NÁVRH

Podľa článku 116 ods. 6 zákona o elektronických komunikáciách (Úradný vestník Slovinskej republiky č. 130/22 a 18/23 – ZDU-1O) Agentúra pre komunikačné siete a služby Slovinskej republiky, berúc do úvahy informačný postup v súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1), vydáva nasledujúci

VŠEOBECNÝ AKT
o dodatočných bezpečnostných požiadavkách a obmedzeniach

Článok 1
(Obsah všeobecného aktu)

Tento všeobecný akt stanovuje:

1. usmernenia, ktoré majú dodržiavať prevádzkovatelia mobilných komunikačných sietí (ďalej len „prevádzkovatelia“) poskytujúci tieto siete kritickým subjektom, ktoré sú správcami kritickej infraštruktúry v iných oblastiach regulácie kritickej infraštruktúry, ako sa uvádza v zákone upravujúcom oblasť kritickej infraštruktúry (ďalej len „správcovia kritickej infraštruktúry“), poskytovateľom základných služieb, ako sa stanovuje v zákone upravujúcom bezpečnosť informácií (ďalej len „poskytovatelia základných služieb“), orgánom štátnej správy stanoveným zákonom upravujúcim informačnú bezpečnosť (ďalej len „orgány štátnej správy“) alebo operátorom kľúčových častí bezpečnostného systému krajiny; a
2. kritické prvky siete a súvisiacich informačných systémov s ich funkciami uvedenými v článku 116 ods. 6 zákona o elektronických komunikáciách (Úradný vestník Slovinskej republiky č. 130/22 a 18/23 – ZDU-1O; ďalej len „zákon“), ako sa uvádza v prílohe, ktorá tvorí neoddeliteľnú súčasť tohto všeobecného aktu a je vypracovaná v spolupráci s orgánom zodpovedným za bezpečnosť informácií.

Článok 2
(Význam pojmov)

(1) Pojmy použité v tomto všeobecnom akte znamenajú:

1. Dodávateľský reťazec znamená celý systém procesov, osôb, organizácie a distribúcie podieľajúcich sa na navrhovaní, výrobe, skladovaní, distribúcii a dodávke, ako aj inštalácii a údržbe komponentov kritických sieťových prvkov inštalovaných v sieti prevádzkovateľa alebo u poskytovateľa cloudových služieb, ktorý takéto služby poskytuje prevádzkovateľovi.

2. Kritické prvky siete sú tie sieťové prvky, funkcie, služby a podporné informačné systémy vo fyzickej, softvérovej alebo virtualizovanej forme u prevádzkovateľa alebo u poskytovateľa cloudových služieb, ktoré sú uvedené v prílohe k tomuto všeobecnému aktu.

3. Kritické subjekty sú správcovia kritickej infraštruktúry v iných oblastiach regulácie kritickej infraštruktúry stanovení v súlade so zákonom upravujúcim oblasť kritickej infraštruktúry, poskytovatelia základných služieb podľa zákona upravujúceho informačnú bezpečnosť, orgány štátnej správy určené zákonom upravujúcim informačnú bezpečnosť a operátori kľúčových častí bezpečnostného systému krajiny.

(2) Ostatné pojmy použité v tomto všeobecnom akte majú rovnaký význam, ako je vymedzený v zákone a vo všeobecnom akte o bezpečnosti sietí, služieb a údajov.

Článok 3
(Všeobecné usmernenia)

(1) Prevádzkovatelia v dodávateľskom reťazci komponentov kritických sieťových prvkov a podporných služieb tretej úrovne pre tieto komponenty zohľadňujú počas celého ich životného cyklu minimálne tieto usmernenia:

