ETTEPANEK

Vastavalt elektroonilise side seaduse (UL RS nr 130/22 ja 18/23 – ZDU-1O) artikli 116 lõikele 6 annab Sloveenia Vabariigi sidevõrkude ja -teenuste amet, võttes arvesse Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiivi (EL) 2015/1535 (millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord) (ELT L 241, 17.9.2015, lk 1) kohast teavitamiskorda, välja järgmise üldakti.

ÜLDAKT
täiendavate turvanõuete ja -piirangute kohta

Artikkel 1
(Üldakti sisu)

Üldaktis on sätestatud

1. suunised, mida peavad järgima mobiilsidevõrgu operaatorid (edaspidi „operaatorid“), kes pakuvad neid võrke kriitilise tähtsusega üksustele, kes on elutähtsate infrastruktuuride reguleerimise muudes valdkondades elutähtsa infrastruktuuri haldajad, nagu on täpsustatud elutähtsa infrastruktuuri valdkonda reguleerivas seaduses (edaspidi „kriitilise tähtsusega taristuettevõtjad“), infoturbeseaduses kindlaks määratud elutähtsate teenuste osutajatele (edaspidi „oluliste teenuste osutajad“), infoturbeseaduses kindlaks määratud riigi haldusasutustele (edaspidi „riigi haldusasutused“) või riigi julgeolekusüsteemi oluliste osade vedajatele; ja
2. võrgu ja sellega seotud infosüsteemide kriitilised elemendid koos nende funktsioonidega, millele on osutatud elektroonilise side seaduse artikli 116 lõikes 6 (UL RS nr 130/22 ja 18/23 – ZDU-1O; edaspidi „akt“), nagu on esitatud lisas, mis on käesoleva üldakti lahutamatu osa ja mis on koostatud koostöös infoturbe eest vastutava organiga.

Artikkel 2
(Mõisted)

(1) Käesolevas üldaktis kasutatud terminid tähendavad järgmist.

1. Tarneahel on kogu protsesside, inimeste, organisatsiooni ja jaotamise süsteem, mis on seotud projekteerimise, tootmise, säilitamise, jaotamise ja tarnimisega, samuti operaatori võrku paigaldatud oluliste võrguelementide komponentide paigaldamise ja hooldamisega või operaatorile selliseid teenuseid osutava pilveteenuse operaatori juures.

2. Võrgu kriitilised elemendid on need võrguelemendid, funktsioonid, teenused ja toetavad infosüsteemid füüsilisel, tarkvara või virtualiseeritud kujul operaatori või pilveteenuse osutaja juures, nagu on loetletud käesoleva üldakti lisas.

3. Kriitilise tähtsusega üksused on elutähtsate infrastruktuuride haldajad muudes elutähtsa infrastruktuuri reguleerimise valdkondades, mis on kindlaks määratud kooskõlas elutähtsa infrastruktuuri valdkonda reguleeriva õigusega, elutähtsate teenuste osutajad, nagu on kindlaks määratud infoturvet reguleerivas seaduses, riigi

haldusasutused, nagu on kindlaks määratud infoturvet reguleerivas seaduses, ja riigi julgeolekusüsteemi oluliste osade kandjad.

(2) Muudel käesolevas üldseaduses kasutatud mõistetel on sama tähendus, mis on määratletud seaduses ja üldseaduses võrkude, teenuste ja andmete turvalisuse kohta.

Artikkel 3
(Üldsuunised)

(1) Kriitilise tähtsusega võrguelementide komponentide tarneahelas osalevad ettevõtjad ja nende komponentide kolmanda taseme tugiteenuste operaatorid peavad nende komponentide kogu olelusringi jooksul arvesse võtma vähemalt järgmisi suuniseid:

