NÁVRH

V souladu s čl. 116 odst. 6 zákona o elektronických komunikacích (Úřední věstník Republiky Slovinsko (RS) č. 130/22 a 18/23 – ZDU-1O) Agentura pro komunikační sítě a služby Republiky Slovinsko s přihlédnutím k informačnímu postupu podle směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1), vydává níže uvedený

OBECNÝ AKT
o dodatečných bezpečnostních požadavcích a omezeních

Článek 1
(Obsah obecného aktu)

Tento obecný akt stanoví:

1. pokyny, kterými se řídí operátoři mobilních komunikačních sítí (dále jen „operátoři“), kteří tyto sítě poskytují kritickým subjektům, které jsou správci kritické infrastruktury v jiných oblastech správy kritické infrastruktury ve smyslu zákona upravujícího oblast kritické infrastruktury (dále jen „správci kritické infrastruktury“), poskytovatelům základních služeb ve smyslu zákona upravujícího bezpečnost informací (dále jen „poskytovatelé základních služeb“), orgánům státní správy ve smyslu zákona upravujícího bezpečnost informací (dále jen „orgány státní správy“) nebo držitelům klíčových částí národního bezpečnostního systému a
2. kritické prvky sítě a související informační systémy s jejich funkcemi podle čl. 116 odst. 6 zákona o elektronických komunikacích (Úřední věstník RS č. 130/22 a 18/23 – ZDU-1O; dále jen „zákon“), ve znění uvedeném v příloze, která je nedílnou součástí tohoto obecného aktu a je vypracována ve spolupráci s orgánem odpovědným za bezpečnost informací.

Článek 2
(Definice)

(1) Pojmy použité v tomto obecném aktu mají tento význam:

1. Dodavatelský řetězec je celý systém procesů, lidí, organizace a distribuce zapojených do návrhu, výroby, ukládání, distribuce a dodávek, jakož i instalace a údržby komponentů kritických prvků sítě instalovaných v síti operátora nebo u poskytovatele cloudových služeb, který tyto služby poskytuje operátorovi.

2. Kritickými prvky sítě se rozumí síťové prvky, funkce, služby a podpůrné informační systémy ve fyzické, softwarové nebo virtualizované podobě u operátora nebo poskytovatele cloudových služeb uvedené v příloze tohoto obecného aktu.

3. Kritickými subjekty jsou správci kritické infrastruktury v jiných oblastech správy kritické infrastruktury ve smyslu zákona upravujícího kritickou infrastrukturu, poskytovatelé základních služeb ve smyslu zákona upravujícího bezpečnost

informací, orgány státní správy ve smyslu zákona upravujícího bezpečnost informací a držitelé klíčových částí národního bezpečnostního systému.

(2) Ostatní pojmy použité v tomto obecném aktu mají tentýž význam jako v zákoně a v obecném aktu o bezpečnosti sítí, služeb a údajů.

Článek 3
(Obecné pokyny)

(1) Operátoři v dodavatelském řetězci komponentů kritických prvků sítě a služeb podpory třetí úrovně pro tyto komponenty musí po celou dobu životního cyklu těchto komponentů dodržovat alespoň následující pokyny:

