DOPORUČENÍ PRO HODNOCENÍ DŮVĚRYHODNOSTI DODAVATELŮ TECHNOLOGIÍ DO 5G SÍTÍ V ČESKÉ REPUBLICE

Národní úřad pro kybernetickou a informační bezpečnost

MINISTERSTVO PRŮMYSLU A OBCHODU

Ministerstvo zahraničních věcí České republiky

Vypracováno Národním úřadem pro kybernetickou a informační bezpečnost, Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím

Obsah

Manažerské shrnutí

- Sítě páté generace (dále jen „5G sítě“) mají potenciál stát se digitální komunikační páteří naší ekonomiky a společnosti a umožnit rozvinutí a využití nových technologií do zcela nových ekosystémů.
- Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je strategickým zájmem státu i společnosti jako celku.
- Jedním ze zásadních předpokladů zajištění kybernetické bezpečnosti technologických řešení 5G sítí je bezpečnost dodavatelského řetězce. Hardware i software technologických řešení 5G sítí jsou již natolik komplexní, že snižovat rizika spojená s dodavateli 5G sítí pouze technickými prostředky je nedostatečné; zásadním faktorem je tudíž důvěryhodnost dodavatele.
- Důvěra v dodavatele musí být přítomna jak na úrovni konečné podoby dodávaného řešení, tak na strategické úrovni v rámci podnikatelského, právního a politického prostředí, ve kterém se dodavatel pohybuje.
- Účelem tohoto doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dále jen „doporučení“) je nabídnout operátorům, potažmo celému odvětví elektronických komunikací, pohled Národního úřadu pro kybernetickou a informační bezpečnost, Ministerstva průmyslu a obchodu, Ministerstva zahraničních věcí, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace a Vojenského zpravodajství (dále jen „vybrané instituce státu“) na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí a navrhnout kritéria, která mohou přispět k výběru důvěryhodných dodavatelů.

Upozornění:

Doporučení prezentuje pohled vybraných institucí státu a slouží jako podpůrné vodítko pro hodnocení některých kritérií důvěryhodnosti dodavatelů technologií do 5G sítí. Doporučení není právně závazné, má toliko doporučující povahu a nerozšiřuje, neruší ani jinak neupravuje jakákoliv práva a povinnosti stanovená obecně závaznými právními předpisy. Právo změny doporučení vyhrazeno.

Úvod

Rozvoj nových informačních a komunikačních technologií a digitální infrastruktury celkově je předpokladem pro úspěšný dlouhodobý rozvoj národních ekonomik. Budoucí mobilní sítě elektronických komunikací a zejména 5G sítě mají potenciál stát se digitální komunikační páteří naší ekonomiky a společnosti.

5G sítě zahrnují různé prvky síťové infrastruktury pro mobilní komunikační technologie, sloužící k připojení koncového účastníka nebo zařízení, přičemž nemusí být tvořeny pouze prvky nových technologií, ale zpravidla využívají i prvky předchozích generací mobilních sítí, jako jsou 4G nebo 3G sítě.

5G sítě přinášejí mimo jiné vysokou přenosovou rychlost, nízkou latenci, vysokou spolehlivost připojení a možnost připojení velkého množství zařízení, a to za využití pokročilé virtualizace, decentralizace, plátkování, tvarování vysílacích paprsků a vyšší míry sdílení datových toků. Tyto vlastnosti umožňují rozvinutí potenciálu a využití nových technologií, jako jsou různorodé autonomní systémy, umělá inteligence a strojové učení, internet věcí, kvantové výpočetní technologie a jejich integraci do zcela nových ekosystémů. Právě tento potenciál předurčuje 5G sítě k tomu, aby se staly zásadní součástí komunikační infrastruktury státu a jako k takovým je k nim třeba přistupovat jak při jejich projektování a budování, tak při jejich provozování.