1. üksiktootja või tarnija ja kolmanda tasandi tugiteenuse osutaja puhul, kes on nendega sõlminud suhted ja kokkulepped, viivad läbi riskihindamise seoses tarnimise ja võimaliku mõjuga, mida avaldavad avalik-õiguslikud või eraõiguslikud füüsilised või juriidilised isikud (edaspidi „kolmandad isikud“), ühilduvusega teiste tootjate seadmetega, toote kvaliteedi ja ohutuse ning võimaliku negatiivse mõjuga operaatori teenuste ja kriitilise tähtsusega üksuste toimimisele;
2. et turvalisus on juba projekteerimisetapis sisse ehitatud ja kasutusele võetud ning et lepingud sisaldavad tähtaegu leitud kitsaskohtade kõrvaldamiseks;
3. peamised turvaelemendid (kättesaadavus, konfidentsiaalsus, terviklikkus ja autentsus) on tagatud kogu nende kasutamise olelusringi jooksul;
4. turvalisus ja katkematu tarne on tagatud ning on kinnitatud, et see toetab kõrgeid turvaelemente vastavalt rahvusvaheliselt tunnustatud standarditele (3GPP) ja Euroopa tehnilistele standarditele (ETSI);
5. et käesoleva lõike punktides 2–4 osutatud suunised on tootja või tarnijaga sõlmitud lepingudokumentidest kontrollitavad;
6. iga tootja või tarnija puhul hinnatakse ja võetakse arvesse ka põhitehnoloogia kasutusõigustega seotud riske, mis on vajalikud seadmete tootmiseks ja kasutamiseks, ning riske, mis on seotud seadmete, varuosade või kolmanda taseme tugiteenuste tarnimisega;
7. kasutatavatel komponentidel ei ole teadaolevaid lahendamata kriitilisi või aktiivselt ärakasutatavaid nõrku kohti;
8. vältida tuleb üksiktootjat või tarnijat, kui see on tehniliselt teostatav ja majanduslikult jätkusuutlik, et vähendada sõltuvust ja suurendada vastupidavust kriitilise tähtsusega komponentide haavatavuste, katastroofiliste võrgutõrgete või kriitilise tähtsusega üksuste võrkude ja teenuste turvaohu korral, mida põhjustavad avalik-õiguslikud või eraõiguslikud kolmandad füüsilised või juriidilised isikud.

(2) Info- ja sideseadmete, -süsteemide ja -teenuste tarnimisel järgivad operaatorid täielikult Euroopa Liidu Küberturvalisuse Ameti (edaspidi „ENISA“) suuniseid ja kehtivaid Euroopa Liidu määrusi, mis käsitlevad turvaliste IKT-toodete ja -teenuste hankimisel põhilisi turvanõudeid. Amet avaldab oma veebisaidil lingid ENISA olemasolevatele dokumentidele ja ELi määrustele eespool nimetatud valdkonnas ning hoiab need ajakohased.

(3) Kriitilise tähtsusega võrguelementide komponentide tarnimisel või pilveteenuste kasutamisel eelistatakse selliste pilveteenuse tootjate või tarnijate või teenuste komponente, mille on sertifitseerinud vastavushindamisasutused, mis on akrediteeritud ja vajaduse korral saanud loa Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määruse (EL) 2019/881 (mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (edaspidi „määrus“)) artikli 60 lõike 3 alusel, et anda välja Euroopa küberturvalisuse sertifikaate teataval usaldusväärsuse tasemel, nagu on kindlaks määratud määruse artiklis 52.

(4) Eelmise lõike kohaldamisel kontrollib käitaja ENISA poolt määruse artikli 55 kohaselt loodud spetsiaalset veebisaiti, mille eesmärk on teavitada üldsust Euroopa küberturvalisuse sertifitseerimise kavadest, Euroopa küberturvalisuse sertifikaatidest ja ELi vastavusdeklaratsioonidest, sealhulgas teabest Euroopa küberturvalisuse sertifitseerimise kavade kohta, mis ei ole enam kehtivad või on kehtetuks tunnistatud, ja aegunud Euroopa küberturvalisuse sertifikaatidest, ELi vastavusdeklaratsioonidest ning küberturvalisuse teabele viivatest linkidest.

Artikkel 4
(Riskihindamine)

(1) Võrgu kriitiliste elementide komponentide tootja või tarnija ja kolmanda tasandi teenuseosutaja riski kindlaksmääramisel puhul võtab operaator arvesse järgmisi riskiaspekte, mida ta hindab.