1. u každého výrobce nebo dodavatele a u poskytovatele služeb podpory třetí úrovně na základě vzájemných vztahů a dohod provedou posouzení rizik, pokud jde o dodávky a potenciální dopady ze strany třetích fyzických osob nebo právnických osob zřízených na základě veřejného nebo soukromého práva (dále jen „třetí strany“), kompatibilitu se zařízením jiných výrobců, kvalitu a bezpečnost výrobků a potenciální negativní dopady na provoz služeb operátora a kritických subjektů,
2. ujistí se, že zabezpečení je zabudováno a provedeno již v návrhu a že smlouvy obsahují lhůty pro odstranění zjištěných zranitelností,
3. ujistí se, že během celého životního cyklu jejich používání jsou zajištěny klíčové bezpečnostní prvky (dostupnost, důvěrnost, integrita a autenticita),
4. ujistí se, že je zaručena jejich bezpečnost a nepřetržité dodávky a že mají certifikaci pro podporu vlastností zajišťujících vysokou bezpečnost v souladu s mezinárodně uznávanými (3GPP) a evropskými technickými normami (ETSI),
5. ujistí se, že pokyny uvedené v bodech 2 až 4 tohoto odstavce jsou ověřitelné ve smluvní dokumentaci u výrobce nebo u dodavatele,
6. u každého výrobce nebo dodavatele rovněž posoudí a zohlední rizika spojená s právy na užívání klíčových technologií, které jsou nezbytné pro výrobu a používání zařízení, a rizika spojená s dodávkou zařízení, náhradních dílů nebo služeb podpory třetí úrovně,
7. ujistí se, že použité komponenty nemají žádné známé kritické zranitelnosti, které nebyly opraveny nebo jsou aktivně zneužívány,
8. vyhnou se jedinému výrobci nebo dodavateli, pokud je to technicky proveditelné a ekonomicky udržitelné, s cílem snížit závislost a zvýšit odolnost v případě zranitelnosti kritických komponentů, katastrofického selhání sítě nebo ohrožení bezpečnosti sítí a služeb kritických subjektů třetími stranami, ať už fyzickými osobami nebo právnickými osobami zřízenými na základě veřejného nebo soukromého práva.

(2) Při poskytování informačních a komunikačních zařízení, systémů a služeb musí operátoři plně dodržovat pokyny Agentury Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) a platné předpisy Evropské unie týkající se základních bezpečnostních požadavků při zadávání veřejných zakázek na bezpečné produkty a služby IKT. Agentura na svých internetových stránkách zveřejní odkazy na stávající dokumenty agentury ENISA a předpisy EU ve výše uvedené oblasti a průběžně je aktualizuje.

(3) Při poskytování komponentů kritických prvků sítě nebo při využívání cloudových služeb se upřednostňuje výběr komponentů od těch výrobců nebo dodavatelů nebo služeb od těch poskytovatelů cloudových služeb, kteří byli certifikováni subjekty posuzování shody,

které byly akreditovány a případně autorizovány na základě čl. 60 odst. 3 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“) pro vydávání evropských certifikátů kybernetické bezpečnosti s určitými úrovněmi záruky, jak je stanoveno v článku 52 nařízení.

(4) Pro účely předchozího odstavce operátor ověří zvláštní internetovou stránku, pokud ji agentura ENISA zřídí v souladu s článkem 55 nařízení za účelem poskytování informací a propagace evropských systémů certifikace kybernetické bezpečnosti, evropských certifikátů kybernetické bezpečnosti a EU prohlášení o shodě, včetně informací o evropských systémech certifikace kybernetické bezpečnosti, které již nejsou platné, o zrušených a neplatných evropských certifikátech kybernetické bezpečnosti a EU prohlášeních o shodě, a úložiště odkazů na informace o kybernetické bezpečnosti.

Článek 4
(Posouzení rizik)

(1) Při určování rizika výrobce nebo dodavatele komponentů a poskytovatele služeb podpory třetí úrovně pro kritické prvky sítě zohledňuje operátor níže uvedené rizikové aspekty, které vyhodnocuje.