Významnou součástí kybernetické bezpečnosti 5G sítí je bezpečnost dodavatelského řetězce. V případě 5G sítí je z důvodu jejich vysoké komplexity a nákladnosti typickým fenoménem na trhu těchto technologií závislost odběratele, tedy subjektu budujícího a provozujícího 5G síť, na dodavateli technologie a jeho dodavatelském řetězci. Tato závislost s sebou přináší nové kybernetické hrozby a zvyšuje riziko spojené s některými stávajícími hrozbami, a to například možností implementovat do dodávaného technologického řešení zranitelnost, která umožňuje narušení důvěrnosti, dostupnosti nebo integrity přenášených dat. Důvěra v dodavatele a jím dodávaná technologická řešení je v tomto ohledu zásadní.

Narušení kybernetické bezpečnosti 5G sítí, a to zejména jeho nejzávažnější případy, jako je narušení dostupnosti sítě ve velkém rozsahu vedoucí ke značným škodám či kybernetická špionáž, představuje podstatný problém jak pro významné ekonomické zájmy a bezpečnost státu, tak pro operátory a jejich uživatele. Vzhledem k roli, jakou budou 5G sítě v následujících letech hrát v souvislosti s rozvojem nových technologií, komunikačních ekosystémů a zvyšováním počtu připojených zařízení, by mělo naplnění výše uvedených hrozeb dalekosáhlé celospolečenské důsledky.

Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je proto strategickým zájmem státu i společnosti jako celku.

1 Zdůvodnění potřeby a cíle doporučení

Jak vyplývá z veřejně dostupných dokumentů bezpečnostních institucí České republiky[1], útoky státních aktérů na systémy kritické pro chod státu se stávají běžnou realitou, ovlivňující život a fungování mnoha obyvatel a institucí. Bezpečnost těchto systémů je ohrožena nejen kybernetickými útoky, ale i prostřednictvím dodavatelů a dodavatelských řetězců, spadajících do sféry vlivu aktérů, jejichž zájmy a mezinárodní působení jsou v konfliktu se zájmy České republiky, a dodavatelé se tak mohou se stát prostředkem k prosazování politických cílů.

V uplynulých letech bylo na evropské a globální úrovni vydáno značné množství dokumentů zabývajících se bezpečností 5G sítí, zejména pak bezpečností dodavatelského řetězce a důvěryhodností dodavatelů technologií pro 5G sítě. Určující jsou v tomto například (i) Pražské návrhy (Prague Proposals)[2], které byly přijaty na 5G bezpečnostní konferenci v Praze v roce 2019, (ii) EU 5G Toolbox[3], který byl v lednu 2020 vydán skupinou pro spolupráci (NIS Cooperation Group), sestávající ze zástupců členských států Evropské unie (dále také „EU"), Evropské komise a Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), (iii) Společné prohlášení k americko-české deklaraci o bezpečnosti sítí 5G[4] a další.[5]

Tyto dokumenty mimo jiné přímo či nepřímo popisují, jak by měly státy a operátoři přistupovat k budování 5G sítí, potažmo k výběru dodavatelů technologií, které budou k provozu 5G sítí využity, tak, aby byly tyto sítě bezpečné a odolné.

Strategické opatření č. 3 (SM03) EU 5G Toolboxu zároveň stanovuje, aby členské státy Evropské unie přijaly rámec pro hodnocení rizikového profilu relevantních dodavatelů na národní úrovni

---

[1] Viz např. výroční zprávy Bezpečnostní informační služby (BIS. Výroční zprávy [online]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/), výroční zprávy Vojenského zpravodajství (VOJENSKÉ ZPRAVODAJSTVÍ. Výroční zprávy [online]. Dostupné z: https://www.vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41) nebo Zprávy o stavu kybernetické bezpečnosti v ČR (NÚKIB. Zprávy o stavu [online]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/)

[2] Pražské návrhy [online]. Praha, 3. 5. 2019. Dostupné z: https://www.nukib.cz/download/5G_site/Prague_Proposals_CZE.pdf

