Pracovní překlad

Pražské návrhy

Prohlášení předsedy o kybernetické bezpečnosti komunikačních sítí v globálně digitalizovaném světě

Mezinárodní bezpečnostní konference o 5G Praha

Praha, 3. května 2019

PREAMBULE: KOMUNIKAČNÍ SÍTĚ V GLOBÁLNĚ DIGITALIZOVANÉM SVĚTĚ

Komunikace je základním kamenem našich společností. Definuje téměř každý aspekt našeho života. Rychlý rozvoj a rozsah, ve kterém využíváme komunikační technologie, však zvyšují naši závislost a zranitelnost.

Sítě 5G a budoucí komunikační technologie podstatně změní způsob, jakým komunikujeme a jakým žijeme. Dopravní, energetická, zemědělská, výrobní, zdravotní, obranná a další odvětví budou prostřednictvím těchto sítí příští generace významně posílena a změněna. Očekává se, že vysokorychlostní technologie s nízkou latencí umožní skutečný digitální rozvoj, který bude stimulovat růst, inovace a blahobyt. Bude umožněna automatizace každodenních činností a využití internetu věcí v plném rozsahu.

Tento vývoj s sebou však přináší významná rizika pro důležité veřejné zájmy a má dopady na národní bezpečnost. Škodliví aktéři dnes působí v kybernetickém prostoru mimo jiné se záměrem podkopat soudržnost našich společností a paralyzovat řádné fungování států nebo podniků. To zahrnuje pokusy o kontrolu nebo rušení našich komunikačních kanálů a přenášených informací. V digitalizovaných společnostech to může mít vážné následky.

Bezpečnost komunikačních kanálů se proto stala životně důležitou. Narušení integrity, důvěrnosti nebo dostupnosti přenášených informací nebo dokonce narušení samotné služby může vážně zkomplikovat každodenní život, společenské funkce, ekonomiku a národní bezpečnost. Komunikační infrastruktury jsou základním kamenem našich společností, přičemž sítě 5G se stanou stavebními kameny nového digitálního prostředí.

K VÝZNAMU BEZPEČNOSTI SÍTÍ 5G

Předseda uznává, že architektura a funkce sítí 5G musí být podloženy odpovídající úrovní bezpečnosti, vzhledem k tomu, že bezpečnost sítí 5G má zásadní význam pro národní bezpečnost, hospodářskou bezpečnost a další národní zájmy a globální stabilitu.

Členské státy EU zdůrazňují svůj vlastní probíhající proces, jehož cílem je definovat společný přístup EU k otázce kybernetické bezpečnosti sítí 5G, který iniciovala Evropská komise vydáním svého doporučení ze dne 26. března 2019.

S úmyslem podpořit probíhající diskuse o tom, jak snížit bezpečnostní rizika spojená s vývojem, nasazováním, provozováním a udržováním složitých komunikačních infrastruktur jako jsou sítě 5G, předseda akceptuje následující východiska:

Kybernetická bezpečnost není jen technickou záležitostí

Kybernetickou bezpečnost nelze považovat za čistě technickou záležitost. Bezpečná, spolehlivá zabezpečená a odolná infrastruktura vyžaduje odpovídající národní strategie, vhodné politiky, komplexní právní rámec a

odborný personál, který je řádně vyškolen a vzděláván. Silná kybernetická bezpečnost podporuje ochranu občanských svobod a soukromí.

Technická i netechnická povaha kybernetických hrozeb

Při řešení kybernetických bezpečnostních hrozeb je třeba vzít v úvahu nejen jejich technický charakter, ale také specifické politické, ekonomické či jiné chování škodlivých aktérů, kteří se snaží využít naší závislosti na komunikačních technologiích.

Možné závažné dopady narušení sítí 5G

Díky širokému uplatnění sítí založených na 5G by neoprávněný přístup ke komunikačním systémům mohl odhalit nebývalé množství informací nebo dokonce narušit celé společenské procesy.

Celostátní přístup

Politiky a činnosti přijaté za účelem zajištění vysoké úrovně kybernetické bezpečnosti by neměly být zaměřeny a prováděny pouze primárními zúčastněnými stranami (tj. provozovateli a dodavateli technologií), ale měly by být zohledňovány také všemi relevantními zúčastněnými stranami v jiných oblastech a odvětvích, která významně ovlivňují obecnou úroveň bezpečnosti, např. vzdělávání, diplomacie, výzkum a vývoj atd. Zajištění kybernetické bezpečnosti komunikační infrastruktury není pouze ekonomickým nebo obchodním problémem.