(2) Při hodnocení uvedeném v předchozím odstavci operátor posoudí a zohlední alespoň:

1. celkovou kvalitu (včetně bezpečnostních aspektů) a spolehlivost;
2. úroveň využívání otevřených standardů a rozhraní, které zabraňují závislosti a vazbě na produkty konkrétního výrobce nebo dodavatele (tzv. obchodní proprietární uzamčení, angl. „vendor lock-in“),
3. soulad s uznávanými mezinárodními a evropskými technickými normami (3GPP, ETSI) a předpisy Evropské unie a také výchozí nastavení zabezpečení v souladu s profesními doporučeními (sdružení GSMA);
4. úroveň kompatibility se zařízeními a síťovými funkcemi třetích stran;
5. schopnost poskytovat modernizace a přizpůsobení;
6. proces řízení a odhalování zranitelností a aktuálnost aktualizací a záplat,
7. dostupnost a transparentnost dokumentace týkající se:
   - klíčových vlastností a informací o bezpečnostních a dalších funkcích a možných nastaveních komponentu a
   - použitý software, včetně softwaru s otevřeným zdrojovým kódem (softwarový kusovník, angl. „Sotware Bill Of Materials – SBOM“);
8. úroveň závislosti na službách podpory třetího stupně při provozování a údržbě zařízení, pokud operátor nevykonává tyto služby sám pomocí svých zaměstnanců;
9. předchozí posouzení shody zařízení nebo subjektu, který by poskytoval službu podpory třetí úrovně, ze strany subjektů akreditovaných v Evropské unii v rámci evropských systémů certifikace kybernetické bezpečnosti, přičemž akreditované subjekty jsou zveřejněny v Úředním věstníku Evropské unie.

(3) Operátor zdokumentuje rizikové faktory a výsledky hodnocení rizik pro každého vybraného výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně uvedených v odstavcích 2 a 3 tohoto článku a pravidelně je aktualizuje.

Článek 5
(Obecné pokyny pro provoz kritických prvků sítě)

(1) Komponenty kritických prvků sítě, jejich provoz a výchozí nastavení nesmí zahrnovat technické prvky, které by mohly negativně ovlivnit bezpečnost nebo provoz kritických subjektů, včetně sabotáže, špionáže, krádeže duševního vlastnictví nebo terorismu.

(2) Kritické prvky sítě jsou zpravidla umístěny ve Slovinské republice nebo, s přihlédnutím ke všem bezpečnostním rizikům a zajištění vysoké úrovně bezpečnostních opatření, pokud platné předpisy nestanoví jinak, v Evropské unii. Operátor informuje Agenturu pro komunikační sítě a služby Republiky Slovinsko (dále jen „agentura“) a orgán odpovědný za bezpečnost informací o svém zamýšleném přemístění nejméně 30 dní před přemístěním mimo Evropskou unii.

(3) Služby podpory třetí úrovně pro kritické prvky sítě se zpravidla poskytují v Republice Slovinsko nebo, s přihlédnutím ke všem bezpečnostním rizikům a zajištění vysoké úrovně bezpečnostních opatření, pokud platné předpisy nestanoví jinak, v Evropské unii. Operátor oznámí agentuře a orgánu odpovědnému za bezpečnost informací zamýšlené přemístění svých služeb podpory třetí úrovně nejméně 30 dnů před přemístěním mimo země Evropské unie.

(4) Poskytování služeb podpory třetí úrovně nesmí ohrozit bezpečnost nebo provoz služeb kritických subjektů nebo národní bezpečnost.

(5) Operátor musí zavést a pravidelně provádět proces identifikace kritických prvků sítě. Ten je nutné provádět alespoň jednou ročně nebo při nákupu komponentů kritických prvků sítě.

(6) Pokud jednotlivý komponent představuje kritický prvek sítě pouze částečně, je považován za součást kritického prvku sítě.

(7) Operátor vede aktuální seznam všech komponentů kritických prvků sítě, jejich funkcí, umístění, osob, které je spravují a řídí, jejich poskytovatelů služeb podpory třetí úrovně a jejich výrobců nebo dodavatelů. Seznam se na požádání zpřístupňuje agentuře a orgánu odpovědnému za bezpečnost informací.