1. v prípade individuálneho výrobcu alebo dodávateľa a poskytovateľa podporných služieb tretej úrovne vykonajú z dôvodu vzťahov a zmlúv s nimi posúdenie rizika z hľadiska dodávky a potenciálnych vplyvov fyzických alebo právnických osôb tretích strán podliehajúcich verejnému alebo súkromnému právu (ďalej len „tretie strany“), kompatibility so zariadeniami iných výrobcov, kvality a bezpečnosti výrobkov a možných negatívnych vplyvov na prevádzku služieb prevádzkovateľa a kritických subjektov;
2. že bezpečnosť je integrovaná a implementovaná už na úrovni návrhu a že zmluvy obsahujú lehoty na odstránenie vnímaných zraniteľných miest;
3. že kľúčové bezpečnostné prvky (dostupnosť, dôvernosť, integrita a autenticita) musia byť zabezpečované počas celého životného cyklu ich používania;
4. že bezpečnosť a ich neprerušované dodávky musia byť zaručené a musí sa potvrdiť podpora prvkov vysokého zabezpečenia v súlade s medzinárodne uznávanými normami (3GPP) a európskymi technickými normami (ETSI);
5. že usmernenia uvedené v bodoch 2 až 4 tohto odseku sú overiteľné v zmluvnej dokumentácii s výrobcom alebo dodávateľom;
6. že sa v prípade každého výrobcu alebo dodávateľa posudzujú a zohľadňujú aj riziká spojené s právami na používanie kľúčových technológií, ktoré sú potrebné na výrobu a používanie zariadení, ako aj riziká súvisiace s dodávkou zariadení, náhradných dielov alebo podporných služieb tretej úrovne;
7. že použité komponenty nemajú nevyriešené známe kritické alebo aktívne zneužívané zraniteľné miesta;
8. aktívna snaha vyhnúť sa službám iba jediného výrobcu alebo dodávateľa, ak je to technicky uskutočniteľné a ekonomicky udržateľné, s cieľom znížiť závislosť a zvýšiť odolnosť v prípade zraniteľných miest kritických komponentov, zabrániť katastrofálnemu zlyhaniu siete alebo ohrozeniu bezpečnosti sietí a služieb kritických subjektov fyzickými alebo právnickými osobami tretích strán, ktoré podliehajú verejnému alebo súkromnému právu.

(2) Pri poskytovaní informačných a komunikačných zariadení, systémov a služieb prevádzkovatelia plne dodržiavajú usmernenia Agentúry Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) a platné nariadenia Európskej únie týkajúce sa základných bezpečnostných požiadaviek pri obstarávaní bezpečných produktov a služieb IKT. Agentúra na svojom webovom sídle uverejňuje odkazy na aktuálne dokumenty ENISA a nariadenia EÚ v uvedenej oblasti a priebežne ich aktualizuje.

(3) Pri dodávaní komponentov kritických sieťových prvkov alebo využívaní cloudových služieb sa uprednostňuje výber komponentov od tých výrobcov, dodávateľov alebo služieb poskytovateľov cloudových služieb, ktorí boli certifikovaní orgánmi posudzovania zhody a ktorí boli akreditovaní a v prípade potreby autorizovaní na základe článku 60 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (ďalej len „nariadenie“) na vydávanie európskych certifikátov kybernetickej bezpečnosti na určitej úrovni uistenia, ako sa stanovuje v článku 52 nariadenia.

(4) Na účely predchádzajúceho odseku prevádzkovateľ skontroluje osobitné webové sídlo zriadené agentúrou ENISA v súlade s článkom 55 nariadenia, ktorého cieľom je informovať verejnosť o európskych systémoch certifikácie kybernetickej bezpečnosti, európskych certifikátoch kybernetickej bezpečnosti a EÚ vyhláseniach o zhode vrátane informácií týkajúcich sa európskych systémov certifikácie kybernetickej bezpečnosti, ktoré už nie sú platné alebo boli zrušené, prípadne ktorých platnosť vypršala, a EÚ vyhlásení o zhode, ako aj register odkazov na informácie o kybernetickej bezpečnosti.

Článok 4
(Posúdenie rizika)

(1) Pri určovaní rizika výrobcu alebo dodávateľa komponentov a poskytovateľa služieb pre kritické sieťové prvky tretej úrovne prevádzkovateľ zohľadňuje tieto aspekty rizika, ktoré vyhodnotí.

(2) Pri vyhodnocovaní uvedenom v predchádzajúcom odseku prevádzkovateľ posudzuje a zohľadňuje minimálne:

