PREDLOG!

Na podlagi šestega odstavka 116. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) izdaja Agencija za komunikacijska omrežja in storitve Republike Slovenije

SPLOŠNI AKT
o dodatnih varnostnih zahtevah in omejitvah

1. člen
(vsebina splošnega akta)

Ta splošni akt določa:

1. usmeritve, ki jih morajo upoštevati operaterji mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja kritičnim subjektom, upravljavcem kritične infrastrukture z drugih področij urejanja kritične infrastrukture, kot so določeni v skladu z zakonom, ki ureja področje kritične infrastrukture (v nadaljnjem besedilu: upravljavci kritične infrastrukture), izvajalcem bistvenih storitev, kot so določeni v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: izvajalci bistvenih storitev), organom državne uprave, kot so določeni v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: organi državne uprave) oziroma nosilcem ključnih delov sistema varnosti države (v nadaljnjem besedilu: operaterji) in
2. kritične elemente omrežja in pripadajoče informacijske sisteme z njihovimi funkcionalnostmi iz šestega odstavka 116. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: zakon), kot so navedeni v prilogi, ki je sestavni del tega splošnega akta in je pripravljena v sodelovanju z organom, pristojnim za informacijsko varnost.

2. člen
(pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu, pomenijo:

1. Dobavna veriga je celotni sistem procesov, ljudi, organizacije in distribucije, ki je vključena v načrtovanje, proizvodnjo, skladiščenje, distribucijo in dobavo ter namestitev in vzdrževanje komponent kritičnih elementov omrežja, ki so nameščene v omrežju operaterja ali pri ponudniku storitev v oblaku, ki operaterju takšne storitve zagotavlja.

2. Kritični elementi omrežja so tisti omrežni elementi, funkcije, storitve in podporni informacijski sistemi v fizični, programski ali virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, kot so navedeni v prilogi tega splošnega akta.

3. Kritični subjekti so upravljavci kritične infrastrukture z drugih področij urejanja kritične infrastrukture, ki so določeni v skladu z zakonom, ki ureja področje kritične infrastrukture, izvajalci bistvenih storitev določeni v skladu z zakonom, ki ureja informacijsko varnost, organi državne uprave, določeni v skladu z zakonom, ki ureja informacijsko varnost in nosilci ključnih delov sistema varnosti države.

(2) Ostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen, kot ga določa zakon.

3. člen
(splošne usmeritve)

(1) Operaterji v dobavni verigi komponent kritičnih elementov omrežja in storitev podpore tretje ravni za te komponente v celotnem življenjskem ciklu upoštevajo najmanj naslednje usmeritve:

1. za vsakega dobavitelja izvajajo oceno tveganja z vidika dobave in potencialnih možnih vplivov s strani tretjih, združljivosti z opremo drugih proizvajalcev, kakovosti in varnosti proizvodov in z vidika potencialnih negativnih vplivov na delovanje storitev operaterja in kritičnih subjektov,
2. da je varnost vgrajena in implementirana že v zasnovi in da pogodbe vključujejo roke za odpravo zaznanih ranljivosti,
3. da so zagotovljene ključne varnostne lastnosti (razpoložljivost, zaupnost, celovitost in avtentičnost) skozi celotni življenjski cikel njihove uporabe,
4. da je varnost ter njihova neprekinjena dobava zagotovljena in je potrjeno, da podpira visoke varnostne lastnosti v skladu z mednarodno priznanimi (3GPP) in evropskimi standardi (ETSI),
5. da so usmeritve, navedene v točkah od 2 do 4 tega odstavka, preverljive v pogodbeni dokumentaciji z dobaviteljem,
6. za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana z dobavo opreme, nadomestnih delov ali storitev podpore tretje ravni,
7. da uporabljene komponente nimajo znanih aktivno zlorabljenih ranljivosti,
8. za vsakega dobavitelja se ocenjuje in upošteva tudi tveganja povezana s pravicami uporabe ključnih tehnologij, ki so potrebne za izdelavo in uporabo opreme in s tem posledično omejitve ali prekinitve pri dobavi opreme, nadomestnih delov ali za storitve podpore tretje ravni,
9. izogibanje enemu samemu dobavitelju, da se prepreči odvisnost ter zagotovi odpornost v primeru kritičnih ranljivosti komponent, katastrofalne okvare omrežja oziroma grožnje za varnost omrežij in storitev kritičnih subjektov s strani tretjih fizičnih ali pravnih oseb javnega ali zasebnega prava.