Článek 6
(Bezpečnostní opatření pro dodávky komponentů kritických prvků sítě)

(1) Operátor musí znát celý dodavatelský řetězec a být si vědom jeho rizik, včetně subdodavatelů jednotlivých komponentů kritických prvků sítě, včetně šifrovacích klíčů, UICC/eUICC a dalších bezpečnostních prvků, jejichž zneužití by mohlo ohrozit bezpečnost kritických subjektů.

(2) Operátor zajistí, aby byly mezi ním a výrobci nebo dodavateli komponentů kritických prvků sítě nebo jeho poskytovateli služeb podpory třetí úrovně smluvně dohodnuty a

zdokumentovány bezpečnostní požadavky, a vyžaduje, aby výrobci nebo dodavatelé dodržovali dohodnutá bezpečnostní opatření v celém dodavatelském řetězci.

(3) S cílem včas zabránit zneužití zranitelnosti subjekty s nekalými úmysly operátor zajistí, aby se výrobce nebo dodavatel komponentů kritického prvku sítě smluvně zavázal, že bude operátora neprodleně informovat o zjištěné zranitelnosti a opatřeních ke zmírnění rizika a poradí mu, jaká ochranná nebo nápravná opatření může operátor v reakci na hrozbu přijmout.

(4) Operátor alespoň jednou ročně vyhodnocuje přiměřenost přístupových práv ke kritickým prvkům sítě nebo je neprodleně aktualizuje v souladu se změnami v organizaci nebo u poskytovatele služeb podpory třetí úrovně.

(5) Operátor se vyhýbá závislosti na jediném dodavateli nebo poskytovateli služeb podpory třetí úrovně (tzv. obchodní proprietární uzamčení, angl. „vendor lock-in“), pokud je to technicky proveditelné a ekonomicky udržitelné, s cílem snížit závislost a zvýšit odolnost v případě zranitelnosti kritických komponentů, a to i tím, že se vyhne dlouhodobým smlouvám s jediným výrobcem nebo dodavatelem nebo poskytovatelem služeb podpory třetí úrovně nebo tyto smlouvy změní s cílem minimalizovat narušení poskytování služeb kritickým subjektům.

Článek 7
(Smluvní ujednání s výrobci, dodavateli nebo poskytovateli služeb podpory třetí úrovně)

V zájmu zajištění vysoké úrovně bezpečnosti zahrne operátor do nových smluvních ujednání s výrobci, dodavateli nebo poskytovateli služeb podpory třetí úrovně alespoň:

1. prohlášení výrobce nebo dodavatele, že komponent nebo jeho výchozí nastavení nemají nedokumentovanou možnost „vstupu zadními dveřmi“ nebo negativní dopad na provoz kritických subjektů,
2. závazek výrobce, dodavatele nebo poskytovatele služeb podpory třetí úrovně chránit informace, které získá nebo ke kterým má přístup v průběhu poskytování služby,
3. závazek výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně neprodleně informovat operátora v případě porušení ochrany komunikačních nebo provozních údajů, které má nebo by mohlo mít vliv na operátora nebo kritické subjekty uvedené v čl. 1 bodě 1 tohoto obecného aktu;
4. závazek výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně neprodleně informovat operátora o jakémkoli bezpečnostním incidentu a zranitelnosti, které by mohly ovlivnit bezpečnost sítě, souvisejících služeb nebo údajů operátora;
5. závazek výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně dodržovat bezpečnostní normy a pravidla stanovená operátorem a přijmout vhodná bezpečnostní opatření k zajištění bezpečnosti informačních systémů a sítí a údajů operátora nebo kritického subjektu;
6. možnost operátora kdykoli zkontrolovat prostředí, postupy, bezpečnostní opatření a nástroje používané poskytovatelem služeb podpory třetí úrovně při přístupu k síti a údajům operátora,
7. odpovědnost výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně za škody vzniklé v důsledku identifikovaných zranitelností nebo zneužití komponentů kritických prvků sítě, jejich výchozího nastavení nebo poskytování

služeb podpory třetí úrovně, které výrobce nebo dodavatel nebo poskytovatel služeb podpory třetí úrovně zanedbá nebo provede úmyslně,

8. povinnost pravidelně školit pracovníky výrobce nebo dodavatele nebo poskytovatele služeb podpory třetí úrovně v oblasti bezpečnosti údajů a informačních systémů a sítí.

