MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

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

Koordinované hodnocení rizika bezpečnosti sítí 5G v EU

(EU-wide coordinated risk assessment of 5G networks security)

Zdroj: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

Autor: Skupina pro spolupráci NIS (Složená ze zástupců Členských států, Evropské komise a Agentury Evropské unie pro bezpečnost sítí a informací (ENISA))

Dokument je hodnocení rizika nových 5G sítí. Tato nová technologie má velký potenciál, ale díky její komplexnosti vznikají nové hrozby, kterým bude muset EU při jejím zavádění a používání čelit. Dokument byl vytvořen na základě hodnocení rizik jednotlivých Členských států EU. Jedná se o první krok při celoevropském vyhodnocování bezpečnosti této nové technologie. Na jeho základě se budou vytvářet nová opatření řízení rizik v této oblasti.

Úvod

5G sítě budou hrát v blízké budoucnosti důležitou roli v transformaci evropské ekonomiky a společnosti. Kybernetická bezpečnost 5G sítí je tudíž nezbytná k plnému využití jejich potenciálu. 5G sítě nabídnou oproti současným technologiím větší rychlost, spolehlivost a možnost podpory velkého počtu zařízení najednou. Nové technologie, které umožní výhody 5G sítí, však přinesou i nové bezpečnostní výzvy, kterým bude třeba čelit.

Proto v březnu 2019 Evropská komise přijala Doporučení Komise týkající se kybernetické bezpečnosti 5G sítí (Doporučení komise 2019/534). Na jeho základě byly Členské státy požádány o hodnocení rizik. V červenci 2019 Členské státy zaslaly výsledky hodnocení rizik Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA), aby mohlo dojít k vyhodnocení hlavních aktiv, hrozeb a zranitelností. Tato zpráva je prvním krokem k dlouhodobému zabezpečení 5G sítí v EU.

Hlavními stakeholdery 5G sítí jsou:

- Mobilní operátoři provozující 5G sítě;
- Dodavatelé mobilním operátorům 5G sítí;
- Výrobci zařízení využívající 5G sítě;
- Poskytovatelé služeb používající 5G sítě;
- Koneční uživatelé 5G sítí.

V oblasti bezpečnosti sítí jsou zejména důležití mobilní operátoři a jejich dodavatelé, kteří díky větší složitosti těchto nových technologií budou hrát větší roli nejen ve vývoji a výrobě 5G infrastruktury, ale také v její údržbě.

MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

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

Hodnocení rizika

Hrozby a zdroje hrozeb

Hlavní hrozby, které Členské státy při svých hodnoceních identifikovaly, se týkají omezení nebo narušení dostupnosti, důvěryhodnosti a integrity. Nejvíce scénářů ohrožení 5G sítí se týká zejména:

- Lokální nebo globální narušení 5G sítí (Dostupnost).
- Špionáž provozu/dat v 5G síti (Důvěryhodnost).
- Modifikování nebo přesměrování provozu/dat v 5G sítí (Důvěryhodnost a integrita);
- Zničení nebo narušení ostatních sítí za pomocí 5G sítí (Dostupnost a integrita).

V blízké budoucnosti se dá čekat zvyšování závislosti na 5G sítích, větší závislost znamená větší dopady jak na ekonomiku, tak na společnost. Vážnost dopadu určitého scénáře ohrožení pak závisí hlavně na:

- Počet a typ ovlivněných uživatelů;
- Délka trvání události a doba na nápravu;
- Typ zasažené služby, rozsah poškození a ekonomické ztráty;
- Typ narušených informací.