(2) Operaterji pri dobavi informacijsko-komunikacijske opreme, sistemov in storitev v celoti upoštevajo smernice Agencije Evropske Unije za kibernetsko varnost (v nadaljnjem besedilu: ENISA) in veljavnih predpisov Evropske Unije glede osnovnih varnostnih zahtev pri naročanju varnih proizvodov in storitev s področja informacijsko-komunikacijskih tehnologij (npr.: angl. »Indispensable baseline security requirements for the procurement of secure ICT products and services«; verzija 1.0, december 2016 ali novejša).

(3) Pri dobavi komponent kritičnih elementov omrežja ali uporabi storitev v oblaku se prednostno izbirajo komponente tistih dobaviteljev oziroma storitve ponudnikov storitev v oblaku, ki so bili certificirani s strani organov za ugotavljanje skladnosti, ki so bili akreditirani in po potrebi pooblaščeni na podlagi člena 60(3) Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (v nadaljnjem besedilu: Uredba), za izdajo evropskih certifikatov kibernetske varnosti na določenih ravneh zanesljivosti, kot jih določa 52. člen Uredbe.

(4) Za namen iz prejšnjega odstavka operater preverja posebno spletišče, ko ga vzpostavi ENISA v skladu s 55. členom Uredbe, namenjeno informiranju in obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost, evropskih certifikatih kibernetske varnosti in izjavah EU o skladnosti, vključno z informacijami v zvezi z evropskimi certifikacijskimi shemami za kibernetsko varnost, ki niso več veljavne, odvzetimi in poteklimi evropskimi certifikati kibernetske varnosti in izjavami EU o skladnosti ter repozitorijem povezav do informacij o kibernetski varnosti.

4. člen
(ocenjevanje tveganosti)

(1) Operater pri ugotavljanju tveganosti dobavitelja komponent in ponudnika storitev tretje ravni za kritične elemente omrežja upošteva tako tehnične kot netehnične vidike tveganosti, ki jih vrednoti.

(2) Pri vrednotenju tehničnih vidikov tveganosti dobavitelja iz prejšnjega odstavka operater ocenjuje in upošteva vsaj:

1. celotno kakovost (vključno z varnostnimi vidiki) in zmogljivosti,
2. raven uporabe odprtih standardov in vmesnikov, ki preprečujejo odvisnost in vezanost na produkte posameznega dobavitelja (t.i. angl. »vendor lock–in«),
3. skladnost s priznanimi mednarodnimi in evropskimi standardi (3GPP, ETSI) in privzetimi varnostnimi nastavitvami v skladu s priporočili stroke (Združenje GSMA),
4. raven združljivosti z opremo in omrežnimi funkcijami drugih proizvajalcev,
5. proces upravljanja z ranljivostmi, njihovim razkritjem in ažurnost s posodobitvami in popravki,
6. razpoložljivost in transparentnost dokumentacije glede:
   - ključnih funkcij in informacij o varnostnih in drugih lastnostih komponente in možnih nastavitvah ter
   - uporabljene programske opreme, vključno z odprto kodo (kosovnica – SBOM),
7. zmožnost lastnega upravljanja in vzdrževanja oziroma stopnjo odvisnosti od storitev podpore tretje ravni,
8. predhodno presojo skladnosti opreme s strani v Evropski uniji akreditiranih organov po evropskih certifikacijskih shemah s področja kibernetske varnosti, pri čemer so akreditirani organi objavljeni v Uradnem listu Evropske unije.

(3) Pri vrednotenju netehničnih vidikov tveganosti iz prvega odstavka operater ocenjuje in upošteva glede na javno dostopne podatke vsaj:

1. zmožnost dobavitelja oziroma ponudnika storitev podpore tretje ravni, da varuje podatke o prometu in komunikacijske podatke in onemogoča nepooblaščen dostop do njih,
2. zmožnost dobavitelja oziroma ponudnika storitev podpore tretje ravni, da zagotavlja neprekinjenost dobave dodatnih komponent kritičnih elementov omrežja ali vzdrževanje obstoječih oziroma izvajanje storitev podpore tretje ravni,
3. transparentnost pri zagotavljanju kibernetske varnosti.

(4) Operater dokumentira dejavnike tveganj in rezultate vrednotenja tveganj za vsakega izbranega dobavitelja iz prvega odstavka tega člena in to redno posodablja.

5. člen
(splošne usmeritve glede delovanja kritičnih elementov omrežja)

(1) Komponente kritičnih elementov omrežja, njihovo delovanje in privzete nastavitve ne smejo vsebovati tehničnih značilnosti, ki bi lahko negativno vplivale na varnost ali na delovanje kritičnih subjektov, med drugim zaradi sabotaž, vohunjenja, kraje intelektualne lastnine ali terorizma.