Článek 8
(Pravidla týkající se přístupu a používání kritických prvků sítě)

(1) Při fyzickém nebo logickém přístupu ke komponentům kritických prvků sítě, jejich nastavení a údajům operátora, které jsou v nich uloženy, zpracovávány nebo upravovány, operátor zajistí:

1. že přístup je přísně omezen na osoby, které k němu byly předem oprávněny,
2. že všechny práce na kritických prvcích sítě prováděné na místě nebo prostřednictvím vzdáleného přístupu jsou kontrolovány operátorem,
3. že u uživatelů, kteří mají nejvyšší oprávnění k přístupu k jednotlivým komponentům kritických prvků sítě, jejich nastavení nebo datům v nich uloženým či zpracovávaným, se provádí vícefaktorové ověřování,
4. že každá oprávněná osoba, které je udělen přístup, má jedinečný uživatelský účet a heslo,
5. že se používají pouze hesla, která jsou měněna pravidelně nebo v případě zjištěného zneužití okamžitě a která mají alespoň 15 znaků a obsahují velká a malá písmena, číslice a speciální znaky, pokud to software umožňuje,
6. že se u přístupu uplatňuje koncepce nulové tolerance nebo důvěry všude, kde je to možné,
7. že bezpečnost komunikačního spojení od oprávněného uživatele k jednotlivým komponentům je chráněna použitím šifrování s ohledem na nejnovější technologický vývoj a osvědčenou průmyslovou správnou praxi v oblasti bezpečnosti informací nebo podle doporučení zavedených institucí v oblasti bezpečnosti informací;
8. že se uchovává nesmazatelný záznam o přístupech a pokusech o přístup po dobu nejméně 6 měsíců, včetně záložní kopie, může však být uchováván po delší dobu, pokud z analýzy řízení rizik a posouzení přijatelné úrovně rizika vyplývá, že rizika by byla přiměřeně zvládnuta delším uchováváním záznamů,
9. že se pokud možno zaznamenávají a monitorují všechny softwarové zásahy do komponentů, včetně změn konfigurace. Záznamy, včetně záložní kopie těchto údajů, se uchovávají po dobu uvedenou v předchozím bodě,
10. že přístup k jednotlivým komponentům a údajům v nich uloženým nebo zpracovávaným je časově omezený a dostupný pouze po dobu trvání požadované práce.

(2) V případě přístupu pracovníků nebo zaměstnanců poskytovatele služeb podpory třetí úrovně k jednotlivým komponentům kritických prvků sítě je nutné:

1. používat pouze zabezpečenou zprostředkovatelskou vyhrazenou pracovní stanici (angl. „jump server“), která podléhá pravidelným bezpečnostním kontrolám,
2. instalovat na vyhrazenou pracovní stanici pouze nezbytně nutné nástroje, komponenty a aktivní služby pro přístup k dalším zdrojům v síti, které jsou zcela nezbytné a musí být aktualizovány nejnovějšími bezpečnostními záplatami,
3. používat na vyhrazené pracovní stanici, která musí být umístěna v síti operátora a pod jeho výhradní kontrolou, zabezpečené kryptografické operace a klíče,
4. aby se každý přístup povoloval ručně a aktivoval jej operátor pouze na dobu trvání přístupu,

5. aby byly všechny přístupy a činnosti fyzicky kontrolovány a zaznamenávány operátorem;
6. používat dvoufaktorové ověřování a hesla o délce nejméně 15 znaků, včetně velkých a malých písmen, číslic a speciálních znaků, jejichž počet se liší podle vyhodnocených rizik.

