



Agencija za komunikacijska omrežja in storitve RS
Stegne 7
1000 Ljubljana

Info.box@akos-rs.si

Ljubljana, 31. 3. 2023

Zadeva: Pripombe družbe A1 Slovenije na predlog Splošnega akta o varnosti omrežij, storitev in podatkov

Zveza: Opr. št. 0073-3/2023

Spoštovani,

v družbi A1 Slovenija, d. d., Ameriška ulica 4, 1000 Ljubljana smo proučili predlog Splošnega akta o varnosti omrežij, storitev in podatkov. Uvodoma ugotavljamo, da je naslovni organ 16. 3. 2023 izvedel posvet na temo predmetnega osnutka splošnega akta, za katerega smo operaterji prispevali veliko število ugotovitev, s katerimi smo opozorili na nekatere pomanjkljivosti, predvsem pa na znatno povezavo s tretjim splošnim aktom iz poglavja o varnosti (116. člen ZEKom-2), ki pa naj bi bil objavljen ter dan v javno posvetovanje šele čez en mesec. Razprava o predmetnem osnutku predloga splošnega akta je tako mestoma preuranjena ter bo v pomembnem delu (predmetni osnutek predloga splošnega akta npr. uvaja pojem kritična sredstva, poleg tega se bo zanesljivost ugotavljala s pomočjo tega tretjega splošnega akta) mogoča vsebinska presoja z oceno vpliva na posamičnega operaterja šele, ko bo objavljen tudi tretji splošni akt. Predlog, ki ga podajamo je torej, da se razprava o predmetnem osnutku predloga splošnega akta izvede po potrebi ponovno, ko bo objavljen tudi ta tretji splošni akt oziroma se omogoči komentiranje. V vsakem primeru menimo, da bi moralo biti usklajen (hkraten) začetek veljavnosti vseh treh splošnih aktov.

Nadalje ugotavljamo tudi, da predmetni osnutek predloga splošnega akta v 10. členu ureja povsem novo vsebino, glede katere trenutno na ravni države potekajo obsežne razprave, testiranja in priprave, v okviru katerih je še toliko odprtih in nerešenih vprašanj, ki pa so pravzaprav enaka, kot se postavijo pri presoji 10. člena. Poleg tega predmetni osnutek predloga splošnega akta posega v zakon o kritični infrastrukturi (ki podobne zahteve povsem pravilno nima), saj prinaša novo opredelitev kritičnosti.

Umestitev 10. člena v osnutek predloga predmetnega splošnega akta je preuranjena ter pretirana, saj menimo, da je tako podrobno urejanje povsem nepotrebno, ker operaterji problematiko, ki jo naslavlja 10. člen, že urejamo v okviru rednega poslovanja in do sedaj ni bila izpostavljena kot problematična. V

nadaljevanju bomo še nekoliko podrobneje utemeljili predlog, da se člen črta oz. poenostavi tako, da bo odražal že več kot dve desetletji vpeljane sisteme (glede katerih država do sedaj ni izrazila nikakršnega dvoma glede njihove primernosti in zadostnosti). Menimo namreč, da mora biti vsak avtoritativen poseg v svobodno delovanje operaterjev zelo dobro utemeljen in podprt s konkretno utemeljitvijo potrebe po posegu.

Splošna pripomba

Splošna pripomba, ki se nanaša na osnutek predloga splošnega akta povsod, kjer ta ureja obveznosti operaterja do Kritičnih subjektov (definirani v tč. 7, 2. člen): opozarjamo, da ne obstaja register teh subjektov. Ureditev tega registra oz. evidence ni tako preprosta, ker se s tem posega v najmanj dva zakona (ki urejata kritično infrastrukturo in informacijsko varnost), osnutek predloga splošnega akta, pa v kritične subjekte prišteva še organe državne uprave (zagotovo s tem niso mišljeni vsi organi?) ter nosilce ključnih delov sistema varnosti države.

Prosimo za pojasnilo, kako se bodo izvajala določila splošnega akta, ki imajo poseben režim za kritične subjekte.

K 3. členu

2. odstavek, 1. točka: predlagamo, da se »navedbo uporabljene metodologije« zamenja z »opis metodologije«, »(vključno z nastavitvami)« pa se črta.

Kot smo operaterji pojasnili na posvetu 16.3.2023, je primerneje in pravilneje, da se opiše tehnologija, ki bo uporabljena, glede nastavitvev pa smo se strinjali, da se te spreminjajo in bi bila to prevelika obremenitev.