[3] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures [online]. 01/2020. Dostupné z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

[4] Joint Statement on United States – Czech Republic Joint Declaration on 5G Security [online]. 7. 5. 2020. Dostupné z: https://cz.usembassy.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/

[5] Mimo to lze uvést také doporučení týkající se využívání zařízení od vysoce rizikových dodavatelů v telekomunikačních sítích Spojeného království britského Národního centra kybernetické bezpečnosti (NCSC. NCSC advice on the use of equipment from high risk vendors in UK telecoms networks [online]. 28. 1. 2020. Dostupné z: https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks), veřejný draft principů dodavatelského řetězce pro kritické technologie australského Ministerstva vnitra (Critical Technology Supply Chain Principles [online]. 2020. Dostupné z: https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-technology-supply-chain-principles-discussion-paper.pdf), nebo kritéria pro bezpečnost a důvěru v telekomunikačních sítích a službách prestižního think-tanku Center for Strategic and International Studies (CSIS. Criteria for Security and Trust in Telecommunications Networks and Services [online]. 13. 5. 2020. Dostupné z: https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services).

nebo společně s dalšími členskými státy. **Práce na vytvoření takového mechanismu prověřování na národní úrovni již probíhají**; v současné době je na základě pověření Bezpečnostní rady státu připravován věcný záměr zákona, který by v České republice tento mechanismus zavedl.

Příprava mechanismu prověřování nicméně bude, vzhledem k jeho povaze, pravděpodobně vyžadovat přijetí legislativních změn. Z důvodu (i) komplexnosti problematiky, (ii) nutnosti konzultací napříč vybranými institucemi státu, se zástupci soukromého sektoru v odvětví elektronických komunikací a s akademickou sférou (iii) a s ohledem na obvyklou délku trvání legislativního procesu přitom **nelze očekávat přijetí takovýchto legislativních změn v současném stadiu příprav budování 5G sítí.** První implementace technologií 5G sítí se objevují již v současnosti a do doby přijetí mechanismu prověřování je nezbytné, aby stát srozumitelně deklaroval národně-bezpečnostní zájmy a východiska a nabídl operátorům kritéria pro výběr důvěryhodných dodavatelů do 5G sítí alespoň v podobě doporučení.

Cílem doporučení však není navrhnout kritéria důvěryhodnosti k jednotné a plošné aplikaci na všechny dodavatele 5G sítí v České republice. Cílem je **poskytnout vodítko zejména pro dodávky do informačních a komunikačních systémů kritické infrastruktury České republiky.** Navržená kritéria jsou nicméně neutrální vzhledem k charakteru a významnosti infrastruktury a dle uvážení jednotlivých operátorů je lze vztáhnout také dodávky do strategicky méně významné infrastruktury.

Cílem doporučení také není navrhnout bez dalšího využitelné podmínky zadávací dokumentace v případě, že by byla dodávka do 5G sítě předmětem veřejné zakázky. V případě využití doporučení při zadávání veřejných zakázek je nezbytné, aby bylo užití kritérií v zadávací dokumentaci odůvodněné dle požadavků příslušných právních předpisů a nezávisle na doporučení. Využití doporučení pro zadávání veřejných zakázek však není vybranými institucemi státu předpokládáno a doporučení nebylo připravováno za tímto účelem.

2 Východiska doporučení

Východiska doporučení představují základ úvah vybraných institucí státu o netechnických aspektech bezpečnosti dodavatelského řetězce, přičemž vycházejí ze základních bezpečnostních zájmů České republiky a reflektují rovněž zahraniční doporučení pro kybernetickou bezpečnost 5G sítí a obdobné materiály uvedené výše.