(3) Před tím, než operátor zadá poskytování služby správy, údržby nebo aktualizace kritických prvků sítě nebo jejich jednotlivých komponentů třetí straně, ověří a zajistí, že tato třetí strana má zavedeny mechanismy a postupy řízení bezpečnosti alespoň rovnocenné nebo lepší než ty, které má zavedeny operátor sám. O záměru zadat poskytování služeb neprodleně informuje kritický subjekt, jehož se změna týká, agenturu a orgán odpovědný za bezpečnost informací.

(4) Operátor ověří skutečný stav bezpečnostních procesů před zahájením poskytování služeb a poté nejméně jednou ročně. Operátor vede záznamy o interních přezkumech a kontrolách poskytování služeb podpory třetích stran a uchovává je po dobu poskytování služeb a po dobu jednoho roku po jejich ukončení, nejdéle však pět let.

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

Článek 9
(Přechodná ustanovení)

(1) Operátor informuje agenturu a orgán odpovědný za bezpečnost informací o stávajícím umístění kritických prvků sítě do 30 dnů od nabytí účinnosti tohoto obecného aktu.

(2) Operátor informuje agenturu a orgán odpovědný za bezpečnost informací o stávajícím místě poskytování služeb podpory třetí úrovně pro kritické prvky sítě do 30 dnů od nabytí účinnosti tohoto obecného aktu.

(3) Agentura poprvé zveřejní dokumenty uvedené v čl. 3 odst. 2 tohoto obecného aktu v den jeho nabytí účinnosti.

Článek 10
(Nabytí účinnosti)

Tento obecný akt nabývá účinnosti třicátým dnem po jeho vyhlášení v Úředním věstníku Republiky Slovinsko, přičemž operátoři mohou používat zařízení a poskytovat služby podpory třetí úrovně až do uplynutí lhůt stanovených v čl. 312 odst. 2 a 3 zákona.

č. _____ mag. Marko Mišmaš

V Lublani, dne _____ ředitel

EVA 2023-3150-0034

NÁVRH

NÁVRH

Příloha

Seznam kritických prvků sítě a příslušných informačních systémů:

Kritické prvky sítě	**Funkce sítě a informačních systémů**
Správa účastníků a mechanismy šifrování	- správa relací (hlasové a datové), - ověřování uživatelů a zařízení v síti, - správa a ukládání klíčů pro autorizaci účastníků a síťových komponentů (UICC/eUICC, digitální certifikáty / HSM), - funkce pro bezpečné ověřování, ochranu integrity komunikace (šifrování) a ukládání uživatelských klíčů, síťových komponentů a komponentů pro správu, - správa přístupových práv.
Propojení	- funkce hostingu a rozhraní s jinými sítěmi a službami.
Řízené síťové služby	- registrace a autorizace síťových služeb, - uchovávání a zpracování komunikačních, lokalizačních a provozních údajů, - vystavení sítě a síťových funkcí externím aplikacím a službám.
Správa a orchestrace virtualizovaných síťových funkcí (NFV) a síťová orchestrace (MANO), včetně virtualizační infrastruktury	- řídící funkce orchestrace a konfigurace NFV bez ohledu na typ implementace (VM, kontejner, mikroslužby), - virtualizační funkce pro implementaci a využívání NFV, - funkce výběru segmentů sítě (NSSF).
Rádiová přístupová síť	- základnové stanice, které podporují technologii 5G nebo vyšší.
Systémy řízení a další podpůrné systémy	- sledování provozu a správy mobilní komunikační sítě, včetně přístupové části (RAN/O-RAN), - systémy pro detekci bezpečnostních událostí, anomálií, hrozeb a jejich řízení (bezpečnostní funkce včetně SIEM/SOAR).
Zákonný odposlech	- funkce pro přístup příslušného orgánu k obsahu komunikací a provozním údajům uživatelů.