných telekomunikačních sítí a podpoře ekonomického růstu a sociálního rozvoje.

15.5 Spojené státy americké

Spojené státy americké jsou dalším příkladem regionu, jak technologicky vyspělá země přistupuje k adopci a podpoře Open RAN a Open Core technologií. Tento přístup je součástí širší strategie země pro zvýšení národní bezpečnosti, posílení domácího telekomunikačního průmyslu a podporu globální konkurenceschopnosti.

Podpora v USA spočívá v posílení investičních aktivit, aktivizováním a průmyslového vývoje, jako globální leader stanovuje regulační rámec. Příklady jednotlivých opatření a aktivit uvádíme jako výčet dále.

15.5.1 Podpora na federální úrovni a investice

- Strategické financování: Americká vláda a federální agentury, jako je Federální komise pro komunikaci (FCC), uznávají význam otevřených a interoperabilních sítí pro budoucí konkurenceschopnost a bezpečnost země. Byly zavedeny programy financování a grantů zaměřené na výzkum, vývoj a nasazení Open RAN technologií.
    - Broadband Technology Opportunities Program (BTOP): Tento program, který spravuje National Telecommunications and Information Administration (NTIA), poskytuje financování pro projekty, které zlepšují přístup k širokopásmovému internetu, včetně podpory pro implementaci Open RAN technologií, které mohou zvýšit konkurenceschopnost a inovace v rozvoji sítí.
    - 5G Experimentation and Test Beds: Ministerstvo obrany USA financuje výzkum a vývoj 5G technologií, včetně Open RAN, prostřednictvím zřizování testovacích laboratoří a experimentálních prostředí, kde mohou být nové technologie testovány v bezpečných a kontrolovaných podmínkách.
    - Trusted Capital Marketplace: DoD také spolupracuje s soukromým sektorem na zajištění bezpečných a spolehlivých zdrojů kapitálu pro start-upy a firmy pracující na kritických technologiích, včetně Open RAN, což pomáhá chránit americkou technologickou infrastrukturu před cizím vlivem.
    - Future of Networks Initiative: NSF poskytuje granty pro výzkum v oblasti pokročilých sítových technologií, včetně projektů zaměřených na rozvoj Open RAN. Tyto projekty často zahrnují kolaborativní výzkum mezi univerzitami, průmyslem a vládními laboratořemi.
    - Partnerships for Innovation: Program NSF, který podporuje transformaci znalostí z akademického výzkumu do společensky prospěšných aplikací, včetně komerčního využití Open RAN technologií.

- Z důvodu obav z bezpečnostních rizik spojených s používáním zařízení od dodavatelů z určitých zemí se USA zaměřily na podporu a implementaci Open RAN jako prostředku k diverzifikaci dodavatelského řetězce a snížení závislosti na cizích technologiích.

15.5.2 Podpora inovací a průmyslového vývoje

- Inovační ekosystém: USA podporují rozvoj domácího ekosystému Open RAN, který zahrnuje start-upy, akademické instituce a stávající telekomunikační společnosti. Cílem je urychlit inovace a komercializaci nových řešení v oblasti bezdrátových sítí.

- Spolupráce s průmyslem: Americká vláda a průmyslové skupiny, jako je Open RAN Policy Coalition, pracují na podpoře politik a iniciativ, které usnadňují spolupráci mezi soukromým sektorem a státními institucemi. Tato spolupráce zahrnuje sdílení osvědčených postupů, standardizaci a vytváření společných výzkumných programů.

15.5.3 Globální lídři a standardizace

- Vedení v mezinárodní standardizaci: USA hrají aktivní roli v mezinárodních organizacích pro standardizaci, jako je 3GPP, s cílem podporovat globální přijetí otevřených standardů a technologií. Americké firmy a instituce jsou často na čele vývoje nových standardů, které umožňují interoperabilitu a zabezpečení sítí.

- Mezinárodní spolupráce: Spojené státy také vyvíjejí úsilí o spolupráci s mezinárodními partnery a spojenci, aby podpořily globální adopci a harmonizaci Open RAN standardů. To zahrnuje bilaterální a multilaterální dohody, které se zaměřují na společný výzkum, vývoj a nasazení otevřených telekomunikačních technologií.

Přístup USA k Open RAN a Open Core zahrnuje širokou škálu iniciativ od federální podpory přes inovační ekosystémy až po mezinárodní spolupráci a standardizaci. Tento přístup je zaměřen na zajištění, že otevřené telekomunikační technologie budou hrát klíčovou roli v budoucí bezpečnosti, hospodářském růstu a technologické suverenitě země.