Jedním ze zásadních předpokladů zajištění kybernetické bezpečnosti technologických řešení 5G sítí, stejně jako mnohých jiných systémů a sítí, je **posouzení důvěryhodnosti dodavatelů a subdodavatelů** takového řešení. Důvěra v dodavatele přitom musí být přítomna jak na úrovni konečné podoby dodávaného řešení, tak na strategické úrovni, tj. podnikatelského, právního a politického prostředí, ve kterém se dodavatel pohybuje.

Snižování rizik spojených s dodavateli do 5G sítí pouze technickými prostředky je přitom nedostatečné; hardware i software těchto technologických řešení jsou natolik komplexní, že je nelze efektivně technicky prověřit a eliminovat případné zranitelnosti. Ty v nich tak mohou zůstat dlouhodobě neodhaleny či do nich mohou být později zavedeny, například v rámci aktualizací. **Důvěra v dodavatele je v tomto ohledu zásadní. Vliv právního a politického prostředí, ze kterého dodavatel pochází nebo kterým je ovlivňován, má na důvěryhodnost značný význam, a proto je nezbytné jej k zajištění bezpečnosti nejdůležitějších součástí 5G sítí zohlednit.**

Důvěryhodnost dodavatelů je v tomto ohledu z pohledu vybraných institucí státu ovlivňována mimo jiné tím, zda dodavatel:

- má sídlo ve státě, resp. podléhá pouze právním řádům států:
  - které mají demokraticky volenou vládu, což mj. zahrnuje existenci nezávislé opozice, svobodných voleb, na základě jejichž výsledku může být stávající vláda vyměněna, a fungující princip tzv. brzd a protivah,
  - které mají nezávislý soudní systém, jenž nepodléhá přímým politickým zásahům, jsou v něm dodržována závazná pravidla, zvyklosti a zásady právního státu, jako je právo na spravedlivý proces vč. ctění presumpce neviny, práva na veřejné projednání věci a práva být souzen bez zbytečného odkladu,
  - jejichž právní předpisy a veřejné politiky se řídí zásadami právního státu a jsou vydávány s ohledem na ně,
  - které dbají na ochranu duševního vlastnictví,
  - které dlouhodobě či systematicky neporušují mezinárodní právo a vůči jimž nebo vůči jejichž aktivitám se oficiálně nevymezují mezinárodní a nadnárodní organizace či aliance, kterých je Česká republika členem, a to např. v podobě rezoluce Rady bezpečnosti Organizace spojených národů či omezujícího opatření společné zahraniční a bezpečnostní politiky Evropské unie,

- které udržují s Českou republikou partnerské vztahy a neprovádí činnosti, které jdou proti základním zájmům České republiky nebo jejích spojeneckých států,
- které nepovažují Českou republiku za nepřátelský stát,

- není nepatřičně ovlivňován zahraniční vládou či orgánem státní správy a je s dostatečnou mírou autonomie schopen zajišťovat dostupnost, integritu a důvěryhodnost dat v dodaných technologických řešeních,
- sleduje obchodní cíle, podniká v souladu se zvyklostmi mezinárodního obchodu a nepožívá od státu, v němž má sídlo nebo pod jehož vliv spadá, nepřiměřených výhod (např. státní podporu významně narušující hospodářskou soutěž),
- naplňuje bezpečnostní standardy, které jsou v době realizace dodávky na trhu běžné, a je ochoten zavázat se k jejich naplňování i do budoucna.

Výše uvedená východiska nejsou zamýšlena k použití jako kritéria pro hodnocení důvěryhodnosti dodavatelů pro operátory; návrhu konkrétních vyhodnotitelných kritérií pro tyto subjekty se věnuje část 3 doporučení.