(2) Eelmises lõikes osutatud hindamisel hindab operaator ja võtab arvesse vähemalt järgmist:

1. üldine kvaliteet (sealhulgas ohutusaspektid) ja usaldusväärsus;
2. selliste avatud standardite ja liideste kasutamise tase, mis hoiavad ära sõltuvuse ja seotuse konkreetse tootja või tarnija toodetega;
3. vastavus tunnustatud rahvusvahelistele ja Euroopa tehnilistele standarditele (3GPP, ETSI) ning Euroopa Liidu määrustele ja vaiketurbe seadetele kooskõlas professionaalsete soovitustega (GSMA Association);
4. ühilduvuse tase kolmandate isikute seadmete ja võrgufunktsioonidega;
5. võime pakkuda uuendusi ja kohandusi;
6. kitsaskohtade juhtimise protsess, selle avalikustamine ja ajakohane protsess koos uuenduste ja parandustega;
7. dokumentide kättesaadavus ja läbipaistvus seoses järgmisega:
   - põhifunktsioonid ja teave komponendi turvalisuse ja muude funktsioonide ning võimalike seadistuste kohta ning
   - kasutatav tarkvara, sealhulgas avatud lähtekoodiga tarkvara (Bill of Materials – SBOM);
8. seadmete haldamisel ja hooldamisel sõltuvus kolmanda taseme tugiteenustest, kui operaator ei osuta neid teenuseid üksi oma töötajatega;
9. Euroopa küberturvalisuse sertifitseerimise kavade kohaselt Euroopa Liidus akrediteeritud asutuste poolt kolmanda taseme tugiteenust osutavate seadmete või üksuse vastavuse esialgne hinnang, mille kohaselt akrediteeritud asutused avaldatakse Euroopa Liidu Teatajas.

(3) Operaator dokumenteerib riskitegurid ja riskihindamise tulemused iga käesoleva artikli lõigetes 2 ja 3 osutatud valitud tootja või tarnija või kolmanda taseme teenuseosutaja kohta ning ajakohastab neid korrapäraselt.

Artikkel 5
(Üldsuunised kriitiliste võrguelementide käitamise kohta)

(1) Kriitilise tähtsusega võrguelementide komponendid, nende käitamine ja vaikeseaded ei tohi sisaldada tehnilisi omadusi, mis võiksid negatiivselt mõjutada kriitilise tähtsusega üksuste turvalisust või toimimist, muu hulgas sabotaaži, spionaaži, intellektuaalomandi varguse või terrorismi tõttu.

(2) Kriitilise tähtsusega võrguelemendid asuvad üldjuhul Sloveenia Vabariigis või, võttes arvesse kõiki turvariske ja tagades turvameetmete kõrge taseme, ning kui kohaldatavates määrustes ei ole sätestatud teisiti, siis Euroopa Liidus. Operaator teavitab Sloveenia Vabariigi sidevõrkude ja -teenuste ametit (edaspidi „amet“) ja infoturbe eest vastutavat asutust nende kavandatavast ümberpaigutamisest vähemalt 30 päeva enne ümberpaigutamist väljapoole Euroopa Liitu.

(3) Kriitiliste võrguelementide kolmanda tasandi tugiteenused asuvad üldjuhul Sloveenia Vabariigis või, võttes arvesse kõiki turvariske ja tagades turvameetmete kõrge taseme, ning kui kohaldatavates määrustes ei ole sätestatud teisiti, siis Euroopa Liidus. Käitaja teavitab ametit ja infoturbe eest vastutavat asutust oma kolmanda tasandi tugiteenuste kavandatavast ümberpaigutamisest vähemalt 30 päeva enne ümberpaigutamist väljapoole Euroopa Liidu riike.

(4) Kolmanda taseme tugiteenuste rakendamine ei tohi ohustada kriitilise tähtsusega ega riigi julgeolekuga seotud üksuste teenuste turvalisust ega toimimist.

(5) Operaator kehtestab kriitiliste võrguelementide kindlakstegemise protsessi ja rakendab seda korrapäraselt. Seda tuleb teha vähemalt kord aastas või siis, kui hangitakse kriitiliste võrguelementide komponente.

(6) Kui üksikkomponent esindab kriitilise tähtsusega võrguelementi ainult osaliselt, käsitatakse seda kriitilise võrguelemendi osana.

(7) Operaator peab ajakohastatud loetelu kõigist oluliste võrguelementide komponentidest, nende funktsioonidest, asukohtadest, administraatoritest ja haldajatest, nende kolmanda taseme tugiteenuste osutajatest ja tootjatest või tarnijatest. Taotluse korral tehakse loetelu kättesaadavaks ametile ja infoturbe eest vastutavale asutusele.