15.6 Japonsko a Jižní Korea

Japonsko a Jižní Korea jsou předními příklady zemí, které se zavázaly k vývoji a nasazení technologií Open RAN a Open Core, což je součást jejich národních strategií pro 5G a budoucí generace telekomunikačních sítí. Tyto země přistupují k inovacím v telekomunikačním sektoru strategicky, s cílem posílit svou globální konkurenceschopnost a zabezpečení.

15.6.1 Japonsko

Podporu 5G sítí v Japonsku řídí strategické vládní iniciativy, odehrává se na úrovni spolupráce s průmyslem a na poli standardizace. Příklady jednotlivých forem podpory dále uvádíme výčtem.

- Strategické vládní iniciativy: Japonská vláda podporuje výzkum a vývoj v oblasti Open RAN prostřednictvím různých iniciativ a grantů, s cílem urychlit adopci této technologie a podpořit domácí průmysl. Jedná se o investice do pilotních projektů a demonstračních testů sítí 5G založených na Open RAN.

- Spolupráce s průmyslem: Japonsko se soustředí na podporu spolupráce mezi vládou, telekomunikačními operátory a výrobci zařízení. Významnými hráči, jako jsou NTT Docomo, Rakuten Mobile a další, jsou aktivní v nasazování a vývoji Open RAN sítí, čímž přispívají k inovaci a konkurenceschopnosti japonského telekomunikačního sektoru.

- Podpora pro domácí a mezinárodní standardizaci: Japonsko hraje aktivní roli v mezinárodních standardizačních organizacích a usiluje o podporu globální harmonizace a interoperability Open RAN technologií. Standardizace se děje formou spolupráce v rámci konsorcií a pracovních skupin zaměřených na vývoj otevřených standardů.

15.6.2 Jižní Korea

Přístup Jižní Korey k podpoře technologií Open RAN a Open Core se kromě posilování aktivit na vládní úrovni, realizuje prostřednictvím předních operátorů. Příklady jednotlivých forem iniciace rozvoje 5G sítí dále uvádíme:

- Vládní investice do 5G a budoucích technologií: Jižní Korea je známá svým rychlým nasazením sítí 5G a vláda aktivně investuje do výzkumu a vývoje technologií budoucí generace, včetně Open RAN. Tyto investice jsou součástí širší strategie pro posílení technologického vedení země.

- Přední operátoři a inovační ekosystém: Korejští operátoři, jako jsou SK Telecom, KT Corporation a LG Uplus, jsou na špici využívání Open RAN technologií pro inovaci svých sítí. Spolupracují s domácími i mezinárodními dodavateli a přispívají k rychlému rozvoji a komercializaci nových služeb a aplikací.

- Závazek ke globální spolupráci: Jižní Korea aktivně podporuje mezinárodní spolupráci a výměnu technologií, což zahrnuje účast v globálních inovačních sítích a standardizačních tělesech. Tímto způsobem se snaží podpořit globální adopci a rozvoj Open RAN jako klíčového průmyslového standardu.

Japonsko a Jižní Korea sdílejí několik klíčových prvků ve svých přístupech k Open RAN a Open Core:

- Inovační Lídři: Oba státy se zaměřují na podporu inovací a technologického vývoje ve svých telekomunikačních sektorech jako prostředek k zajištění globální konkurenceschopnosti a ekonomického růstu.

- Podpora domácího průmyslu: Existuje silný důraz na podporu domácích firem a ekosystému start-upů prostřednictvím investic, výzkumu a vývoje, což pomáhá posílit lokální průmyslovou základnu a vytvářet pracovní místa.

- Mezinárodní spolupráce a standardizace: Oba státy jsou aktivní v mezinárodních fórech a standardizačních tělesech, což podporuje globální interoperabilitu a bezpečnost Open RAN technologií.

Tímto způsobem Japonsko a Jižní Korea přispívají k rychlému rozvoji a adopci Open RAN a Open Core technologií, což napomáhá formování budoucnosti globálních telekomunikačních sítí.

15.7 Podpora výzkumu a vývoje (V&V)

Podpora výzkumu a vývoje (V&V) v oblasti Open RAN a Open Core urychluje inovace, zajištění konkurenceschopnosti a zabezpečení telekomunikačního sektoru. Pro země, které se snaží využít potenciál těchto otevřených technologií, je podpora V&V nepostradatelná.

Skrze strategické investice a spolupráci je možné urychlit vývoj a nasazení otevřených, interoperabilních a bezpečných sítí budoucnosti.