1. celkovú kvalitu (vrátane bezpečnostných aspektov) a spoľahlivosť;
2. úroveň využívania otvorených štandardov a rozhraní, ktoré zabraňujú závislosti a odkázanosti na výrobky konkrétneho výrobcu alebo dodávateľa;
3. súlad s uznávanými medzinárodnými a európskymi technickými normami (3GPP, ETSI) a predpismi Európskej únie a predvolenými bezpečnostnými nastaveniami v súlade s odbornými odporúčaniami (Združenie GSMA);
4. úroveň kompatibility so zariadeniami a sieťovými funkciami tretích strán;
5. schopnosť poskytovať aktualizácie a prispôsobenia;
6. proces riadenia zraniteľných miest, ich zverejňovanie informácií a aktualizovaný proces aktualizácií a opráv;
7. dostupnosť a transparentnosť dokumentácie týkajúcej sa:
   - kľúčových funkcií a informácií o bezpečnosti a ďalších funkciách komponentu, ako aj možných nastaveniach, a
   - použitého softvéru vrátane otvoreného zdrojového kódu (kusovník – SBOM);
8. úroveň závislosti od podporných služieb tretej úrovne pri riadení a údržbe zariadení, ak prevádzkovateľ tieto služby nevykonáva sám so svojimi zamestnancami;
9. predbežné posúdenie zhody zariadení alebo subjektu, ktorý by poskytoval podporné služby tretej úrovne orgánmi akreditovanými v Európskej únii podľa európskych systémov certifikácie kybernetickej bezpečnosti, pričom akreditované orgány sú uverejnené v *Úradnom vestníku Európskej únie*.

(3) Prevádzkovateľ zdokumentuje rizikové faktory a výsledky posúdenia rizika každého vybraného výrobcu alebo dodávateľa alebo poskytovateľa služieb tretej úrovne uvedených v odsekoch 2 a 3 tohto článku a pravidelne ich aktualizuje.

Článok 5
(Všeobecné usmernenia k prevádzke kritických sieťových prvkov)

(1) Komponenty kritických sieťových prvkov, ich prevádzka a štandardné nastavenia nesmú obsahovať technické charakteristiky, ktoré by mohli negatívne ovplyvniť bezpečnosť alebo prevádzku kritických subjektov, okrem iného v dôsledku sabotáže, špionáže, krádeže duševného vlastníctva alebo terorizmu.

(2) Kritické sieťové prvky sa vo všeobecnosti nachádzajú v Slovinskej republike alebo – berúc do úvahy všetky bezpečnostné riziká a zabezpečovanie vysokej úrovne bezpečnostných opatrení – v Európskej únii, ak to nie je v platných nariadeniach stanovené inak. Prevádzkovateľ informuje agentúru pre komunikačné siete a služby Slovinskej republiky (ďalej len „agentúra“) a orgán zodpovedný za informačnú bezpečnosť o svojom plánovanom premiestnení aspoň 30 dní pred premiestnením mimo Európskej únie.

(3) Podporné služby tretej úrovne pre kritické prvky siete sa vo všeobecnosti vykonávajú v Slovinskej republike alebo – s prihliadnutím na všetky bezpečnostné riziká a zabezpečovanie vysokej úrovne bezpečnostných opatrení – v Európskej únii, ak to nie je v platných nariadeniach stanovené inak. Prevádzkovateľ informuje agentúru a orgán zodpovedný za bezpečnosť informácií o plánovanom premiestnení svojich podporných služieb tretej úrovne najmenej 30 dní pred premiestnením mimo krajín Európskej únie.

(4) Vykonávanie podporných služieb tretej úrovne nesmie ohroziť bezpečnosť alebo prevádzku služieb kritických subjektov ani národnú bezpečnosť.

(5) Prevádzkovateľ zavedie a pravidelne vykonáva proces identifikácie kritických sieťových prvkov. To sa musí vykonávať aspoň raz ročne alebo po obstaraní komponentov kritických sieťových prvkov.

(6) Aj keď jednotlivý komponent predstavuje kritický sieťový prvok iba čiastočne, považuje sa za súčasť kritického sieťového prvku.

(7) Prevádzkovateľ vedie aktualizovaný zoznam všetkých komponentov kritických sieťových prvkov, ich funkcií, lokalít, správcov a manažérov, ich poskytovateľov podporných služieb tretej úrovne a ich výrobcov či dodávateľov. Zoznam sa na požiadanie sprístupní agentúre a orgánu zodpovednému za bezpečnosť informácií.

Článok 6
(Bezpečnostné opatrenia pre dodávku komponentov kritických sieťových prvkov)

(1) Prevádzkovateľ si je vedomý celého dodávateľského reťazca a s ním spojených rizík vrátane subdodávateľov jednotlivých komponentov kritických sieťových prvkov, ktoré zahŕňajú aj šifrovacie kľúče, UICC/eUICC a iné bezpečnostné prvky, ktorých zneužitie by mohlo ohroziť bezpečnosť kritických subjektov.