Nezbytné je správné hodnocení rizik

Systematické a pečlivé hodnocení rizik, které zahrnuje technické i netechnické aspekty kybernetické bezpečnosti, je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Měly by být vypracovány a zavedeny bezpečnostní rámce založené na posuzování rizika, které by zohledňovaly nejmodernější politiky a prostředky ke zmírnění bezpečnostních rizik.

Široká povaha bezpečnostních opatření

Opatření v oblasti kybernetické bezpečnosti musí být dostatečně široká tak, aby zahrnovala celou škálu bezpečnostních rizik, tj. lidí, procesů, fyzické infrastruktury a nástrojů na operační i strategické úrovni.

Žádná univerzální řešení

Rozhodnutí o optimální cestě vpřed při stanovování/ustavování vhodných opatření ke zvýšení bezpečnosti by mělo reflektovat jedinečné společenské a právní rámce, ekonomiku, soukromí, technologickou soběstačnost a další relevantní faktory důležité pro každý národ.

Zajištění bezpečnosti při podpoře inovací

Inovace je hlavní hnací silou rozvoje a hospodářského růstu v moderních společnostech. Podporuje také nová bezpečnostní řešení. Politiky, zákony a normy by měly umožnit, aby bezpečnostní opatření byla flexibilní, aby

bylo možné řídit propojení mezi bezpečností a specifickými národními podmínkami. Skrze tuto flexibilitu by měla být podporována tvořivost a inovace.

Bezpečnost stojí peníze

Dosažení řádné úrovně bezpečnosti někdy vyžaduje vyšší náklady. Zvýšené náklady by měly být tolerovány, pokud to bezpečnost vyžaduje. Zároveň ale bezpečnost vyšší náklady nutně přinášet nemusí.

Bezpečnost dodavatelského řetězce

Společná odpovědnost všech zúčastněných stran by měla být hnací silou bezpečnosti dodavatelského řetězce. Operátoři komunikační infrastruktury jsou často závislí na technologii od jiných dodavatelů. Značná bezpečnostní rizika vyplývají z přeshraniční komplexity stále globálnějšího dodavatelského řetězce, který poskytuje vybavení ICT. Tato rizika by měla být zvážena v rámci posuzování rizik na základě relevantních informací a měla by se snažit zabránit šíření kompromitovaných zařízení a používání škodlivého kódu a funkcí.

S ohledem na tyto perspektivy předsedající vyzývá k odpovědnému rozvoji, zavádění a údržbě sítí 5G a budoucích komunikačních technologií s přihlédnutím k následujícím návrhům a osvědčeným postupům.

PRAŽSKÉ NÁVRHY

Předseda předkládá následující návrhy ve čtyřech různých kategoriích v přípravě na zavedení 5G a budoucích sítí.

A. Politiky

- Komunikační sítě a služby by měly být navrženy s ohledem na odolnost a bezpečnost. Měly by být budovány a udržovány s využitím mezinárodních, otevřených, konsenzuálních standardů a osvědčených postupů kybernetické bezpečnosti založených na vědomí rizik. Měly by být podporovány jasné globálně interoperabilní pokyny kybernetické bezpečnosti, které by podporovaly produkty a služby kybernetické bezpečnosti při zvyšování odolnosti všech zúčastněných stran.
- Každá země může v souladu s mezinárodním právem stanovit své vlastní požadavky na bezpečnost a vymáhání práva, které by měly respektovat soukromí a dodržovat zákony chránící informace před neoprávněným shromažďováním a zneužíváním.
- Zákony a politiky upravující sítě a služby konektivity by se měly řídit zásadami transparentnosti a nestrannosti, s přihlédnutím ke globální ekonomice a interoperabilním pravidlům, s dostatečným dohledem a respektem k vládě práva.
- Je třeba vzít v úvahu celkové riziko vlivu třetí země na dodavatele, zejména ve vztahu ke způsobu vlády, neexistenci dohod o spolupráci v oblasti bezpečnosti nebo podobných ujednání, jakými jsou rozhodnutí o přiměřenosti, pokud jde o ochranu údajů, nebo zda je tato země účastníkem multilaterálních, mezinárodních nebo bilaterálních dohod o kybernetické bezpečnosti, boji proti počítačové trestné činnosti nebo ochraně údajů.