3 Kritéria pro posílení důvěryhodnosti dodavatelů

Operátoři a další zástupci odvětví elektronických komunikací mohou při výběru dodavatele posoudit níže uvedená kritéria, která reflektují východiska uvedená v části 2 doporučení, a jejich naplnění zvyšuje pravděpodobnost výběru důvěryhodného dodavatele. V takovém případě je vhodné vztáhnout kritéria na všechny pořizované dodávky technologií, které jsou relevantní z hlediska bezpečnosti budovaných 5G sítí, a to s ohledem na významnost konkrétní dodávky pro technologický celek. Kritéria je proto za daných okolností možné a vhodné aplikovat jak na dodavatele, kteří vstupují s odběratelem do přímého smluvního vztahu, tak v přiměřeném rozsahu na jejich dodavatele a subdodavatele, pokud to povaha a okolnosti dodávky umožňují.

Vybrané instituce státu, které doporučení zpracovaly, jsou si přitom plně vědomy toho, že je to právě stát, který je nejlépe vybaven k posuzování strategických kritérií důvěryhodnosti dodavatelů a že některými informacemi nezbytnými k takovému posouzení disponují pouze vybrané bezpečnostní instituce státu. Jak však již bylo uvedeno v části 1 doporučení, do doby vzniku zákonného rámce prověřování důvěryhodnosti ze strany státu nabízejí vybrané instituce státu níže uvedená nezávazně aplikovatelná kritéria operátorům a všem dalším zájemcům z odvětví elektronických komunikací ke zohlednění při výběru dodavatelů dle jejich úvahy a možností.

Přestože byla kritéria doporučení připravována s maximálním ohledem na jejich využitelnost v praxi, **nemožnost posouzení nebo zohlednění některého z kritérií doporučení či nenaplnění kritéria ze strany dodavatele nemusí automaticky znamenat nevhodnost využití dodavatele nebo vysoké riziko s ním spojené.** Vhodnost aplikace a váhu každého kritéria pro důvěryhodnost dodavatele je nezbytné posoudit vždy s ohledem na kontext příslušné dodávky, včetně významnosti dodávky pro technologický celek.

Ambicí doporučení také není stanovit maximální či minimální počet kritérií, které by měl dodavatel splnit, aby byl považován za důvěryhodného; doporučení má sloužit jako jedno z vodítek využitelných pro výběr vhodných kritérií. **Doporučení nemění či neomezuje jakoukoliv povinnost orgánů a osob povinných dle zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti.**

3.1 Strategická kritéria

Obchodní aktivity každého dodavatele vychází z určitého státoprávního rámce. Tento rámec je zpravidla definován právním řádem státu, v němž má dodavatel své sídlo a jeho kulturním prostředím. Dodavatelé nicméně často spadají také do jurisdikce, resp. právního a kulturního prostředí, jiných států. Z hlediska bezpečnosti je proto vhodné (dle možností konkrétního subjektu) analyzovat a posoudit kritéria reflektující souladnost právních norem, zásad a zvyklostí, kterými je dodavatel dle různých právních řádů vázán, s normami, zásadami a zvyklostmi českého právního řádu.

Strategická kritéria zvyšující důvěryhodnost dodavatele jsou zejména:

- Dodavatel a jeho ovládající osoby[6] mají sídlo v členském státě EU či Severoatlantické aliance (dále jen „NATO“).
- Dodavatel má sídlo ve státě, resp. podléhá pouze právním řádům států, které jsou smluvními stranami mezinárodních smluv o kybernetické bezpečnosti, mají s Českou republikou platné dohody o spolupráci v oblasti bezpečnosti či podobná ujednání nebo se na ně taková pravidla vztahují. Jedná se zejména o:
  - členské státy EU a státy zajišťující odpovídající ochranu osobních údajů ve smyslu čl. 45 obecného nařízení o ochraně osobních údajů (GDPR)[7],
  - státy, které jsou smluvní stranou některé ze smluv o výměně a vzájemné ochraně utajovaných informací s Českou republikou[8],
  - státy, které jsou smluvní stranou Dohody o vládních zakázkách[9], či
  - státy, které jsou smluvní stranou tzv. Budapešťské úmluvy o počítačové kriminalitě[10].
- Dodavatel má sídlo ve státě, resp. podléhá pouze právním řádům států, na které veřejně neupozorňují bezpečnostní instituce České republiky v souvislosti s prováděním zpravodajských či jiných operací, poškozujících zájmy České republiky nebo členských států EU či NATO[11].
- Dodavatel je ochoten zavázat se prohlášením, že je právně i fakticky schopen odmítnout sdělení či zpřístupnění důvěrných informací od svých zákazníků nebo o svých zákaznících třetím stranám; v případě zákonné informační povinnosti odkazuje dodavatel na příslušná ustanovení v právních předpisech.

