Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Manažerské shrnutí

Vyhláška o nepominutelných funkcích stanoveného rozsahu navazuje na obsah nového Zákona o kybernetické bezpečnosti hned několika způsoby a týká se výhradně potřeb Mechanismu prověřování bezpečnosti dodavatelského řetězce (Část První, Hlava II zákona).

Mechanismus se uplatní pouze na ty poskytovatele regulované služby v režimu vyšších povinností, o jejichž službách je to výslovně uvedeno ve Vyhlášce o regulovaných službách (§ 6). Mechanismus se pak použije jen v případě těch aktiv, které jsou 1) v zákonem stanoveném rozsahu řízení bezpečnosti a 2) jsou tzv. kritickou částí stanoveného rozsahu. Zákon o kybernetické bezpečnosti pak definuje, že touto kritickou částí jsou 1) aktiva, u kterých poskytovatel regulované služby v režimu vyšších povinností postupem podle Vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností (příloha č. 1 vyhlášky) ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická, nebo – a to je zde podstatné – 2) jsou to aktiva, která zajišťují nepominutelné funkce stanoveného rozsahu. Co je „nepominutelnou funkcí stanoveného rozsahu" stanovuje právě tato vyhláška, která s ohledem na specifický význam ICT pro sektor elektronických komunikací upravuje prioritně právě tento sektor. Její obsah je tak jedním ze dvou způsobů, jak identifikovat aktiva, na kterých se bude mechanismus prověřování bezpečnosti dodavatelského řetězce realizovat.

Tento dokument slouží jako rozpracované teze budoucí vyhlášky a je proto podkladem k další diskuzi. Může se měnit a to v závislosti jak na obsahu připomínek odborné veřejnosti, tak na obsahu připomínek v průběhu legislativního procesu.

Návrh

VYHLÁŠKA

ze dne dd.mm.rrrr,

o nepominutelných funkcích stanoveného rozsahu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle X zákona č. X Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):

§ 1
Předmět právní úpravy

Tato vyhláška upravuje podle § X odst. 4 *[Prověřování rizik spojených s dodavatelem]* zákona č. X Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „zákon“), nepominutelné funkce stanoveného rozsahu pro regulovanou službu zajišťování veřejné komunikační sítě a regulovanou službu poskytování veřejně dostupné služby elektronických komunikací podle přílohy k vyhlášce č. XX/XXXX Sb., o regulovaných službách *[Vyhláška o regulovaných službách]*.

§ 2
Vymezení pojmů

Pro účely této vyhlášky se rozumí veřejnou komunikační sítí veřejná komunikační síť podle právního předpisu upravujícího elektronické komunikace[1].

§ 3
Nepominutelné funkce

Nepominutelné funkce podle § X odst. 4 *[Prověřování rizik spojených s dodavatelem]* zákona jsou nepominutelné funkce uvedené v příloze této vyhlášky.

§ 4
Účinnost

Tato vyhláška nabývá účinnosti dnem dd.mm.rrrr.

Ředitel:
Ing. Lukáš Kintr v. r.

[1] § 2 odst. 2 písm. d) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

Příloha k vyhlášce XX/XXXX Sb.