Artikkel 6
(Turvameetmed elutähtsate võrguelementide komponentide tarnimiseks)

(1) Operaator peab olema teadlik kogu tarneahelast ja sellega seotud riskidest, sealhulgas kriitiliste võrguelementide üksikute komponentide alltöövõtjatest, mis hõlmavad

ka krüpteerimisvõtmeid, UICC/eUICC ja muid turvaelemente, mille väärkasutamine võib ohustada kriitilise tähtsusega üksuste turvalisust.

(2) Operaator peab tagama, et turvanõuded operaatori ja kriitilise tähtsusega võrguelementide komponentide tootjate või tarnijate või tema kolmanda tasandi tugiteenuste osutajate vahel on lepinguliselt kokku lepitud ja dokumenteeritud, ning nõudma tootjatelt ja tarnijatelt kokkulepitud turvameetmete järgimist kogu tarneahelas.

(3) Selleks et pahatahtlikud osalejad ei kasutaks turvanõrkust aegsasti ära, peab operaator tagama, et kriitilise võrguelemendi komponentide tootja või tarnija kohustub lepinguliselt teavitama operaatorit viivitamata tuvastatud haavatavusest ja riskide vähendamise meetmetest ning andma nõu kaitse- või parandusmeetmete kohta, mida operaator saab ohule reageerimiseks kasutusele võtta.

(4) Operaator kontrollib vähemalt kord aastas kriitilise tähtsusega võrguelementidele juurdepääsuõiguste piisavust või ajakohastab neid viivitamata vastavalt muudatustele organisatsioonis või kolmanda tasandi tugiteenuste osutajate poolt.

(5) Kui see on tehniliselt teostatav ja majanduslikult jätkusuutlik, peab operaator vältima sõltuvust üksikust tarnijast või kolmanda taseme teenuseosutajast (st „tarnijaga seotusest“), et vähendada sõltuvust ja suurendada vastupanuvõimet kriitilise tähtsusega komponentide haavatavuste korral, muu hulgas vältides pikaajalisi lepinguid üksikute tootjate või tarnijate või kolmanda tasandi tugiteenuste osutajatega või võimaldades neid muuta, et viia kriitilise tähtsusega üksustele teenuste osutamise katkestused miinimumini.

Artikkel 7
(Lepingutingimused tootjate, tarnijate või kolmanda tasandi tugiteenuste osutajatega)

Kõrge turvalisuse taseme tagamiseks lisab operaator tootjate, tarnijate või kolmanda taseme tugiteenuste osutajatega uutesse lepingutingimustesse vähemalt järgmise:

1. tootja või tarnija kinnituse selle kohta, et komponendil või selle vaikeseadetel ei ole dokumenteerimata juurdepääse ega mis tahes negatiivset mõju kriitilise tähtsusega üksuste toimimisele;
2. tootja, tarnija või kolmanda taseme teenuseosutaja kohustuse kaitsta andmeid, millega nad tutvusid teenuste osutamise või neile juurdepääsu andmise ajal seoses juurdepääsuteenuse osutamisega;
3. tootja, tarnija või kolmanda taseme teenuseosutaja kohustuse teavitada operaatorit viivitamata sideandmete või liiklusandmete kaitse rikkumistest, mis mõjutavad või võivad mõjutada käesoleva üldakti artikli 1 punktis 1 osutatud operaatorit või kriitilise tähtsusega üksusi;
4. tootja, tarnija või kolmanda taseme teenuseosutaja kohustuse teavitada operaatorit viivitamata igast turvaintsidendist ja turvanõrkustest, mis võivad mõjutada operaatori võrgu, sellega seotud teenuste või andmete turvalisust;
5. tootja, tarnija või kolmanda taseme teenuseosutaja kohustuse järgida operaatori kehtestatud turbestandardeid ja -eeskirju ning võtta asjakohaseid turvameetmeid, et tagada infosüsteemide ja -võrkude ning operaatori või kriitilise tähtsusega üksuse andmete turvalisus;

6. operaatori suutlikkuse vaadata igal ajal üle kolmanda tasandi tugiteenuse osutaja poolt operaatori võrgule ja andmetele juurdepääsul kasutatavad keskkonnad, protseduurid, turvameetmed ja -vahendid;
7. tootja, tarnija või kolmanda taseme tugiteenuste osutaja vastutuse kahju eest, mille põhjustaks leitud haavatavus või kriitilise tähtsusega võrguelementide komponentide väärkasutamine, nende vaikeseade või kolmanda taseme tugiteenuste osutamise ajal, mille tootja või tarnija või kolmanda taseme tugiteenuse osutaja jättis tähelepanuta või mida ta tahtlikult rakendas;
8. kohustuse koolitada korrapäraselt tootja või tarnija või kolmanda taseme tugiteenuste osutaja töötajaid andmeturbe ja infosüsteemide ja -võrkude valdkonnas.