---

[6] Ve smyslu § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, přiměřeně.

[7] V případě států, které nejsou členy EU, se bude jednat zejména o státy, na něž se vztahuje rozhodnutí Komise o odpovídající ochraně dle čl. 45 obecného nařízení o ochraně osobních údajů (GDPR). Pro přehled platných rozhodnutí Komise viz ÚOOÚ. Předávání založené na rozhodnutí o odpovídající úrovni ochrany osobních údajů [online]. Dostupné z: https://www.uoou.cz/predavani-zalozene-na-rozhodnuti-o-odpovidajici-urovni-ochrany-osobnich-udaju/ds-5065

[8] NBÚ. Mezinárodní smlouvy o výměně a vzájemné ochraně utajovaných informací [online]. Dostupné z: https://www.nbu.cz/cs/mezinarodni-vztahy/941-mezinarodni-smlouvy-o-vymene-a-vzajemne-ochrane-utajovanych-informaci/

[9] WTO. Parties, observers and accessions: Agreement on Government Procurement [online]. Dostupné z: https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm

[10] COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185 [online]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=aLFDJWbF

[11] Tato veřejná upozornění mohou být například součástí výroční zprávy Bezpečnostní informační služby (BIS. Výroční zprávy [online]. Dostupné z: https://www.bis.cz/vyrocni-zpravy/), výroční zprávy Vojenského zpravodajství (VOJENSKÉ ZPRAVODAJSTVÍ. Výroční zprávy [online]. Dostupné z: https://www.vzcr.cz/vyrocni-zpravy-o-cinnosti-vojenskeho-zpravodajstvi-41) nebo Zprávy o stavu kybernetické bezpečnosti v ČR (NÚKIB. Zprávy o stavu [online]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/).

3.2 Obchodní kritéria

Mnozí dodavatelé působí na trhu již delší dobu a mají tak určitou reputaci a historii chování v obchodních vztazích. Povědomí o obchodních praktikách dodavatele je dalším významným aspektem, který je při volbě dodavatele důležité zhodnotit. Stejně tak je pro posouzení důvěryhodnosti dodavatele vhodné disponovat relevantními informacemi o vlastnické struktuře, financování, struktuře řízení dodavatele a dalších faktorech, které mají zásadní vliv na obchodní chování dodavatele.

Obchodní kritéria zvyšující důvěryhodnost dodavatele jsou zejména:

- Dodavatel má transparentní vlastnickou strukturu a strukturu řízení společnosti a významné změny v těchto strukturách odběrateli sděluje či umožňuje sledovat.
- Odběrateli není známo, že by nad dodavatelem vykonával účinnou míru kontroly hospodářské činnosti[12] stát, který nenaplňuje některá ze strategických kritérií relevantních pro státy (viz část 3.1 doporučení).
- Odběrateli není známo, že by byl dodavatel skrytě nebo neprůhledně financován nebo získával neprůhlednou finanční podporu či jiné finanční prostředky, které nejsou z obchodního hlediska zdůvodnitelné.
- Odběrateli není známo, že by dodavatel či jeho zástupci[13] jednali dlouhodobě nebo systematicky neeticky, v rozporu s péčí řádného hospodáře či v rozporu s pravidly mezinárodního obchodu a v případě jejich předchozího působení v České republice také v závažném rozporu s právním řádem České republiky[14].

[12] Ve smyslu § 5 zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic), přiměřeně.