Nepominutelné funkce

Kategorie nepominutelných funkcí	Popis nepominutelné funkce
1. Nepominutelné funkce ve veřejné komunikační síti	1.1 Funkce související s řízením síťových zdrojů se směrováním a jinou kontrolou nebo řízením provozu koncových uživatelů ve veřejné komunikační síti, které mohou mít významný dopad na síťový provoz. Zde náleží zejména služby či komponenty významné co do velikosti zeměpisné oblasti pokrytí nebo počtu připojených uživatelů, služby nebo komponenty řídící významnou část provozu komunikační sítě a služby či komponenty datového centra, které jsou nutné pro provoz kritické části veřejné komunikační sítě.
	1.2 Evidence, správa přístupu, ověřování a autorizace koncových uživatelů, přidělování síťových zdrojů koncovým uživatelům a správa připojení a relací koncových uživatelů.
	1.3 Registrace, autentizace a autorizace funkcí veřejné komunikační sítě a síťových služeb.
	1.4 Funkce umožňující přístup k údajům o zeměpisné poloze koncových zařízení zpracovávaných v rámci veřejné komunikační sítě nebo umožňující určení polohy zařízení pomocí prostředků veřejné komunikační sítě.
	1.5 Funkce související s ukládáním síťových dat a dat koncových uživatelů.
	1.6 Infrastrukturní služby nezbytné pro podporu provozu veřejné komunikační sítě a veřejné dostupné služby elektronických komunikací.
	1.7 Funkce zavádějící rozhraní pro propojování mezi jednotlivými veřejnými komunikačními sítěmi nebo službami, včetně roamingu.
	1.8 Funkce související s vystavováním jádra sítě externím aplikacím.
	1.9 Funkce, kterými jsou veřejné komunikační sítě nebo služby propojeny, pokud může mít taková funkce významný dopad na přístup k veřejné komunikační síti nebo na síťový provoz.
	1.10 Centralizované řízení šifrování veřejné komunikační sítě, funkcí veřejné komunikační sítě a provozu koncových uživatelů a šifrovacích klíčů.
	1.11 Funkce zabezpečení informací ovlivňujících nepominutelné funkce veřejné komunikační sítě.
	1.12 Systémy řízení veřejné komunikační sítě a monitorování této sítě, včetně řízení a monitoringu kybernetické bezpečnosti, pokud se tyto systémy týkají řízení nebo monitorování nepominutelných funkcí veřejné komunikační sítě nebo pokud mohou mít významný dopad na přístup k síti nebo na síťový provoz.

	1.13	Fakturační, podpůrné a back-end systémy, které mohou mít významný dopad na přístup k veřejné komunikační síti nebo na síťový provoz.
	1.14	Funkce zavádějící záznam a monitorování provozních a lokalizačních údajů.
	1.15	Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic.
	1.16	Funkce virtualizace, je-li použita pro implementaci nepominutelné funkce nebo opatření považovaného za nepominutelnou funkci veřejné komunikační sítě a jakékoliv funkce a opatření spadající pod takovou virtualizaci.
2. Nepominutelné funkce sítí 4. generace (veřejná komunikační síť provozovaná s využitím standardu 3GPP LTE (Release 8 a vyšší) nebo standardem IEEE 802.16m))	2.1	Registr předplatitelů, který ukládá data pro zpracování uživatelských připojení a relací [Home Subscriber Server (HSS)].
	2.2	Brána poskytující spojení mezi uživatelským zařízením a externí paketovou datovou sítí [Packet Gateway (PGW)].
	2.3	Brána přepojující pakety mezi vnitřní IP sítí operátora a externí IP sítí [Packet Data Network Gateway (PDN GW)].
	2.4	Brána používaná k navázání spojení mezi uživateli s přístupem mimo 3GPP směřování provozu [Evolved Packet Data Gateway (ePDG)].
	2.5	Funkce sloužící k řízení zásad připojení uživatelů a platby [Policy and Charging Rules Function (PCRF)].
	2.6	Funkce odpovědná za správu koncového připojení a mobility [Mobile Management Entity (MME)].
	2.7	Brána odpovědná za směrování provozu na uživatelské úrovni [Serving Gateway (SGW)].
	2.8	Funkce předávací název centrální databáze obsahující uživatelská data funkce HSS z registru předplatitelů do dalších síťových funkcí [Subscription Locator Function (SLF)].
	2.9	Registr identit zařízení obsahující informace o autorizaci k používání mobilního zařízení [Equipment Identity Register (EIR)].
	2.10	Server odpovědný za ověřování a autorizaci uživatelů s přístupem mimo síť 3GPP [3GPP AAA Server].
	2.11	Proxy server odpovědný za ověřování a autorizaci uživatelů s přístupem mimo síť 3GPP [3GPP AAA Proxy Server].
	2.12	Funkce řídící uživatelský provoz mezi mobilní sítí a přístupovými sítěmi mimo síť 3GPP [Access Network Discovery and Selection Function (ANDSF)].
3. Nepominutelné funkce sítí 5. generace (veřejná komunikační síť vyhovující standardu sítí elektronických	3.1	Funkce autentizace koncových zařízení uživatelů [Authentication Server Function (AUSF)].
	3.2	Funkce odpovědná za ukončení provozu v řídící rovině, registraci koncových zařízení a řízení mobility [Access and Mobility Management Function (AMF)].
	3.3	Funkce sloužící k ukládání a získávání nestrukturovaných dat [Unstructured Data Storage Function (UDSF)].