2. odstavek, 4. in 5. točka: Predlagamo brisanje obeh točk, ki nista potrebni, saj sta že vključeni v metodologijo ter SUVI.

2. odstavek, 11. in 12. točka: Obe točki sta del SUNP in ne SUVI, zato predlagamo, da se brišeta kot nepotrebni.

4. odstavek: Ni povsem jasno, zakaj bi operaterji Agenciji posredovali SUVI (ali katerega od drugih dokumentov - informacijsko varnostno politiko iz 4. odstavka 4. člena), saj zadostuje, da Agencija vanj vpogleda. Gre za zaupen dokument in operater, če bi ga posredoval tretjim, pa čeprav agenciji, bi bil s tem izpostavljen dodatnemu varnostnemu tveganju, če bi politike prišle v napačne roke. Predlagamo, da se 4. odstavek spremeni in glasi: » Operater omogoči agenciji vpogled v SUVI na njeno zahtevo.«, ter se črta obveza posredovanja.

K 4. členu

2. odstavek: menimo, da je sklicevanje na konkretne standarde neprimerno in da zadostuje sklic na upoštevanje uveljavljenih standardov. Predlagamo, da se briše besedilo v oklepaju.

Prosimo tudi za pojasnilo, kakšna so pričakovanja agencije – je upoštevanje standardov, ki so navedeni, priporočljivo ali obvezno? Če agencija pričakuje upoštevanje v oklepaju navedenih standardov, naj prosimo točno opredeli, katere člene ISO standardov 27001, 27002 ter 22301 moramo upoštevati.

Prosimo še za pojasnilo, katera organizacija bo preverjala skladnost s standardom?

2. odstavek: Po posvetu z dobavitelji opreme menimo tudi, da ni primerna opredelitev, da se upoštevajo dobre prakse. Če agencija meni, da je to potrebno ohraniti, naj navede, katere dobre prakse so tu mišljene. Opozarjamo, da te prakse

strokovno niso nikjer specifično definirane, taka široka opredelitev pa glede na cilje, ki jih zasleduje predmetni splošni akt, z vidika jasnosti ni primerno in se mu je treba izogibati. Podobna dikcija je uporabljena tudi v 3. odstavku 9. člena, ki se prav tako sklicuje na neopredeljene »dobre prakse«, ne da bi opredelil, kaj te prakse so.

Predlagamo črtanje besede »praksami«.

4. odstavek: Enako, kot smo predlagali k 3. členu, 4. odstavek, predlagamo tudi na tem mestu, da se črta besedilo »ali posreduje«. Posredovanje dokumentiranih ukrepov tretjim osebam je za operaterja preveliko zunanje tveganje, poleg tega agencija po našem mnenju tega dokumenta ne rabi.

K 6. členu in k 7. členu

Pripomba ni vsebinska, saj se nanaša na uporabo pridevnikov, ki v besedilu niso potrebni, in sicer »dobro« v 1. tč. 1. odst. 6. člena in »stroga« v 1. odst. 7. člena. Obe besedi ne prineseta nobene dodane vrednosti siceršnjemu besedilu, že sama navodila 6. člena bodo poskrbela, da bo strategija »dobro« dokumentirana, navodila 7. člena pa, da bo operater pripravil »stroga« pravila dostopa.

Predlagamo, da se besedi črtata.

K 9. členu

Uvodoma smo navedli, da je/bo za razumevanje predmetnega splošnega akta, verjetno treba upoštevati tudi tretji splošni akt (116. člen ZEKom-2), ki pa bo javno objavljen šele v roku enega meseca. Predmetni splošni akt namreč ne opredeljuje razmejitve, ki jo bo verjetno prinesel pričakovani tretji splošni akt. To je zadosten razlog, da se oba splošna akta, oziroma verjetno vsi trije, obravnavajo skupaj. V konkretnem primeru to pomeni, da bi bilo z nadaljnjim sprejemom predmetnega splošnega akta treba počakati, če bo tretji splošni akt neposredno vplival na predmetnega. V tem primeru predlagamo, da se javna razprava za predmetni splošni akt začne ponovno oz. dovoli, da se predmetni splošni akt po potrebi dodatno komentira.

3. odstavek: Podobno kot smo predlagali k 2. odstavku 4. člena, predlagamo tudi na tem mestu, da se briše pojem »dobre prakse«. Če obstajajo »dobre prakse«, naj jih agencija opredeli zelo natančno. Po naši oceni te dobre prakse, vsaj da bi bile poenotene, ne obstajajo. Po mnenju stroke zadostuje sklic na splošno sprejeta aktualna priporočila stroke.