B. Technologie

- Zúčastněné strany by měly pravidelně provádět hodnocení zranitelnosti a zmírňování rizika ve všech součástech a síťových systémech, před vydáním produktu a během provozu systému, a podporovat kulturu vyhledání/opravy/záplaty, která by zmírnila zjištěné zranitelnosti a rychle nasadila opravy nebo záplaty.
- Při posuzování rizik produktů dodavatele by měly být zohledněny všechny relevantní faktory, včetně příslušného právního prostředí a dalších aspektů ekosystém dodavatele, neboť tyto faktory mohou být relevantní pro úsilí zúčastněných stran o udržení nejvyšší možné úrovně kybernetické bezpečnosti.
- Při budování odolnosti a bezpečnosti je třeba vzít v úvahu, že škodlivé kybernetické aktivity nemusí vždy vyžadovat využití technické zranitelnosti, např. v případě útoku zevnitř organizace.
- V zájmu zvýšení přínosů globální komunikace by státy měly přijmout politiky umožňující účinné a bezpečné toky dat v síti.
- Zúčastněné strany by měly vzít v úvahu technologické změny, které doprovázejí zavedení sítí 5G, např. využití Edge computing a softwarově definovaných sítí / virtualizaci síťových funkcí a jejich dopad na celkovou bezpečnost komunikačních kanálů.
- Zákazník - ať už vláda, provozovatel nebo výrobce - musí být schopen být informován o původu a etymologii součástí a softwaru, které ovlivňují úroveň bezpečnosti výrobku nebo služby, v souladu s nejnovějšími a příslušnými obchodními a technickými postupy, včetně transparentnosti údržby, aktualizací a nápravou produktů a služeb.

C. Ekonomika

- Pro bezpečnost a ekonomickou odolnost je nezbytný rozmanitý a živý trh komunikačních zařízení a dodavatelský řetězec.
- Robustní investice do výzkumu a vývoje jsou přínosem pro globální ekonomiku a technologický pokrok a představují způsob, jak potenciálně zvýšit rozmanitost technologických řešení s pozitivními účinky na bezpečnost komunikačních sítí.
- Komunikační sítě a síťové služby by měly být financovány otevřeně a transparentně pomocí standardních osvědčených postupů v oblasti zadávání veřejných zakázek, investic a uzavírání smluv.
- Státem podporované pobídky, dotace nebo financování komunikačních sítí 5G a poskytovatelů služeb by měly respektovat zásady férovosti, být obchodně přiměřené, prováděné otevřeně a transparentně, založené na zásadách hospodářské soutěže na otevřeném trhu, při zohlednění obchodních závazků.
- Rozhodující je efektivní dohled nad klíčovými finančními a investičními nástroji ovlivňujícími rozvoj telekomunikační sítě.
- Komunikační sítě a poskytovatelé síťových služeb by měli mít transparentní vlastnictví, partnerství a struktury správy a řízení společnosti.

D. Bezpečnost, soukromí a odolnost

- Všechny zúčastněné strany včetně průmyslu by měly spolupracovat na podpoře bezpečnosti a odolnosti sítí, systémů a připojených zařízení národní kritické infrastruktury.
- Mělo by být podporováno sdílení zkušeností a osvědčených postupů, včetně případné pomoci, se zmírňováním, vyšetřováním, reakcí a zotavováním se ze síťových útoků, kompromitace nebo narušení.
- Hodnocení bezpečnosti a rizik dodavatelů a síťových technologií by mělo brát v úvahu vládu práva, bezpečnostní prostředí, špatné chování dodavatelů a dodržování otevřených, interoperabilních, bezpečných standardů a osvědčených postupů v průmyslu, aby se podpořila živá a robustní dodávka produktů a služeb v oblasti kybernetické bezpečnosti, čelící vzrůstajícím výzvám.
- Měl by být zaveden rámec řízení rizik způsobem, který respektuje zásady ochrany údajů, aby se zajistilo soukromí občanů využívajících síťová zařízení a služby.