[13] Ve smyslu § 436 odst. 1 a násl. zákona č. 89/2012 Sb., občanského zákoníku, přiměřeně.

[14] Např. že dodavatel či jeho zástupci nebyli v ČR odsouzeni za úmyslné spáchání trestného činu.

3.3 Technicko-bezpečnostní kritéria

Přestože jsou napříč tímto doporučením vyzdvihována netechnická kritéria pro posouzení důvěryhodnosti dodavatele, je třeba si uvědomit, že zcela zásadní jsou pro bezpečnost sítí 5G rovněž technické aspekty dodávek do těchto sítí. Přístup dodavatele k bezpečnostně-technickým pravidlům a procesům a ochota být v tomto směru transparentní je významným znakem vypovídajícím o jeho důvěryhodnosti.

Technicko-bezpečnostní kritéria zvyšující důvěryhodnost dodavatele jsou zejména:

- Dodavatel je schopen prokázat, že ve svých produktech používá tzv. princip security by design a praktikuje účinná bezpečnostní pravidla a procesy.
- Dodavatel a jím nabízená řešení odpovídají standardům v oblasti ochrany osobních údajů a ochrany duševního vlastnictví, a to včetně jejich souladu s právními předpisy v těchto oblastech.
- Dodavatel je ochoten zavázat se k dodržování bezpečnostních pravidel, která si s odběratelem stanovil.
- Dodavatel je schopen a ochoten poskytovat odběrateli přesné informace o svém dodavatelském řetězci a kontroluje a vymáhá dodržování bezpečnostních pravidel ujednaných se svými dodavateli.
- Dodavatel je schopen a ochoten poskytovat odběrateli přesné informace o původu a skladbě jednotlivých dodávaných komponent, software i hardware, které mají dopad na bezpečnost dodávaného technologického řešení.
- Dodavatel je ochoten zavázat se, že bude odběrateli nahlašovat zranitelnosti, které v jím dodávaném technologickém řešení existují nebo v něm budou v budoucnosti objeveny.
- Dodavatel je schopen a ochoten poskytovat odběrateli informace o kybernetických nebo jiných bezpečnostních incidentech, které se týkají odběratele nebo které mají významný dopad na činnost odběratele nebo dodaného technologického řešení.
- Dodavatel je ochoten zavázat se, že umožní odběrateli provádět u dodavatele nezávislé bezpečnostní audity a zpřístupní odběrateli závěry z nezávislého penetračního testování dodávaného technologického řešení.
- Dodavatel poskytuje odběrateli informace ohledně aktualizací a údržby jím dodávaného technologického řešení a je ochoten zavázat se poskytovat odběrateli během životního cyklu dodávaného technologického řešení aktualizace opravující (dodavateli) známé zranitelnosti.
- Dodavatel je ochoten se zavázat, že do dodávaného technologického řešení úmyslně neintegruje nebo vědomě neumožní integrovat zranitelnosti.

Závěr

Cílem tohoto doporučení je představit pohled státu na posuzování důvěryhodnosti dodavatelů technologií 5G sítí a podpůrné vodítko pro volbu důvěryhodných dodavatelů.

Bezpečnost je klíčovou a nezbytnou součástí fungování systémů kritických pro chod státu a musí být integrována již od počátku jejich budování, včetně výběru dodavatele těchto systémů. Pro splnění tohoto požadavku je mj. nutné velmi dobře rozumět tomu, kdo jsou dodavatelé a výrobci technologií, zda jsou důvěryhodní a zda jednají eticky a v souladu s českým právním řádem.

Přestože se toto doporučení zaměřuje na volbu důvěryhodných dodavatelů do 5G sítí strategicky nejvýznamnější infrastruktury České republiky, a to s implikací pro národní bezpečnost, doporučená kritéria jsou univerzálními zásadami. Je tedy možné je obdobně aplikovat i v dalších oblastech při zavádění technologií.