A1 Slovenija, d. d.
Ameriška ulica 4
1000 Ljubljana

M +386 40 40 40 40
F +386 40 44 35 99
A1.si

Agencija za komunikacijska omrežja in storitve RS
Info.box@akos-rs.si

Ljubljana, 8. 5. 2023

Zadeva: **Pripombe k predlogu Splošnega akta o dodatnih varnostnih zahtevah in omejitvah**

Zveza: **Opr. št. 0073-3/2023**

Spoštovani,

v družbi A1 Slovenija, d. d., Ameriška ulica 4, 1000 Ljubljana smo proučili predlog Splošnega akta o dodatnih varnostnih zahtevah in omejitvah. V nadaljevanju podajamo nekatere ugotovitve in pripombe.

A. Nejasnost opredelitve kritične infrastrukture upravljalcev kritične infrastrukture

Splošni akt bo veljal za operaterje, »*ki zagotavljajo ta omrežja upravljavcem kritične infrastrukture z drugih področij urejanja kritične infrastrukture, določenim v skladu z zakonom, ki ureja področje kritične infrastrukture (v nadaljnjem besedilu: upravljavci kritične infrastrukture), izvajalcem bistvenih storitev, določenih v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: izvajalci bistvenih storitev), organom državne uprave, določenim v skladu z zakonom, ki ureja informacijsko varnost (v nadaljnjem besedilu: organi državne uprave) oziroma nosilcem ključnih delov sistema varnosti države,*".

Opozarjamo, da operaterji večinoma ne vemo, kaj je kritična infrastruktura upravljalcev kritične infrastrukture (evidenca ni ažurirana, v njej so različna pojmovanja ter podjetja vpisujejo po lastni presoji), ki jim nudimo in zagotavljamo mobilna povezljivost, ni jasno, na kaj se nanaša opredelitev, da jim zagotavljamo omrežja (na splošno, za določene – kritične lokacije?), opozarjamo ponovno, da ne obstaja seznam IBS in potemtakem ni jasno, ali se te dodatne obveznosti

nanašajo na operaterja itd. – **če naj bo obveza realizirana, naj splošni akt predvidi aktivno ravnanje na strani varovanih subjektov, ki morajo biti določno opredeljeni, da naj bo precizirano, kaj pomeni „zagotavljanje omrežij", predvsem pa, da naj se ti varovani subjekti obrnejo na operaterje in zahtevajo to posebno obravnavo. Ne zadostuje opredelitev „če je operaterju znano". To je še toliko bolj pomembno zaradi obveznosti, opredeljene v 2. odstavku 5. člena.**

Poleg tega opozarjamo, da opredeljeni mobilni operaterji zagotavljajo storitve različnemu številu varovanih subjektov – nekateri operaterji le nekaterim, drugi bistveno večjemu obsegu, veljajo pa zaveze po predmetnem splošnem aktu za vse (breme je enako ne glede na obseg nudenja storitev varovanim subjektom).

B. Opredelitev kritičnih sredstev oziroma kritičnih komponent

Ugotavljamo, da so **med kritičnimi komponentami zajeti tudi dostopovni (RAN) deli omrežja** (torej same bazne postaje, njihove transportne poti in sistemi za upravljanje ter nadzor baznih postaj), **upravljavski sistemi in drugi podporni sistemi ter tudi ne transport in prenosne funkcije**. Pri pregledu različnih evropskih praks je zaslediti obe stališči glede umeščanja teh delov omrežja med kritične, torej, da dostopovno radijsko omrežje, upravljavski sistemi in drugi podporni sistemi ter transport in prenosne funkcije ne predstavljajo kritičnosti glede varnosti. So pa po drugi strani tudi države, ki te dele omrežja umeščajo med kritične. Vsekakor ima ta odločitev za operaterje dolgoročen poslovni in nenazadnje razvojni vpliv, zato mora po naši strokovni oceni regulatorna zavezujoča odločitev temeljiti na skrbnem premisleku vsake posamične države. Naj spomnimo, da velja RAN skladno z 3GPP, ki kot kritične opredeljuje samo jedrno omrežje in njegove funkcije ter upravljanje NFV ter omrežno orkestracijo, za manj občutljiv element omrežne arhitekture, upravljavski sistemi ne vplivajo na uporabnika in nimajo vpliva na dostop do omrežja ali promet, transport in prenosni sistemi pa že glede na funkcijo izvajajo le prenos ter ne nadzorujejo prometa.

Zato kot pripombo dajemo poziv, da agencija in URSIV natančneje pojasnita na čem je temeljila ta odločitev, da v prilogo umešča elemente »Radijsko dostopovno omrežje«, »Upravljavski sistemi in drugi podporni sistemi« ter »Transport in prenosne funkcije«.

C. Odvisnost od dobaviteljev

Predlog predmetnega splošnega akta med drugim predvideva tudi, da se morajo operaterji v dobavni verigi kritičnih sredstev izogibati enemu samemu dobavitelju, da se prepreči prekomerna odvisnost ter zagotovi odpornost v primeru ranljivosti, okvar oziroma groženj.

Splošni akt pri tem posega tudi neposredno v odnose z dobavitelji, saj določa konkretno vsebino, ki jo morajo vsebovati pogodbena določila. Menimo, da takšne določbe presegajo zakonsko pooblastilo za sprejem splošnega akta iz šestega odstavka 116. člena ZEKom-2. Omenjeni 116. člen daje AKOS pooblastilo za opredelitev "kritičnih elementov" omrežja in informacijskih sistemov ter tehničnih usmeritev za operaterje, ne napotuje pa na kakršno koli obliko regulacije dobavnih verig (opozarjamo na določila 120. člena Ustave o vezanosti podzakonskih predpisov na nadrejeni zakon) in tudi ne daje okvira za poseganje v pogodbena določila z dobavitelji.