(2) Prevádzkovateľ zabezpečuje, aby bezpečnostné požiadavky medzi prevádzkovateľom a výrobcami alebo dodávateľmi komponentov kritických sieťových prvkov alebo jeho poskytovateľmi podporných služieb tretej úrovne boli zmluvne dohodnuté a zdokumentované a aby výrobcovia alebo dodávatelia dodržiavali dohodnuté bezpečnostné opatrenia v celom dodávateľskom reťazci.

(3) S cieľom včas zabrániť zneužívaniu zraniteľných miest škodlivými aktérmi prevádzkovateľ zabezpečuje, aby sa výrobca alebo dodávateľ komponentov kritického sieťového prvku zmluvne zaviazal prevádzkovateľa okamžite informovať o zistenom zraniteľnom mieste a o opatreniach na zníženie rizík, ako aj poskytol odporúčanie o ochranných alebo nápravných opatreniach, ktoré môže prevádzkovateľ prijať v reakcii na hrozbu.

(4) Prevádzkovateľ aspoň raz ročne overuje primeranosť prístupových práv ku kritickým sieťovým prvkom alebo ich bezodkladne aktualizuje v súlade so zmenami v organizácii alebo na strane poskytovateľov podporných služieb tretej úrovne.

(5) Prevádzkovateľ zabraňuje tomu, aby bol od individuálneho dodávateľa alebo poskytovateľa služieb tretej úrovne závislý (t. j. „odkázanosť na určitého dodávateľa“), ak je to technicky uskutočniteľné a ekonomicky udržateľné, s cieľom znížiť závislosť a zvýšiť odolnosť v prípade zraniteľnosti kritických komponentov, a to aj tým, že sa vyhne dlhodobým zmluvám s jednotlivými výrobcami alebo dodávateľmi alebo poskytovateľmi podporných služieb tretej úrovne. alebo si zachová možnosť ich zmeniť s cieľom znížiť narušenia pri poskytovaní služieb kritickým subjektom na najnižšiu možnú úroveň.

Článok 7
(Zmluvné podmienky s výrobcami, dodávateľmi alebo poskytovateľmi podporných služieb tretej úrovne)

S cieľom zabezpečiť vysokú úroveň bezpečnosti prevádzkovateľ do nových zmluvných podmienok s výrobcami, dodávateľmi alebo poskytovateľmi podporných služieb tretej úrovne zahrnie aspoň tieto informácie:

1. vyhlásenie výrobcu alebo dodávateľa, že komponent alebo jeho predvolené nastavenia nemajú žiadne nezdokumentované zadné dvierka ani žiadny negatívny vplyv na prevádzku kritických subjektov;
2. záväzok výrobcu, dodávateľa alebo poskytovateľa služieb tretej úrovne, že bude chrániť údaje, s ktorými sa oboznámi počas poskytovania služieb alebo prístupu k nim v súvislosti s poskytovaním služby prístupu;
3. záväzok výrobcu, dodávateľa alebo poskytovateľa služieb tretej úrovne prevádzkovateľa okamžite informovať v prípade narušenia ochrany komunikačných údajov alebo prevádzkových údajov, ktoré ovplyvňuje alebo by mohlo ovplyvniť prevádzkovateľa alebo kritické subjekty uvedené v článku 1 bode 1 tohto všeobecného aktu;
4. záväzok výrobcu, dodávateľa alebo poskytovateľa služieb tretej úrovne prevádzkovateľa okamžite informovať o akomkoľvek bezpečnostnom incidente či slabých miestach, ktoré by mohli ovplyvniť bezpečnosť siete, súvisiacich služieb alebo údajov prevádzkovateľa;

5. záväzok výrobcu, dodávateľa alebo poskytovateľa služieb tretieho stupňa dodržiavať bezpečnostné normy a pravidlá stanovené prevádzkovateľom a prijať primerané bezpečnostné opatrenia na zaistenie bezpečnosti informačných systémov, sietí a údajov prevádzkovateľa alebo kritického subjektu;
6. schopnosť prevádzkovateľa kedykoľvek skontrolovať prostredia, postupy, bezpečnostné opatrenia a nástroje používané poskytovateľom podporných služieb tretej úrovne pri prístupe do siete a k údajom prevádzkovateľa;
7. zodpovednosť výrobcu, dodávateľa alebo poskytovateľa podporných služieb tretej úrovne za škodu, ktorá by vznikla identifikovanými zraniteľnými miestami alebo zneužitím komponentov kritických sieťových prvkov, ich predvoleným nastavením alebo počas poskytovania podporných služieb tretej úrovne, ktoré výrobca, dodávateľ alebo poskytovateľ podpory tretej úrovne zanedbal alebo úmyselne implementoval;
8. povinnosť pravidelne školiť zamestnancov výrobcu, dodávateľa alebo poskytovateľa podporných služieb tretej úrovne v oblasti bezpečnosti údajov a informačných systémov a sietí.