Artikkel 8
(Kriitiliste võrguelementide juurdepääsetavust ja kasutamist käsitlevad eeskirjad)

(1) Kui operaator kasutab füüsiliselt või loogiliselt juurdepääsu kriitiliste võrguelementide komponentidele, nende seadistustele ja operaatori salvestatud, töödeldud või muudetud andmetele, peab ta tagama, et:

1. juurdepääs on rangelt piiratud isikutega, kellele on eelnevalt luba antud;
2. operaator kontrollib kõiki kohapealseid või kaugjuurdepääsu kaudu kriitilisi võrguelemente käsitlevaid töid;
3. kasutajate puhul, kellele on antud kõrgeimad õigused juurdepääsuks kriitiliste võrguelementide üksikutele komponentidele, nende seadetele või seal salvestatud või töödeldud andmetele, kasutatakse mitmeteguriilist autentimist;
4. igal volitatud isikul, kellele juurdepääs antakse, on kordumatu kasutajakonto ja parool;
5. kasutatakse ainult selliseid paroole, mida muudetakse korrapäraselt või kohe kui avastatakse väärkasutamine, ja mis sisaldavad vähemalt 15 tähemärki, suur- ja väiketähti, numbreid ja erimärke, kui tarkvara seda võimaldab;
6. võimaluse korral rakendatakse juurdepääsul nulltolerantsi või -usalduse põhimõtet;
7. volitatud kasutaja sideühenduse turvalisus üksikute komponentidega on kaitstud krüpteerimisega, võttes arvesse uusimaid tehnoloogilisi arenguid ja parimaid tööstuslikke häid tavasid infoturbe valdkonnas, või kui seda soovitavad loodud institutsioonid infoturbe valdkonnas;
8. juurdepääsud ja juurdepääsukatsed registreeritakse kustutamatult ja säilitatakse vähemalt kuus kuud koos varukoopiaga, kuid mis võib olla ka pikem, kui riskijuhtimise analüüs ja vastuvõetava riskitaseme hindamine näitavad, et riske tuleks asjakohaselt juhtida, säilitades logisid pikema aja jooksul;
9. võimaluse korral salvestatakse ja jälgitakse kõiki komponentidega seotud tarkvarasekkumisi, sealhulgas konfiguratsioonimuudatusi. Andmeid, sealhulgas nende andmete varukoopiat, säilitatakse eelmises punktis märgitud aja jooksul;
10. juurdepääs üksikutele komponentidele ja neis säilitatavatele või töödeldud andmetele on ajaliselt piiratud ja avatud ainult vajaliku töö ajaks.

(2) Kui töötajad või kolmanda tasandi tugiteenuse osutaja töötajad saavad juurdepääsu kriitiliste võrguelementide üksikutele komponentidele, peavad nad:

1. kasutama ainult turvalist spetsiaalset vahetööjaama (hüppeserverit), millele tehakse korrapäraseid turvakontrolle;

2. paigaldama spetsiaalsesse tööjaama ainult hädavajalikud vahendid, komponendid ja aktiivsed teenused juurdepääsuks võrgu muudele ressurssidele, mis on hädavajalikud ja mida tuleb ajakohastada uusimate turvapaikadega;
3. kasutama turvalisi krüptooperatsioone ja võtmeid spetsiaalses tööjaamas, mis peab asuma operaatori võrgus ja olema tema ainukontrolli all;
4. operaator kiidab iga juurdepääsu heaks ja aktiveerib selle käsitsi ja ainult juurdepääsu kestuse ajaks;
5. operaator kontrollib ja registreerib füüsiliselt kõiki juurdepääse ja tegevusi;
6. kasutama kahetegurilist autentimist ja paroole, mis on vähemalt 15 tähemärki pikad ning sisaldavad suur- ja väiketähti, numbreid ja erimärke, mida muudetakse vastavalt hinnatud riskidele.