Jak povzbudit aktivity výzkumu a vývoje v oblastí Open RAN a Open Core a zajistit, aby výsledků V&V byly aplikovatelné v domácím průmyslu? Zkušenosti vyspělých ekonomik a jednotlivé kroky aplikovatelného V&V popisují další odstavce.

15.7.1 Stanovení priorit výzkumu

Výzkum bývá mnohdy nekoordinovaný a roztříštěný do dílčích úloh. Pokud má V&V směrovat k aplikovatelnému vývoji a výzkumu je zapotřebí stanovit jeho priority. Identifikovat a definovat klíčové oblasti pro výzkum a vývoj by měly vlády a regulační orgány. Vědí, které oblasti jsou kritické pro národní zájmy a průmyslový rozvoj, jako jsou kybernetická bezpečnost, škálovatelnost, energetická efektivnost a integrace s pokročilými aplikacemi (např. IoT, AI).

Klíčovým bodem stanovení priorit je zaměření se na inovace, tedy v seznamu projektů držet projekty, které se zaměřují na inovativní řešení a překonávání technických výzev v oblasti Open RAN a Open Core, s potenciálem pro komerční uplatnění a posílení konkurenceschopnosti.

15.7.2 Finanční a materiální podpora

Zdroje jsou činiteli, kteří přenášejí myšlenky do realizace. Mohou být poskytovány formou grantů, dotací či jiných forem financování pro výzkumné instituce, univerzity a průmyslové partnery.

Stojí za zmínku, že výzkumní a vývojáři pracují s vysoce kvalitními výzkumnými zařízeními a potřebují prostředí a data pro experimenty a testování nových technologií.

15.7.3 Spolupráce a partnerství

Podněcování spolupráce mezi akademickým sektorem, průmyslem a vládními agenturami (vytváření konsorcií nebo inovačních klastrů se zaměřením na specifické téma výzkum) vede ke sdílení znalostí, zdrojů a osvědčených postupů. Také podpora mezinárodních výzkumných partnerství a výměnných programů pro výzkumníky pomáhá integrovat globální perspektivy a odborné znalosti do místního výzkumu a vývoje.

15.7.4 Vzdělávání a rozvoj talentů

Posledními prvky podpory výzkumu a vývoje jsou investice do vzdělávání. Podpora vzdělávacích programů a kurzů zaměřených na výuku dovedností a znalostí potřebných pro práci s Open RAN a Open Core technologiemi, včetně nabídky stipendií a stáží pro studenty a mladé vědce, přiláká do oboru nové talenty s neotřelými přístupy a flexibilitou v přijímání nových myšlenek a výsledků výzkumu.

Rozvoj odborných dovedností a znalostí stávající pracovní síly v telekomunikačním průmyslu není nezanedbatelnou položkou v přijímání výsledků V&V, neboť připravuje zaměstnance na přechod na nové technologie a pracovní metody.

15.8 Regulační a normativní podpora

Regulační a normativní podpora hraje klíčovou roli ve zjednodušování adopce a rozvoje technologií Open RAN a Open Core. Přístup k regulaci a normám by měl být vyvážený, aby podporoval inovace, zajišťoval bezpečnost a soukromí a zároveň umožňoval flexibilitu pro rychlou adaptaci na nové technologie.

15.8.1 Stanovení transparentních regulací

Je důležité, aby regulační orgány vytvořily jasné, předvídatelné a průhledné regulační prostředí. Regulace představuje definování standardů pro interoperabilitu, bezpečnost, ochranu dat a další klíčové aspekty spojené s Open RAN a Open Core technologiemi.

Regulační orgány by měly podporovat vývoj a adopci otevřených standardů, které usnadňují interoperabilitu a zajišťují širší kompatibilitu mezi různými systémy a zařízeními.

15.8.2 Zajištění bezpečnosti a soukromí

Regulační orgány by měly spolupracovat s průmyslem a akademickými kruhy na vývoji a implementaci bezpečnostních norem a pravidel pro sítě Open RAN a Open Core, aby nebyly normy pouhou restrikcí a ztělesněním obav a nezastavovaly inovace či flexibilitu.

Je důležité rovněž zapracovat opatření, která deklarují a korigují, aby nové technologie respektovaly soukromí uživatelů a byly v souladu s právními předpisy o ochraně dat, jako je GDPR v Evropské unii.

15.8.3 Podpora inovací a experimentů

Regulační orgány by měly poskytovat mechanismy a podporovat aktivity, jako jsou dočasné testovací licence, které umožní vývojářům a operátorům experimentovat s novými technologiemi v reálných podmínkách bez plného splnění všech regulativních požadavků.