Při hodnocení rizik Členské státy popsaly následující hrozby jako ty nejzásadnější :

- **Náhodný zdroj bez protivníka**, například lidská chyba, přírodní katastrofa nebo selhání techniky. Přírodní katastrofa může poškodit infrastrukturu a narušit dostupnost sítě.
- **Osamělý hacker** motivovaný finančním ziskem nebo touhou po slávě. Hacker může narušit komunikaci a získat tak citlivá data, která může prodat.
- Politicky motivovaná **hacktivistická skupina** například s cílem poškodit své protivníky nebo šířit svoje přesvědčení.
- **Skupina organizovaného zločinu** motivovaná finančním ziskem, může získat přihlašovací údaje koncových uživatelů do různých aplikací a vydírat jejich majitele.
- **Člověk pracující v oblasti 5G sítí**, který může být součástí zločinecké nebo hacktivistické skupiny a nebo je motivován vlastním ziskem. Tento zdroj je obzvláště nebezpečný díky praktické znalosti systému.
- **Státní skupina nebo skupina podporovaná státem** s politickými motivacemi. Tento zdroj je v současnosti nejrelevantnějším a disponuje velkou kapacitou provádět opakované sofistikované útoky na 5G sítě. V případě EU se tento zdroj s největší pravděpodobností bude nacházet mimo Unii.
- **Právnické osoby** motivované finančním ziskem. Například korporace může získat data od konkurenta a získat tak nad ním výhodu.

MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

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

Aktiva

Aktiva v 5G sítích jsou rozmanitou skupinou hmatatelné infrastruktury, komplexního softwaru, základních služeb sítě a abstraktních konfigurací pravidel sítě. Konkrétně sem mohou patřit následující aktiva:

- Vysílače a stanice, které jsou součástí rádiové přístupové sítě, které komunikují se zařízeními koncových uživatelů (například telefonem).
- Základní funkce sítě, jako například úložiště dat koncových uživatelů nebo služba registrace a autorizace.
- Přenosové vybavení jako routery nebo switche nebo filtrovací software jako firewall.
- Podpůrné funkce, jako například systémy řízení bezpečnosti.

Slabiny

Jako každá jiná digitální struktura můžou i sítě 5G trpět klasickými zranitelnostmi softwaru, hardwaru a nedostatků v bezpečnostních procesech. Počet těchto zranitelností se bezpochyby zvětší díky větší komplexnosti 5G sítí. Většina těchto nových zranitelností plyne právě z této složitosti. Následují zranitelnosti týkající se operátorů mobilních sítí a dodavatelů technologií a vybavení potřebných k provozování 5G sítí.

Zranitelnosti týkající se operátorů mobilních sítí a jejich dodavatelů:

- **Nedostatek specializovaného a vyškoleného personálu k zabezpečení, monitorování a udržování 5G sítí**. Komplexnost 5G sítí si bude žádat velké množství nových IT specialistů.
- **Nedostatek odpovídajících vnitřních bezpečnostních opatření při řízení bezpečnosti a rizik,** což bude mít za následek zvýšení rizika.
- **Nedostatek bezpečnostní a operační údržby**. 5G sítě budou vyžadovat častější aktualizace systému. Špatně udržovaný systém bude náchylnější bezpečnostním hrozbám.
- **Nedodržování standardů 3GPP** (Standardy partnerského projektu třetí generace mobilních sítí)[1] **nebo jejich nesprávná implementace.** To by opět znamenalo snížení bezpečnosti sítí.

[1] Ačkoli byl projekt vytvořen pro stanovení standardu 3G sítí pokračuje pro stanovování standardů 4G a 5G.

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

Zranitelnosti týkající se operátorů mobilních sítí:

- **Špatný design sítě a jeho architektury.** Například neefektivní nouzové a kontinuální mechanismy nebo nesprávné nastavení sítě.
- **Špatná fyzická bezpečnost sítí a IT infrastruktury**. Nedostatky mohou vést ke zvýšenému ohrožení nejen infrastruktury, ale i softwaru, dat a obsluhy.
- **Špatné zásady pro místní a vzdálený přístup k síťovým komponentům**. 5G sítě budou tvořeny z velkého množství virtuálních zařízení, ke kterým bude možno vzdáleně přistupovat v celé síti.
- **Nedostatečné bezpečnostní požadavky při zadávání zakázek**. Při zadávání zakázek mohou někteří operátoři preferovat jiné priority než bezpečnost.
- **Špatně nastavené řízení změn**. Jedná se například o hrozby spojené se změnou konfigurace sítě neautorizovaným uživatelem.