Článok 8
(Pravidlá týkajúce sa prístupu a používania kritických sieťových prvkov)

(1) Pri fyzickom alebo logickom prístupe ku komponentom kritických sieťových prvkov, k ich nastaveniam a k údajom prevádzkovateľa, ktoré sú v nich uložené, spracúvané alebo upravované, musí prevádzkovateľ zabezpečiť to, že:

1. prístup je prísne obmedzený na osoby, ktoré majú predchádzajúce povolenie;
2. všetky práce na kritických sieťových prvkoch vykonávané na mieste alebo prostredníctvom vzdialeného prístupu sú zo strany prevádzkovateľa kontrolované;
3. v prípade používateľov, ktorým sú pridelené najvyššie práva na prístup k jednotlivým komponentom kritických sieťových prvkov, k ich nastaveniam alebo k údajom, ktoré sú v nich uložené alebo spracúvané, sa vykonáva viacstupňové overenie;
4. každá oprávnená osoba, ktorej bol udelený prístup, má jedinečný používateľský účet a heslo;
5. sa používajú iba heslá, ktoré sa menia pravidelne alebo okamžite v prípade zisteného zneužitia, pričom obsahujú aspoň 15 znakov aj veľké a malé písmená, čísla a špeciálne znaky, ak to softvér umožňuje;
6. sa uplatňuje koncepcia nulovej tolerancie alebo dôvery v otázke prístupu tam, kde je to možné;
7. je bezpečnosť komunikačného spojenia od oprávneného používateľa k jednotlivým komponentom chránená šifrovaním, berúc do úvahy najnovší technologický vývoj a najlepšie priemyselné osvedčené postupy v oblasti informačnej bezpečnosti, alebo odporúčania uznávaných inštitúcií v oblasti informačnej bezpečnosti;
8. sa vykoná nezmazateľný záznam o prístupoch a pokusoch o prístup, ktorý sa uchováva najmenej 6 mesiacov vrátane záložnej kópie, no môže ísť aj o dlhšie obdobie, ak z analýzy riadenia rizík a posúdenia prijateľnej úrovne rizík vyplýva, že riziká by sa mali primerane riadiť uchovávaním záznamov na dlhšie obdobie;
9. tam, kde je to možné, sa vykonáva zaznamenávanie a monitorovanie všetkých softvérových zásahov do komponentov vrátane zmien konfigurácie. Záznamy vrátane záložnej kópie týchto údajov sa uchovávajú tak dlho, ako je uvedené v predchádzajúcom bode;
10. prístup k jednotlivým komponentom a k údajom, ktoré sú na nich uložené alebo spracúvané, je časovo obmedzený a otvorený len počas trvania nevyhnutnej práce.

(2) V prípade prístupu zamestnancov alebo zamestnancov poskytovateľa podporných služieb tretej úrovne k jednotlivým komponentom kritických sieťových prvkov títo musia:

1. používať len zabezpečenú prechodne vyhradenú pracovnú stanicu („jump server“), ktorá podlieha pravidelným bezpečnostným kontrolám;
2. na vyhradenej pracovnej stanici inštalovať len absolútne nevyhnutné nástroje, komponenty a aktívne služby na prístup k iným zdrojom v sieti, ktoré sú absolútne nevyhnutné a musia byť aktualizované najnovšími bezpečnostnými opravami;
3. používať na vyhradenej pracovnej stanici zabezpečené kryptografické operácie a kľúče, pričom stanica musí byť umiestnená v sieti prevádzkovateľa a byť pod jeho výlučnou kontrolou;
4. každý prístup musí byť manuálne schválený a aktivovaný prevádzkovateľom a len počas trvania prístupu;
5. všetky prístupy a činnosti sú fyzicky kontrolované a zaznamenávané prevádzkovateľom;
6. používať dvojstupňové overenie a heslá, ktoré majú aspoň 15 znakov a obsahujú veľké aj malé písmená, ako aj čísla a osobitné znaky, ktoré sa menia na základe posudzovaných rizík.

