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)

(1) Ta splošni akt določa:

1. usmeritve, ki jih morajo upoštevati in izvajati operaterji mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja kritičnim subjektom in operaterji, ki upravljajo z zasebnimi omrežji za potrebe kritičnih subjektov (v nadaljnjem besedilu: operaterji) , pri oceni tveganj, ki izhajajo iz odnosov in dogovorov s proizvajalci oziroma dobavitelji (v nadaljnjem besedilu: dobavitelji) informacijskih sistemov in omrežne opreme (v nadaljnjem besedilu: oprema) ter tveganj, ki izhajajo iz storitev podpore tretje ravni, ki jih tem operaterjem zagotavljajo ponudniki storitev podpore tretje ravni (v nadaljnjem besedilu: ponudniki storitev tretje ravni) in
2. seznam kritičnih sredstev, ki vsebuje kategorije posameznih kritičnih sredstev in njihove funkcionalnosti in je določen v prilogi, ki je sestavni del tega splošnega akta.

(2) Ta splošni akt določa dodatne varnostne zahteve, ki veljajo za operaterje. Ostale varnostne zahteve so opredeljene v zakonu, ki ureja elektronske komunikacije ter v splošnem aktu, ki ureja varnosti omrežij, storitev in podatkov.

2. člen
(pomen izrazov)

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

1. Dobavna veriga je celotni ekosistem procesov, ljudi, organizacije in distribucije, ki je vključena v načrtovanje, proizvodnjo, skladiščenje, distribucijo in dobavo, namestitev, vzdrževanje kritičnih sredstev, ki so nameščena v omrežju operaterja ali pri ponudniku storitev v oblaku, ki operaterju takšne storitve zagotavlja.
2. Kritična sredstva so sredstva, ki vključujejo elemente, funkcije ter storitve omrežja ter podporni informacijski sistemi v fizični, programski ali kakršni koli virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, ki operaterju takšne storitve zagotavlja, katerih potencialna odpoved ali zloraba bi lahko imela zelo velik negativni vpliv na razpoložljivost, avtentičnost, celovitost ali zaupnost v njih shranjenih, prenesenih ali obdelanih podatkov ali podatkov, ki so prek njih dostopni ter s tem ogrozila varnost in nemoteno delovanje storitev kritičnih subjektov ali na varnost in nemoteno delovanje zasebnih omrežij kritičnih subjektov ali bi kako drugače pomembno ogrozila vitalne gospodarske ali družbene aktivnosti države oziroma njeno nacionalno varnost.
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.

4. Zasebno omrežje je elektronsko komunikacijsko omrežje, ki ni javno dostopno.

(2) Ostali izrazi uporabljeni v tem splošnem aktu imajo pomen, kot ga določa Zakon o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: zakon).

3. člen
(splošne usmeritve)

(1) Operaterji v dobavni verigi kritičnih sredstev in storitev podpore tretje ravni v celotnem življenjskem ciklu zagotavljajo in upoštevajo najmanj naslednje usmeritve:

1. za vsakega dobavitelja kritičnega sredstva ali ponudnika storitev tretje ravni izvajajo oceno tveganja z vidika lastništva, dobave, združljivostjo 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) kritičnih sredstev skozi celotni življenjski cikel njihove uporabe;
4. da je varnost kritičnih sredstev ter njihova 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 potencialnega dobavitelja kritičnega sredstva iz seznama v prilogi se ocenjuje in upošteva tudi tveganja glede njegove dostopnosti do potrebnih surovin, polprevodnikov, pravic 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;
7. izogibanje enemu samemu dobavitelju, da se prepreči odvisnost ter zagotovi odpornost v primeru kritičnih ranljivosti sredstev, 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 (primer: »Indispensable baseline security requirements for the procurement of secure ICT products and services«; verzija 1.0, december 2016 ali novejša).

(3) Pri dobavi kritičnih sredstev ali uporabi storitev v oblaku se prednostno izbirajo sredstva tistih dobaviteljev oziroma storitve ponudnikov storitev v oblaku, ki so prestala varnostna testiranja in so certificirana glede na namen uporabe s strani evropskih akreditiranih organov za preverjanje skladnosti in uveljavljenih evropskih certifikacijskih shem kibernetske varnosti (npr. EUCC, EU5G in EUCS).

4. člen
(ocenjevanje tveganosti)

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

(2) Pri vrednotenju tehničnih vidikov tveganosti dobavitelja kritičnega sredstva oziroma ponudnika storitev podpore tretje ravni iz prejšnjega odstavka operater ocenjuje in upošteva vsaj:

1. celotno kakovost (vključno z varnostnimi vidiki) in zmogljivosti kritičnih sredstev ali storitev podpore tretje ravni,
2. raven uporabe odprtih standardov in vmesnikov, ki preprečujejo odvisnost in vezanost na produkte posameznega dobavitelja kritičnih sredstev (t.i. »vendor lock–in«),
3. skladnost s priznanimi mednarodnimi in evropskimi standardi (3GPP, ETSI) in privzetimi varnostnimi nastavitvami v skladu s priporočili stroke (GSMA),
4. raven združljivosti z opremo in omrežnimi funkcijami drugih proizvajalcev,
5. način upravljanja razvoja kritičnega sredstva skozi celotno življenjsko obdobje,
6. način upravljanja z varnostjo,
7. proces upravljanja z ranljivostmi, njihovim razkritjem in ažurnost s posodobitvami in popravki,
8. razpoložljivost in ažurnost dokumentacije glede:
   - ključnih funkcij in informacij o varnostnih in drugih lastnostih kritičnega sredstva in možnih nastavitvah
   - uporabljene programske opreme, vključno z odprto kodo (kosovnica – SBOM),
9. zmožnost lastnega upravljanja in vzdrževanja kritičnega sredstva oziroma stopnja odvisnosti od storitev podpore tretje ravni,
10. predhodna presoja skladnosti opreme s strani v Evropski uniji akreditiranih organov po evropskih certifikacijskih shemah s področja kibernetske varnosti,

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

1. dobaviteljevo poslovno prakso oziroma poslovno prakso ponudnika storitev podpore tretje ravni,
2. zmožnost dobavitelja oziroma ponudnika storitev tretje ravni, da zagotavlja neprekinjenost dobave dogovorjenih kritičnih sredstev oziroma storitev podpore tretje ravni, tudi glede na nacionalne in evropske usmeritve in potencialne omejitve,
3. dobaviteljevega ugleda oziroma ugleda ponudnika storitev tretje ravni glede zagotavljanja kibernetske varnosti ter transparentnosti.

(4) Operater dokumentira dejavnike tveganj in rezultate vrednotenja tveganj za vsakega izbranega dobavitelja kritičnega sredstva oziroma za ponudnika storitev tretje ravni in to redno posodablja.

5. člen
(splošne usmeritve glede kritičnih sredstev)

(1) Kritična sredstva, njihovo delovanje in 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) Kritična sredstva so praviloma nameščena v Republiki Sloveniji oziroma ob upoštevanju vseh varnostnih tveganj in ob zagotavljanju visoke ravni varnostnih ukrepov in kjer to z veljavnimi predpisi ni določeno drugače, v Evropski uniji. Če se kritično sredstvo iz seznama v prilogi nahaja izven Republike Slovenije in ga ima namen operater preseliti oziroma uporabiti izven nje, mora operater o tej nameri nemudoma obvestiti kritični subjekt iz tretje točke prvega odstavka drugega člena tega splošnega akta ter agencijo in organ pristojen za informacijsko varnost ter predhodno pridobiti soglasje organa pristojnega za informacijsko varnost.

(3) Storitve podpore tretje ravni za kritična sredstva iz prejšnjega odstavka se praviloma izvajajo v Republiki Sloveniji oziroma ob upoštevanju vseh varnostnih tveganj in ob zagotavljanju visoke ravni varnostnih ukrepov in kjer to z veljavnimi predpisi ni določeno drugače, v Evropski uniji. Za prenos storitve podpore tretje ravni izven Evropske unije mora operater o tej nameri nemudoma obvestiti subjekte iz prejšnjega odstavka ter predhodno pridobiti soglasje organa pristojnega za informacijsko varnost.

(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 sredstev. Ta se mora izvajati vsaj enkrat letno oziroma ob vseh večjih spremembah na trgu, ki bi lahko vplivala na varnost kritičnih subjektov oziroma na nacionalno varnost. Pri procesu prepoznave se morajo upoštevati vsa sredstva operaterja, ki omogočajo delovanje, upravljanje nadzor in varnost njegovega omrežja in storitev, ki jih zagotavlja kritičnim subjektom.

(6) Če posamezni element omrežja izvaja kritično funkcijo iz seznama v prilogi samo delno ali v celoti, se identificiran (fizični ali virtualni) element oziroma oprema šteje kot kritično sredstvo.

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

6. člen
(usmeritve glede varnostnih ukrepov)

(1) Operater mora biti seznanjen s celotno dobavno verigo in tveganji v povezavi z njo, vključno s podizvajalci posameznih komponent kritičnih sredstev, kar vključuje tudi šifrirne ključe, UICC/eUICC in druge varnostne elemente, s katerimi se preverja pristnost in izvaja avtorizacijo uporabnikov, omrežnih rezin, sej ipd.

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

(3) Z namenom, da se pravočasno prepreči izraba ranljivosti s strani sovražnih akterjev, operater zagotovi, da se dobavitelj kritičnega sredstva pogodbeno zaveže, da bo o zaznani ranljivosti ter o ukrepih za zmanjšanje tveganj takoj obvestil operaterja.

(4) Operater vsaj enkrat letno preverja ustreznost dostopnih pravic na kritičnih sredstvih 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. »vendor lock–in«) tudi z izogibanjem dolgoročnim pogodbam (pet let ali več) s posameznim dobaviteljem oziroma ponudnikom storitev tretje ravni oziroma ima možnost njune menjave z namenom zmanjševanja motenj pri zagotavljanju storitev kritičnih subjektov na najmanjšo možno raven.