Umožnění určité míry flexibility v regulačním rámci může podporovat inovace tím, že umožní průmyslu rychleji reagovat na technologický vývoj a měnící se tržní podmínky.

15.8.4 Podpora mezinárodní spolupráce

Aktivní účast na mezinárodních fórech a ve standardizačních organizacích je klíčová pro dosažení globální harmonizace technických standardů. Snižují se tím technické bariéry v mezinárodním obchodě, který v důsledku podporuje globální interoperabilitu.

Mezinárodní spolupráce je rovněž důležitá pro sdílení osvědčených postupů, znalostí a informací o hrozbách a zranitelnostech, což posiluje celkovou odolnost telekomunikačních sítí proti kybernetickým útokům.

15.9 Spolupráce mezi stakeholdery

Spolupráce mezi různými stakeholdery vede k úspěchu a rozvoji technologií Open RAN a Open Core. Spolupráce se odehrává na mnoha úrovních a mezi různými subjekty, včetně vlád, telekomunikačních operátorů, výrobců zařízení, výzkumných institucí a akademické sféry.

15.9.1 Vytváření multisektorových partnerství

Vytváření nebo podpora průmyslových konsorcií a aliancí, které sdružují různé stakeholdery, aby se účastnili společného výzkumu, vývoje a standardizace technologií Open RAN a Open Core může podporovat sdílení znalostí, zkušeností a osvědčených postupů globálně. Vlády by měly usnadňovat tento dialog a spolupráci.

15.9.2 Podpora inovačních ekosystémů

Vznik inovačních hubů, inkubátorů a akcelerátorů vytváří prostředí pro startupy a malé a střední podniky (MSP) zaměřené na vývoj Open RAN a Open Core řešení. Nabízejí jim mentorství, přístup k síti potenciálních partnerů a zákazníků, nebo je mohou finančně či jinak materiálně podpořit.

Posílení spolupráce mezi akademickými institucemi a průmyslem pro společný výzkum a vývoj, včetně společných projektů napomáhá sdílení zařízení a uskutečňování výměnných programů pro studenty a vědecké pracovníky.

15.10 Zabezpečení a důvěra

Zabezpečení a důvěra představuje pro úspěšnou implementaci a široké přijetí technologií Open RAN a Open Core základní stavební kámen. Vzhledem k rostoucím kybernetickým hrozbám a narůstající závislosti společnosti na digitálních komunikacích je nezbytné, aby tyto technologie byly zabezpečené a důvěryhodné.

15.10.1 Integrace bezpečnosti od počátku

Zabezpečení by mělo být integrováno do všech fází vývojového cyklu produktu, od návrhu přes vývoj, testování a nasazení, až po údržbu. Tento přístup zajistí, že zabezpečení není dodatečným doplňkem, ale základní součástí produktu.

Prověření stupně bezpečnosti se realizuje prostřednictvím implementace průběžných procesů hodnocení zabezpečení a penetračního testování a pomáhá identifikovat a opravit nastavení bezpečnosti před vznikem bezpečnostního incidentu.

15.10.2 Budování důvěry a transparentnosti

Budování důvěry a transparentnosti je založeno na použití osvědčených technikách. Známkou držení transparentních podmínek mohou nést kromě referencí, platné certifikace a akreditace. Zatímco certifikační a akreditační programy pro ověření bezpečnostních vlastností a dodržování standardů posilují důvěru v produkty a řešení Open RAN a Open Core, otevřené standardy a protokoly se uplatňují více v provozu a umožňují nezávislou verifikaci a kontrolu bezpečnostních vlastností produktů. To zvyšuje důvěru uživatelů a operátorů ve využívané technologie.

15.10.3 Posílení kybernetické obranyschopnosti

Podpora platforem a iniciativ pro sdílení informací o kybernetických hrozbách a zranitelnostech mezi operátory, výrobci a vládními agenturami pomáhá vytvořit koordinovanou obranu proti kybernetickým útokům.

15.10.4 Vzdělávání a školení

Zabezpečení i důvěra nejsou bezvýznamné pro všechny zainteresované strany, včetně zaměstnanců, managementu a koncových uživatelů, Jejich vzdělává a odborná příprava zajistí, že organizace mají k dispozici nejen kvalifikované odborníky pro správu a ochranu svých sítí, ale také personál, který důvěřuje danému produktu a usiluje o jeho zlepšování.

Grant Thornton

www.grantthornton.cz