(2) Kritični elementi omrežja se praviloma nahajajo v Republiki Sloveniji oziroma, ob upoštevanju vseh varnostnih tveganj in ob zagotavljanju visoke ravni varnostnih ukrepov in če to z veljavnimi predpisi ni določeno drugače, v Evropski uniji. Operater obvesti Agencijo za komunikacijska omrežja in storitve Republike Slovenije (v nadaljnjem besedilu: agencija) in organ pristojen za informacijsko varnost o njihovi nameravani selitvi vsaj 30 dni pred selitvijo.

(3) Storitve podpore tretje ravni za kritične elemente omrežja se praviloma izvajajo v Republiki Sloveniji oziroma, ob upoštevanju vseh varnostnih tveganj in ob zagotavljanju visoke ravni varnostnih ukrepov in če to z veljavnimi predpisi ni določeno drugače, v Evropski uniji. Operater obvesti agencijo in organ pristojen za informacijsko varnost o njihovi nameravani selitvi vsaj 30 dni pred selitvijo.

(4) Izvajanje storitev podpore tretje ravni ne sme ogroziti varnosti ali delovanja storitev kritičnih subjektov oziroma nacionalne varnosti.

(5) Operater mora vzpostaviti in redno izvajati proces prepoznave kritičnih elementov omrežja. Ta se mora izvajati vsaj enkrat letno oziroma ob nabavi komponent kritičnih elementov omrežja.

(6) Če posamezna komponenta le delno predstavlja kritični element omrežja, se šteje kot del kritičnega elementa omrežja.

(7) Operater vodi ažuren seznam vseh komponent kritičnih elementov omrežja, njihovih funkcij, lokacij, skrbnikov in upravljalcev, njihovih ponudnikov storitev podpore tretje ravni in njihovih dobaviteljev. Na zahtevo mora biti seznam dostopen agenciji in organu, pristojnemu za informacijsko varnost.

6. člen
(varnostni ukrepi pri dobavi komponent kritičnih elementov omrežja)

(1) Operater mora biti seznanjen s celotno dobavno verigo in tveganji v povezavi z njo, vključno s podizvajalci posameznih komponent kritičnih elementov omrežja, kar vključuje tudi šifrirne ključe, UICC/eUICC in druge varnostne elemente, katera zloraba bi lahko ogrozile varnost kritičnih subjektov.

(2) Operater zagotovi, da so varnostne zahteve med njim in dobavitelji komponent kritičnih elementov omrežja oziroma njegovimi ponudniki storitev podpore tretje ravni pogodbeno dogovorjene in dokumentirane in zahteva od dobaviteljev, da dogovorjene varnostne ukrepe spoštujejo skozi celotno dobavno verigo.

(3) Z namenom, da se pravočasno prepreči izraba ranljivosti s strani zlonamernih akterjev, operater zagotovi, da se dobavitelj komponent kritičnega elementa omrežja pogodbeno

zaveže, da bo o zaznani ranljivosti ter o ukrepih za zmanjšanje tveganj takoj obvestil operaterja in svetoval glede zaščitnih ali popravnih ukrepih, ki jih lahko operater sprejme kot odziv na grožnjo.

(4) Operater vsaj enkrat letno preverja ustreznost dostopnih pravic na kritičnih elementih omrežja oziroma jih nemudoma posodobi v skladu s spremembami v organizaciji ali na strani ponudnikov storitev podpore tretje ravni.

(5) Operater preprečuje svojo odvisnost od posameznega dobavitelja oziroma ponudnika storitev tretje ravni (t.i. angl. »vendor lock–in«) tudi z izogibanjem dolgoročnim pogodbam s posameznim dobaviteljem oziroma ponudnikom storitev podpore tretje ravni oziroma ima možnost njune menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnim subjektom na najmanjšo možno raven.