komunikací dle specifikace 3GPP/ETSI zahrnující minimálně standard přístupové rádiové sítě 5G NR (New Radio) v architektuře, která splňuje požadavky specifikací ETSI TS 123 501 (3GPP TS 23.501) a ETSI TS 138 401 (3GPP TS 38.401) nebo aktuálnějších.	3.4	Funkce umožňující poskytování funkcí jádra sítí 5. generace třetím stranám a externím aplikacím [Network Exposure Function (NEF)].
	3.5	Funkce umožňující poskytování funkcí jádra sítí 5. generace třetím stranám a externím aplikacím [Intermediate Network Exposure Function (I-NEF)].
	3.6	Funkce řízení dostupnosti, registrace a autorizace síťových služeb [Network Repository Function (NRF)].
	3.7	Funkce odpovědná za služby a specifikace segmentace sítě [Network Slice Selection Function (NSSF)].
	3.8	Funkce odpovědná za ověřování a autorizaci jednotlivých síťových segmentů [Network Slice Specific Authentication and Authorisation Function (NSSAAF)].
	3.9	Funkce odpovědná za řízení provozu a zavedení politiky řízení přístupu [Policy Control Function (PCF)].
	3.10	Funkce řídící uživatelské relace [Session Management Function (SMF)].
	3.11	Funkce řídící přístup uživatelů a vytváření a řízení šifrovacích klíčů [Unified Data Management (UDM)].
	3.12	Datové úložiště schopné ukládat a získávat informace (zejména informace o předplatitelích) [Unified Data Repository (UDR)].
	3.13	Funkce odpovědná za směrování, kontrolu a řízení provozu na uživatelské datové rovině [User Plane Function (UPF)].
	3.14	Funkce pro ukládání a uchovávání identifikačních dat uživatelských zařízení (tzv. radio capability ID data) [UE Radio Capability Management Function (UCMF)].
	3.15	Funkce podporující rozhodování o směrování v síti [Application Function (AF)].
	3.16	Registr identit zařízení či vybavení, který obsahuje informace o autorizaci k používání mobilních zařízení [5G-Equipment Identity Register (5G-EIR)].
	3.17	Funkce shromažďující a analyzující data pro řízení sítě [Network Data Analytics Function (NWDAF)].
	3.18	Funkce umožňující online a offline platby, které určují zejména účtování uživateli za využité služby [Charging Function (CHF)].
	3.19	Směrování zpráv do ostatních síťových funkcí [Service Communication Proxy (SCP)].
	3.20	Proxy server, který zajišťuje propojení s jinými sítěmi [Security Edge Protection Proxy (SEPP)].
	3.21	Funkce umožňující přístup k síťovým funkcionalitám pro uživatele mimo mobilní síť [Non-3GPP InterWorking Function (N3IWF)].
	3.22	Funkce umožňující připojení uživatelského zařízení k jádru sítí 5. generace prostřednictvím přístupové technologie jiné než 3GPP [Trusted Non-3GPP Gateway Function (TNGF)].
	3.23	Funkce zajišťující propojení mezi kabelovou sítí a jádrem sítí 5. generace [Wireline Access Gateway Function (W-AGF)].