K 10. členu

Splošna pripomba: Umestitev tega določila v predmetni splošni akt bi bila razumljiva, če bi bila povezana s stanjem ogroženosti (ter zaradi situacije vezane na krizo v Ukrajini, ki se povsem predvidljivo lahko zaostri). Tveganje v zvezi z oskrbo električne energije je bilo do sedaj zanemarljivo in ne vidimo razloga, da bi se to kakorkoli spremenilo. Upravljanje je bilo dejansko vezano na zagotovitev delovanja bazne postaje v primeru izpadov, kritični elementi (vozlišča), pa so zaščitena pred nedelovanjem z ustreznim agregatnim napajanjem, ki zagotavlja več urno premostitev. Glede na urejenost tega področja ni jasno, zakaj se je agencija odločila, da to tveganje, ki ni različno od drugih tveganj, ureja s tem predmetnim splošnim aktom. Dodatno, ob vseh potekajočih izredno kompleksnih simulacijah (redukcije), ni bilo mogoče natančno in zanesljivo analizirati, kaj bi finančno pomenil predmetni splošni akt – na koliko lokacijah bi bile potrebne prilagoditve. Vsekakor pa smo mnenja, da je to tveganje še vedno minimalno in da predvsem ne potrebuje posebne ureditve, sploh ne takšne, ki vpliva na utečeno ureditev upravljana s tveganji. Predlagamo, da se člen v celoti briše.

Podredno komentiramo člen po odstavkih:

1. odstavek: A1 Slovenija že ima vzpostavljen sistem obveščanja – v celoti se sklicujemo na podatke, ki smo vam jih posredovali 23. 3. 2023 (dogovorjeno na sestanku 16.3.2023). Ali je sistem učinkovit, ne moremo oceniti, vsekakor ni popoln, to pa zato, ker imajo distributerji različne načine obveščanja, ki smo se jim prisiljeni prilagoditi. Učinkovitost bi bilo treba nasloviti neposredno pri distributerjih in urediti najmanj to, da bi bila obveščanja avtomatizirana, dostop pa omogočen preko ustreznega vmesnika (API). Druga težava, ki onemogoča učinkovitost je, da so obveščanja možna le glede lokacij z lastnimi merilnimi mesti. Ker tega podatka, kot Agencija ve, nimamo za vse lokacije, je obveščanje le delno učinkovito. Sicer se strinjamo, da je potrebna učinkovita izmenjava podatkov o izpadih, a bi moral predmetni splošni akt veljati tudi za distributerje električne energije. Ker temu ni tako, je določilo neučinkovito.

2. odstavek: Predvideno je že del neprekinjenega poslovanja operaterja in ni problematično. To pomeni, da posebno urejanje ni potrebno in se določilo lahko izbriše.

3. odstavek: Ob upoštevanju vsega navedenega, da oskrba z električno energijo ni posebno tveganje in ni razloga, da bi se to spremenilo ter pomanjkanju zanesljivih podatkov o trajanju izpadov (razpolagamo le s preliminarnimi podatki), predlagamo, da se rezervna avtonomija zniža na 1 uro oz. se sploh ne ureja, kar bi bilo primerneje, obseg uporabnikov pa poviša na 700 uporabnikov, ki so registrirani v omrežju.

4. odstavek: Ni potreben, ker je to del rednega poslovanja operaterja ter predlagamo brisanje določila.

5. odstavek: Glede na potekajoče simulacije (gl. zapisnik srečanja operaterjev z AKOS in URSIV 16. 3. 2023), je ureditev, ki je predvidena v 5. odstavku, preuranjena, poleg tega zelo verjetno skuša urejati stanje ogroženosti, ki pa je že urejeno v ZEKom-2. Predlagamo brisanje odstavka.

K 17. členu

Opozarjamo, da lahko Splošni akt o varnosti omrežij in storitev (Ur. l. RS, št. 75/13) preneha le skupaj z uveljavitvijo predvidenega Splošnega akta o poročanju in vrednotenju varnostnih incidentov (v javnem posvetovanju), če naj bodo vse obveznosti ustrezno celostno urejene (poročanje).

S spoštovanjem,

Gregor Krsmanović
Prokurist

Špela Dekleva
Višja ekspertka za regulativne in institucionalne zadeve

A1 01
A1 Slovenija, d. d.

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