7. člen
(pogodbena določila z dobavitelji oziroma ponudniki storitev podpore tretje ravni)

Z namenom zagotavljanja visoke ravni varnosti, operater v nova pogodbena določila z dobavitelji komponent kritičnih elementov omrežja, in ponudniki storitev podpore tretje ravni vključi najmanj:

1. izjavo dobavitelja, da komponenta ali njene privzete nastavitve nimajo nedokumentiranih stranskih vrat ali kakršnega koli negativnega vpliva na delovanje kritičnih subjektov,
2. zavezo dobavitelja oziroma ponudnika storitev tretje ravni k varovanju podatkov, s katerimi se pri opravljanju storitev seznani ozirom do njih v zvezi z opravljanjem storitve dostopa,
3. zavezo dobavitelja oziroma ponudnika storitev podpore tretje ravni k takojšnjemu obveščanju operaterja v primeru kršitev varstva komunikacijskih podatkov ali podatkov o prometu, ki vpliva ali bi lahko vplivala na operaterja ali na kritične subjekte iz prve točke prvega člena tega splošnega akta,
4. zavezo dobavitelja oziroma ponudnika storitev podpore tretje ravni k takojšnjemu obveščanju operaterja o vsakem varnostnem incidentu in ranljivostih, ki bi lahko vplival na varnost omrežja, pripadajočih storitev ali podatkov operaterja,
5. zavezo dobavitelja oziroma ponudnika storitev podpore tretje ravni k upoštevanju varnostnih standardov in pravil, ki jih določi operater in sprejemanju ustreznih varnostnih ukrepov pri zagotavljanju varnosti informacijskih sistemov in omrežij, in podatkov operaterja ali kritičnega subjekta,
6. možnost operaterja, da kadarkoli pregleda okolja, postopke, varnostne ukrepe in orodja, ki jih uporablja izvajalec storitev podpore tretje ravni pri dostopu do omrežja in podatkov operaterja,
7. odgovornost dobavitelja oziroma ponudnika storitev podpore tretje ravni za škodo, ki bi nastala zaradi ugotovljenih ranljivosti ali zlorab komponent kritičnih elementov omrežja, njihovi privzeti nastavitvi ali pri izvajanju storitev podpore tretje ravni, ki jih je dobavitelj oziroma ponudnik podpore tretje ravni zanemaril ali namenoma izvedel,
8. obveznost rednega usposabljanja osebja dobavitelja oziroma ponudnika storitev podpore tretje ravni s področja varnosti podatkov ter informacijskih sistemov in omrežij.

8. člen
(pravila glede dostopov in uporabe kritičnih elementov omrežja)

(1) Pri fizičnem ali logičnem dostopu do komponent kritičnih elementov omrežja, njihovih nastavitev ter podatkov operaterja, ki se v njih shranjujejo ali obdelujejo, operater zagotovi, da:

1. je dostop strogo omejen le na osebe, ki so predhodno avtorizirane,
2. se izvaja večfaktorsko preverjanje pristnosti uporabnikov, ki so jim dodeljeni najvišji privilegiji pravic za dostop do posameznih komponent kritičnih elementov omrežja, njihovih nastavitev ali do podatkov, ki so tam shranjeni ali se tam obdelujejo,
3. ima vsaka pooblaščena oseba, ki ji je dodeljena pravica za dostop, unikaten uporabniški račun in geslo,
4. se uporablja samo gesla, ki se menjajo redno oziroma takoj v primeru ugotovljene zlorabe in vsebujejo najmanj 15 znakov in vključujejo velike in male črke, številke in posebne znake, če programska oprema to omogoča,
5. se pri dostopih izvaja koncept ničelne tolerance oziroma zaupanja, kjer je to možno,
6. je varnost komunikacijske povezave od pooblaščenega uporabnika do posameznih komponent zaščitena z uporabo šifriranja ob upoštevanju najnovejšega tehnološkega razvoja in najboljših industrijskih dobrih praks s področja informacijske varnosti oziroma jih priporočajo uveljavljene institucije s področja informacijske varnosti,
7. se izvaja neizbrisno beleženje dostopov in poskusov dostopov, ki se hrani vsaj 12 mesecev, vključno z varnostno kopijo,
8. se izvaja beleženje in nadzor vseh programskih posegov nad komponentami, kjer je to mogoče, vključno s spremembami konfiguracij. Zapisi se hranijo vsaj 12 mesecev, vključno z varnostno kopijo,
9. so dostopi do posameznih komponent in do podatkov, ki so na njih shranjeni ali se na njih obdelujejo, časovno omejeni in odprti samo za čas potrebnih del.

(2) V primeru dostopa do posameznih komponent kritičnih elementov omrežja s strani osebja oziroma zaposlenih pri ponudniku storitev podpore tretje ravni se:

1. uporablja samo varna posredniška namenska delovna postaja (angl. »Jump server«), ki se redno varnostno pregleduje,
2. na namenski delovni postaji namešča le nujno potrebna orodja, komponente in aktivne storitve za dostop do drugih virov v omrežju, ki so nujno potrebne in morajo biti posodobljene z zadnjimi varnostnimi popravki,
3. na namenski delovni postaji, ki se mora nahajati v omrežju operaterja in je izključno pod njegovim nadzorom, uporablja varne kriptografske operacije in ključe,
4. vsak dostop ročno in le za čas trajanja dostopa odobri in aktivira s strani operaterja,
5. vsi dostopi in aktivnosti fizično nadzorujejo in beležijo s strani operaterja,
6. uporablja dvofaktorsko avtentikacijo in gesla, ki vsebujejo najmanj 15 znakov in vključujejo velike in male črke, številke in posebne znake, ki jih menja glede na ocenjena tveganja.