Zranitelnosti týkající se čistě dodavatelů jsou zejména spojené s dodavateli operujícími mimo EU. Ty budou fungovat pod jinými bezpečnostními standardy a nebo mohou být ovlivněny státními aktéry se škodlivými úmysly proti Unii. Zranitelnost plyne z možné závislosti na jednom nebo malém množství dodavatelů. Například pokud se značná část sítě stane závislá na určitém komponentu, který nelze nahradit substitutem.

Příklady scénářů ohrožení

Následuje několik scénářů ohrožení, které by mohly nastat:

- **Špatná konfigurace sítí:** Hacker objeví špatné nastavení sítě, které vzniklo díky nedostatku vyškoleného personálu obsluhy sítě, a díky tomu se dostane k úložišti dat konečných uživatelů, které získá a poškodí tak důvěryhodnost sítě.
- **Vybavení nízké kvality:** Operátor mobilní sítě pořídí software od dodavatele, který má zásadní bezpečnostní vady, které operátor přehlídne díky mnohem větší komplexnosti softwaru pro 5G sítě. Tato síť bude při potencionálních budoucích kybernetických útocích vysoce zranitelná.
- **Využití 5G sítě organizovaným zločinem:** Skupina získá kontrolu nad důležitou částí infrastruktury 5G sítě. Naruší službu, na které bezprostředně závisí odvětví ekonomiky a bude vyžadovat výkupné za znovuobnovení této služby.
- **Závislost kritických služeb na 5G síti:** Skupina hackerů podporovaná nepřátelským státem naruší službu sítě, na které závisí určitá oblast kritické infrastruktury. Dojde tak k oslabení funkce dané kritické infrastruktury, což zkompromituje dostupnost její funkce.

MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

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

Současná opatření

Následují opatření, která jsou v současnosti k dispozici:

- Díky Telekomunikačnímu rámci EU (Směrnice 2002/19, 2002/20, 2002/21, 2002/22 a 2002/58) může relevantní Členský stát nastavit mobilním operátorům podmínky, za kterých může poskytovat svoje služby.
- V rámci Směrnici Evropského parlamentu o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS) musí určité odvětví (jako zdravotnictví nebo energetika) provádět dodatečná bezpečnostní opatření.
- Další právní rámce v EU, zejména GDPR, mají zvýšené bezpečnostní požadavky na kritickou infrastrukturu.
- Členské státy přijímají řadu svých opatření k ochraně budoucích 5G sítí.
- Operátoři mobilních sítích také pracují na zvýšení bezpečnosti například novým šifrováním nebo systémy detekcí hrozeb.
- Některá opatření v rámci standardů 3GPP řeší částečně bezpečnostní hrozby vznikající s novými 5G systémy.

Závěr

Ačkoli nové 5G sítě přinesou spoustu výhod, vyskytnou se i nové bezpečnostní problémy převážně související s velkou komplexností těchto sítí oproti jejich předchůdcům. Díky velké složitosti budou muset operátoři těchto sítí více spoléhat na dodavatele. Tato potřeba zvýší počet vstupů pro potencionální útočníky.

Nové hrozby spojené se zaváděním těchto sítí přináší tlak na současná opatření ať už se jedná o právní rámce nebo monitorování veřejnými orgány. K tomu, aby mohl být potenciál této nové technologie plně využit, je potřeba zvážit řadu možných opatření. Některá opatření jsou už na místě alespoň částečně. Současná opatření pro 4G sítě mohou být aplikovatelné na nové sítě, ale díky velkým rozdílům mezi technologiemi stále není znám plný seznam nových hrozeb vůči 5G sítím. V potaz by se měla vzít i možnost vytvoření vlastní kapacity EU vyvíjet a vyrábět nezbytné vybavení pro 5G sítě.