(3) Predtým, ako prevádzkovateľ prevedie službu riadenia, údržby alebo aktualizácie kritických sieťových prvkov alebo ich jednotlivých komponentov na tretiu stranu, musí overiť a zabezpečiť, že táto má zavedené aspoň rovnaké alebo lepšie bezpečnostné mechanizmy a procesy riadenia bezpečnosti v porovnaní so svojimi mechanizmami a procesmi. O zámere prevodu bezodkladne informuje dotknutý kritický subjekt, agentúru a orgán zodpovedný za bezpečnosť informácií.

(4) Prevádzkovateľ overuje skutočný stav bezpečnostných procesov pred začiatkom poskytovania služieb a následne aspoň raz ročne. Prevádzkovateľ vedie záznamy o interných preskúmaniach a kontrolách týkajúcich sa poskytovania podporných služieb tretích strán a uchováva ich počas trvania poskytovania služieb, ako aj jeden rok po ich ukončení, ale nie po obdobie dlhšie ako päť rokov.

PRECHODNÉ A ZÁVEREČNÉ USTANOVENIE

Článok 9
(Prechodné ustanovenia)

(1) Prevádzkovateľ agentúre a orgánu zodpovednému za bezpečnosť informácií oznamuje existujúce lokality kritických sieťových prvkov do 30 dní od nadobudnutia účinnosti tohto všeobecného aktu.

(2) Prevádzkovateľ agentúre a orgánu zodpovednému za bezpečnosť informácií oznamuje existujúce lokality podporných služieb tretej úrovne pre kritické sieťové prvky do 30 dní od nadobudnutia účinnosti tohto všeobecného aktu.

(3) Agentúra uverejňuje dokumenty uvedené v článku 3 ods. 2 tohto všeobecného aktu po prvýkrát odo dňa nadobudnutia jeho účinnosti.

Článok 10
(Nadobudnutie účinnosti)

Tento všeobecný akt nadobúda účinnosť tridsiatym dňom po jeho uverejnení v Úradnom vestníku Slovinskej republiky, pričom prevádzkovatelia môžu používať zariadenie a udržiavať poskytovanie podporných služieb tretej úrovne až do uplynutia lehôt stanovených v článku 312 ods. 2 a 3 zákona.

Č. _____ mag. Marko Mišmaš

Ľubľana, dňa _____ riaditeľ

EVA 2023-3150-0034

NÁVRH

Príloha

Zoznam kritických sieťových prvkov a súvisiacich informačných systémov:

Kritické sieťové prvky	**Funkcie siete a informačných systémov**
Riadenie účastníkov a šifrovacie mechanizmy	- Riadenie relácie (hlas a údaje), - overenie používateľov a zariadení v sieti, - riadenie a ukladanie kľúčov na overenie účastníkov a sieťových komponentov (UICC/eUICC, digitálne certifikáty/HSM), - funkcie na bezpečné overenie, ochranu komunikačnej integrity (šifrovanie) a ukladanie používateľských kľúčov, sieťových a riadiacich komponentov, - riadenie prístupových práv.
Prepojenie	- Hostingové funkcie a rozhrania k iným sieťam a službám.
Spravované sieťové služby	- Registrácia a povoľovanie sieťových služieb, - uchovávanie a spracúvanie komunikačných, lokalizačných a prevádzkových údajov, - vystavenie siete a sieťových funkcií externým aplikáciám a službám.
Riadenie a orchestrácia virtualizovaných sieťových funkcií (NFV) a sieťová orchestrácia (MANO) vrátane virtualizačnej infraštruktúry	- Funkcie riadenia orchestrácie a konfigurácie NFV bez ohľadu na typ zavedenia (VM, kontajner, mikroslužby), - virtualizačné funkcie na zavedenie a používanie NFV, - funkcia výberu sieťových segmentov („Network Slice Selection Function“, NSSF).
Rádiová prístupová sieť	- Základňové stanice, ktoré podporujú technológiu 5G alebo vyššiu.
Systémy riadenia a iné podporné systémy	- Monitorovanie prevádzky a riadenia mobilnej komunikačnej siete vrátane prístupovej časti (RAN/O-RAN), - systémy na odhaľovanie bezpečnostných udalostí, anomálií, hrozieb a ich riadenie (bezpečnostné funkcie vrátane SIEM/SOAR).
Zákonné odpočúvanie	- Funkcie prístupu príslušného orgánu ku komunikačnému obsahu a údajom o používateľskej prevádzke.