(3) Preden operater prenese storitev upravljanja, vzdrževanja ali posodabljanja kritičnih elementov omrežja ali njihovih posameznih komponent na tretjo osebo, preveri in zagotovi, da so pri njej vzpostavljeni vsaj enaki ali boljši varnostni mehanizmi in procesi upravljanja z varnostjo, kot jih ima vzpostavljene sam. O nameri prenosa nemudoma obvesti kritični subjekt ter agencijo in organ pristojen za informacijsko varnost.

(4) Operater preveri dejansko stanje varnostnih procesov pred začetkom izvajanja storitev in nato vsaj enkrat letno. Operater o notranjih pregledih in nadzorih nad izvajanjem storitev podpore tretjih oseb vodi zapise in jih hrani za čas trajanja izvajanja storitev in še eno leto po njihovem prenehanju, vendar največ pet let.

PREDLOG!

PREHODNA IN KONČNA DOLOČBA

9. člen
(prehodna določba)

(1) Operater o obstoječih lokacijah kritičnih elementov omrežja obvesti agencijo in organ pristojen za informacijsko varnost v roku 30 od uveljavitve tega splošnega akta.

Operater o obstoječih lokacijah izvajanja storitev podpore tretje ravni za kritične elemente omrežja obvesti agencijo in organ pristojen za informacijsko varnost v roku 30 od uveljavitve tega splošnega akta.

10. člen
(začetek veljavnosti)

Ta splošni akt začne veljati trideseti dan po objavi v Uradnem listu Republike Slovenije, pri čemer lahko operaterji uporabljajo opremo in ohranijo zagotavljanje storitev podpore tretje ravni do izteka rokov, določenih v 2. in 3. odstavku 312. člena zakona.

Št. _____ mag. Marko Mišmaš

Ljubljana, dne _____ direktor

EVA _____

Priloga

Seznam, kritičnih elementov omrežja in pripadajočih informacijskih sistemov:

Kritični elementi omrežja	**Funkcionalnosti omrežja in informacijskih sistemov**
Upravljanje z naročniki in šifrirni mehanizmi	– Upravljanje s sejami (govor in podatki), – Avtentikacija uporabnikov in opreme z omrežjem, – Upravljanje in hramba ključev za avtorizacijo naročnikov in omrežnih komponent (UICC/eUICC, digitalna potrdila/HSM), – Funkcije za varno avtentikacijo, varovanje celovitosti komunikacije (šifriranje) in shranjevanje uporabniških ključev, komponent omrežja in upravljanja, – Upravljanje dostopnih pravic.
Medomrežno povezovanje	– Funkcije gostovanja in vmesniki do drugih omrežij in storitev
Upravljane omrežne storitve	– Registracija in avtorizacija omrežnih storitev, – Hramba in obdelava komunikacijskih, lokacijskih in prometnih podatkov, – Izpostavljenost omrežja in omrežnih funkcij zunanjim aplikacijam in storitvam.
Upravljanje in orkestracija virtualiziranih omrežnih funkcij (NFV) in omrežna orkestracija (MANO), vključno z virtualizacijsko infrastrukturo	– Upravljavske funkcije orkestracije in konfiguracije NFV ne glede na tip implementacije (VM, kontejner, mikro-storitve), – Virtualizacijske funkcije za izvedbo in uporabo NFV, – Funkcije izbire in uporabe omrežne rezine (NSSF).
Radijsko dostopovno omrežje	– Bazne postaje, ki podpirajo tehnologijo 5G ali višje.
Upravljavski sistemi in drugi podporni sistemi	– Nadzor delovanja in upravljanja mobilnega komunikacijskega omrežja, vključno z dostopovnim delom (RAN/O-RAN), – Sistemi zaznavanja varnostnih dogodkov, anomalij, groženj in njihovo upravljanje (varnostne funkcije vključno s SIEM/SOAR).
Zakonito prestrezanje	– Funkcije dostopa do vsebine komunikacije in podatkov o prometu uporabnikov s strani pristojnega organa.