(3) Enne kui operaator annab kriitilise tähtsusega võrguelementide või nende üksikkomponentide haldamise, hooldamise või ajakohastamise teenuse üle kolmandale isikule, kontrollib ta ja tagab, et tal on oma mehhanismide ja protsessidega võrreldes vähemalt samad või paremad turbemehhanismid ja turbehalduse protsessid. Ta teavitab üleandmise kavatsusest viivitamata asjaomast kriitilise tähtsusega üksust, ametit ja infoturbe eest vastutavat asutust.

(4) Operaator kontrollib turvaprotsesside tegelikku seisu enne teenuse osutamise algust ja seejärel vähemalt kord aastas. Operaator säilitab andmeid kolmandate isikute tugiteenuste osutamise sisemiste läbivaatamiste ja kontrollide kohta ning säilitab neid teenuste osutamise aja jooksul ja ühe aasta jooksul pärast nende lõpetamist, kuid mitte kauem kui viis aastat.

ÜLEMINEKU- JA LÕPPSÄTE

Artikkel 9
(Üleminekusätted)

(1) Operaator teavitab ametit ja infoturbe eest vastutavat asutust kriitiliste võrguelementide olemasolevatest asukohtadest 30 päeva jooksul alates käesoleva üldakti jõustumisest.

(2) Operaator teavitab ametit ja infoturbe eest vastutavat asutust kriitiliste võrguelementide kolmanda tasandi tugiteenuste olemasolevatest asukohtadest 30 päeva jooksul alates käesoleva üldakti jõustumisest.

(3) Amet avaldab käesoleva üldakti artikli 3 lõikes 2 osutatud dokumendid esimest korda alates selle jõustumise kuupäevast.

Artikkel 10
(Jõustumine)

Käesolev üldakt jõustub kolmekümnendal päeval pärast selle avaldamist Sloveenia Vabariigi ametlikus väljaandes, mille kohaselt ettevõtjad võivad kasutada seadmeid ja jätkata kolmanda taseme tugiteenuste osutamist kuni seaduse artikli 312 lõigetes 2 ja 3 sätestatud tähtaegade möödumiseni.

Nr _____ mag. Marko Mišmaš

Ljubljana, [kuupäev] _____ direktor

EVA 2023-3150-0034

ETTEPANEK

Lisa

Kriitiliste võrguelementide ja nendega seotud infosüsteemide loetelu:

Kriitilised võrguelemendid	**Võrgu ja infosüsteemide funktsioonid**
Abonentide haldamise ja krüpteerimise mehhanismid	- Sessioonide haldamine (hääl ja andmed); - kasutajate ja seadmete autentimine võrguga; - abonentidele ja võrgukomponentidele loa andmise võtmete haldamine ja säilitamine (UICC/eUICC, digitaalsed sertifikaadid/HSM); - funktsioonid turvaliseks autentimiseks, side terviklikkuse kaitsmiseks (krüpteerimine) ning kasutajavõtmete, võrgu- ja halduskomponentide salvestamiseks; - juurdepääsuõiguste haldamine.
Vastastikune sidumine	- Veebimajutuse funktsioonid ja liidesed teistesse võrkudesse ja teenustesse.
Hallatavad võrguteenused	- Võrguteenuste registreerimine ja neile lubade andmine; - side-, asukoha- ja liiklusandmete säilitamine ja töötlemine; - võrgu- ja võrgufunktsioonide kokkupuude väliste rakenduste ja teenustega.
Virtualiseeritud võrgufunktsioonide (NFV) ja võrgu orkestratsiooni (MANO) haldamine ja orkestreerimine, sealhulgas virtualiseerimistaristu	- NFV orkestratsiooni ja konfiguratsiooni juhtimisfunktsioonid, olenemata rakendamise liigist (VM, konteiner, mikroteenused); - virtualiseerimisfunktsioonid NFV rakendamiseks ja kasutamiseks; - võrgu lõikude valiku funktsioon (NSSF).
Raadio juurdepääsuvõrk	- Tugijaamad, mis toetavad 5G- või kõrgemat tehnoloogiat.
Juhtimissüsteemid ja muud tugisüsteemid	- Mobiilsidevõrgu, sealhulgas juurdepääsuosa (RAN/O-RAN) toimimise ja haldamise jälgimine; - turvasündmuste, kõrvalekallete, ohtude ja nende haldamise tuvastamise süsteemid (turvafunktsioonid, sealhulgas SIEM/SOAR).
Seaduslik pealtkuulamine	- Pädeva asutuse poolt sidesisule ja kasutajaliikluse andmetele juurdepääsu funktsioonid.