7. člen
(usmeritve glede pogodbenih določil z dobaviteljem oziroma ponudniki storitev podpore tretje ravni)

(1) Z namenom zagotavljanja visoke ravni varnosti, operater v pogodbena določila z dobaviteljem kritičnih sredstev in ponudniki storitev podpore tretje ravni vključi najmanj:

1. izjavo dobavitelja, da kritično sredstvo ali njegove 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, ki jih pri opravljanju storitev prejme ali 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 podatkov, 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 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, predvsem kritičnih sredstev 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 v kritičnem sredstvu, njihovi privzeti nastavitvi ali pri izvajanju storitev, ki jih je dobavitelj oziroma ponudnik podpore tretje ravni zanemaril ali namenoma izvedel,
8. obveznost rednega usposabljanja osebja dobavitelja oziroma ponudnika storitev tretje ravni s področja varnosti podatkov ter informacijskih sistemov in omrežij.

8. člen
(usmeritve glede dostopov in uporabe kritičnih sredstev)

(1) Pri fizičnem ali logičnem dostopu do omrežja in kritičnih sredstev, 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 varnostno preverjene in predhodno avtorizirane,
2. se izvaja večfaktorsko preverjanje pristnosti uporabnikov, ki so jim dodeljeni najvišji privilegiji pravic pri dostopu do omrežja, kritičnih sredstev, njihovih nastavitev ali podatkov, ki so tam shranjeni ali se tam obdelujejo,
3. ima vsaka pooblaščena oseba, ki ji je dodeljena pravica dostopa do kritičnih sredstev unikaten uporabniški račun in geslo,
4. se uporablja samo kompleksna gesla, ki se menjajo vsaj enkrat mesečno, v primeru ugotovljene zlorabe pa takoj,
5. se pri dostopu do kritičnih sredstev izvaja koncept ničelne tolerance oziroma zaupanja, kjer je to možno,
6. je varnost komunikacijske povezave od pooblaščenega uporabnika do kritičnih sredstev zaščitena z uporabo šifriranja ob upoštevanju najnovejšega tehnološkega razvoja in najboljših industrijskih varnostnih praks, ki jih priporočajo uveljavljene institucije s področja informacijske varnosti,
7. se izvaja neizbrisno beleženje dostopov in poskusov dostopov, ki se hrani na varen način vsaj 12 mesecev,
8. se izvaja beleženje in nadzor vseh aktivnosti nad kritičnim sredstvom, ki se hrani na varen način vsaj 12 mesecev,
9. so dostopi do kritičnih sredstev in podatkov, ki so tam shranjeni ali se na njem obdelujejo časovno omejeni in odprti samo za čas potrebnih del.

(2) V primeru dostopa do kritičnih sredstev s strani osebja oziroma zaposlenih ponudnikov storitev tretje ravni se:

1. uporablja samo varna posredniška namenska delovna postaja (angl. »Jump server«), ki se redno varnostno pregleduje,
2. na namenski delovni postaji nameščа le nujno potrebna orodja, komponente in aktivne storitve za dostop do drugih virov v omrežju, ki so nujno potrebne in mora biti posodobljena 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 enkratna kompleksna gesla, ki se izmenjajo na varen način.

(3) Preden operater prenese storitev upravljanja, vzdrževanja ali posodabljanja kritičnih sredstev na tretjo osebo, preveri in zagotovi, da so pri zagotavljanju storitev podpore tretje ravni vzpostavljeni vsaj enaki ali boljši varnostni mehanizmi in procesi upravljanja z varnostjo, kot jih ima vzpostavljen sam. O nameri prenosa nemudoma obvesti kritični subjekt ter agencijo in organ pristojen za informacijsko varnost, od katerega mora pred prenosom pridobiti soglasje.

(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.

9. člen
(začetek veljavnosti)

Ta splošni akt začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

Št. _____ mag. Tanja Muha

Ljubljana, dne _____ v.d. direktorja

EVA _____

PREDLOG!

Priloga

Seznam kritičnih sredstev

Kategorija	Funkcionalnost
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.
Vmesniki za medomrežno povezovanje	- Funkcije gostovanja (signalizacija prometa, izmenjava CDR zapisov, sistemi za zaznavanje zlorab), - Funkcije in poizvedbe v povezavi s prenosljivostjo številk - Vmesniki in povezave do drugih omrežij in ponudnikov vsebin
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 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, katerih sevalno območje sega na območje objektov kritične infrastrukture.
Upravljavski sistemi in drugi podporni sistemi	- Nadzor delovanja in upravljanja omrežja, vključno z dostopovnim delom (RAN/O-RAN), - Nameščanje in administracija virtualiziranih omrežij in podomrežij, - Sistemi zaznavanja varnostnih dogodkov, anomalij, groženj in njihovo upravljanje (varnostne funkcije vključno s SIEM/SOAR)
Transport in prenosne funkcije	- Transportne funkcije, ki omogočajo prenos in usmerjanje občutljivega govora in podatkov (usmerjanje, SMSC, IMS).
Zakonito prestrezanje	- Funkcije dostopa do vsebine komunikacije in meta podatkov uporabnikov s strani pristojnega organa