Regulacija nabave komunikacijske opreme, kot je začrtana v predlogu splošnega akta, bistveno posega v odnos med dobavitelji opreme in operaterji oz. ponudniki storitev in s tem v ustavno varovano svobodo gospodarske pobude (74. člen Ustave). Skladno z Ustavo je omejevanje ali predpisovanje načina uresničevanja z Ustavo varovanih pravic ali svoboščin mogoče le z zakonom, ne pa s podzakonskim aktom. Kot navedeno že zgoraj, vsebina predlaganega splošnega akta bistveno presega materijo, ki jo opredeljuje 116. člen ZEKom-2.

D. Druge pripombe

K 6. točki 1. odstavka 3. člena ter k 4. in 5. členu:
Ta tveganja se bodo lahko preverjala le v okviru poslovnega sodelovanja ter na način, da bo operater od proizvajalca pridobil izjavo. Ni jasno, kako bo sicer lahko operater izvedel presojo vseh v 4. členu opredeljenih elementov. Vsled temu predlagamo, da se splošnemu aktu doda nova priloga, s katero naj se opredeli matrika za ocenjevanje tveganj, ki naj velja za vse operaterje, kar bo pripomoglo nenazadnje k poenotenju varnostnega pregleda in varnosti kritičnih subjektov.

K 2. odstavku 3. člena:
Ugotavljamo, da je ugotavljanje in vrednotenje tveganosti zelo zapleteno in bo brez ustreznejših navodil (prej predlagane matrike) ugotavljanje zelo otežkočeno in vprašljivo s stališča podanih parametrov. V izogib nejasnostim naj agencija in URSIV pripravita ustrezne podlage - vprašalnik, s katerimi naj operaterji ugotavljamo tveganja.

Kot že v predhodnih predlogih obeh splošnih aktov s področja varnosti omrežij, storitev in informacij, tudi na tem mestu predlagamo, da se opredelijo vse relevantne smernice, ki naj jih operaterji upoštevajo. Ta seznam se lahko opredeli bodisi kot priloga splošnega akta bodisi na način, da se ažuren seznam objavi na spletni strani agencije, se sproti posodablja ter agencija obvešča operaterje, ko pride do vsebinskih sprememb, ki vplivajo na proces dobave.

K 2. točki 1. odstavka 4. člena:

Pripominjamo, da operaterji praviloma vključujemo rešitve svetovnih proizvajalcev telekomunikacijskih rešitev, ki so v skladu z 3GPP in ETSI standardi, kar pomeni, da za komunikacijo med posameznimi elementi uporabljamo standardizirane protokole in mehanizme, posledično pa že to preprečuje vendor lock-in.

K 9. točki 1. odstavka 4. člena:
Pojasnjujemo, da se v A1 nivo podpore 1 in drugega nivoja v primeru radijskega, transportnega in jedrnega omrežja izvaja lokalno, z ekipami inženirjev, zaposlenih pri operaterju. Nivo tretje ravni je pokrit v okviru določil veljavne vzdrževalne pogodbe s posameznih dobaviteljem.

K 2. odstavku 5. člena
(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 nahaja izven Republike Slovenije in ga~~ ima operater namen kritično sredstvo iz seznama v prilogi 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.

Predlagamo tudi, da agencija in URSIV opredelita postopek izdaje soglasja, rok, v katerem se soglasje izda ali zavrne (predlagamo 8 dni). Soglasje se naj izda v upravnem postopku, opredeli naj se, da je soglasje pravni akt in zagotovi pravno sredstvo zoper soglasje oziroma zavrnitev soglasja.

K 1. točki 1. odstavka 7. člena:
Takšne klavzule običajno v že sklenjene pogodbe niso vključene in obstaja tveganje, da bi dobavitelj lahko zavrnil izdajo dodatnih izjav – tega ni bilo mogoče preveriti v času posvetovanja. Zaradi pravne varnosti štejemo, da splošni akt ne ureja vsebin retroaktivno in takšna nova določila veljajo za naprej, za vse na novo sklenjene dogovore z dobavitelji.

K 8. členu:

K 1. točki 1. odstavka: Definirati je treba do katere stopnje (zaupno, tajno,...).

K 4. točki 1. odstavka ter k 6. točki 2. odstavka: Definirati je treba natančneje kaj se šteje za kompleksna gesla oziroma določi, da je to prepuščeno operaterju.

K 5. točki 1. odstavka: Ali to pomeni, da je za vsak dostop obvezna avtentikacija uporabnika brez SSO?

K 6. točki 1. odstavka: Definirati je treba kaj so najboljše industrijske varnostne prakse, saj opozarjamo da ta kategorija v stroki ne obstaja.

K 7. točki 1. odstavka: Definirati je treba kaj je varen način – je to kriptiran, zaklenjen z zgoščevalno funkcijo,...?

K 8. točki 1. odstavka: Ni opredeljeno na kakšen način se izvaja beleženje, kar sicer pravilno pomeni, da se lahko posamični operater odloči kako bo beleženje izvajal. V tem primeru nadzorni organ ne more zahtevati spremembe beleženja. Če ni tako, naj se jasno opredeli kaj nadzorni organ pričakuje. Je pa seveda menda jasno, da je beleženje odvisno od podatkov, ki se jih pričakuje (poleg log datotek).

S spoštovanjem,

Gregor Krsmanović
Prokurist

01

A1 Slovenija, d. d.

Špela Dekleva
Višja ekspertka za regulativne in institucionalne zadeve

Poslano na elektronski naslov: info.box@akos-rs.si