



## Agencija za komunikacijska omrežja in storitve RS

Stegne 7  
1000 Ljubljana  
[info.box@akos-rs.si](mailto:info.box@akos-rs.si)

Ljubljana, 7. 4. 2023

Zadeva: **Pripombe SOEK k osnutku predloga Splošnega akta o poročanju in vrednotenju varnostnih incidentov**

Zveza: **Opr. št. 0073-1/2023**

Spoštovani,

v Sekciji operaterjev elektronskih komunikacij (SOEK<sup>1</sup>), pri Združenju za informatiko in telekomunikacije (ZIT) pri Gospodarski zbornici Slovenije (GZS) smo preučili predlog Splošnega akta o poročanju in vrednotenju varnostnih incidentov. V nadaljevanju podajamo nekaj predlogov. Ob tem dodajamo, bo operater Telekom Slovenije, d. d., svoje pripombe na splošni akt podal posebej.

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 že opozorili na nekatere pomanjkljivosti in s katerimi se je strinjal že tudi naslovni organ, kar se seveda še ne odraža v predmetnem predlogu splošnega akta.

Predmetni splošni akt ni povsem nov, saj je bila do sedaj deloma njegova vsebina že urejena v Splošnem aktu o varnosti omrežij in storitev, s čimer opozarjamo, da morata nova splošna akta (predmetni in o varnosti omrežij, storitev in podatkov) začeti veljati hkrati. Vsekakor pa se do ureditve še naprej uporablja obrazec Poročilo o incidentu varnosti in celovitosti.

### K 3. členu

Kot smo na posvetu 16. 3. 2023 navzoči operaterji opozorili, postopek priglasitve, kot je opredeljen v 3. členu ni izvedljiv. K namreč pride do incidenta operaterji izvajamo vse potrebne ukrepe, da incident identificiramo in odpravimo. Obrazec, ki ga je agencija predvidela v 4. členu je tako izjemno kompleksen, da bi v trenutku ko pride do incidenta vzel operaterju toliko časa, ko bi se operater moral ukvarjati z njegovo odpravo.

Predlagamo, da se obveznost prilagodi realnosti in se predvsem spremeni čas v katerem je operater dolžan javiti agenciji incident iz »v največ v eno uri« (v tem času še ne razpolagaš z dovolj podatki o naravi »incidenta«) in sicer v 24 ur saj dodatno opozarjamo tudi, da ni vsak izpad že tudi varnostni incident, vsekakor pa da se ne poroča po parametrih 4. člena, pač da se poročajo za incident relevantni podatki s katerimi razpolagamo takrat ko je že jasno, da je izpad tudi varnostni incident.

---

<sup>1</sup> Člani: A1 Slovenija, d.d., Telekom Slovenije, d.d., Telemach, d.o.o., HOT mobil, d.o.o., T-2, d.o.o.

*(1) Operaterji morajo brez nepotrebnega odlašanja oziroma največ v 24 urah po zaznavi varnostnega incidenta, ki pomembno vpliva na delovanje javnih komunikacijskih omrežij (v nadaljnjem besedilu omrežja) ali izvajanje javnih komunikacijskih storitev (v nadaljnjem besedilu: storitve), v skladu z merili iz prvega in drugega odstavka 4. člena tega splošnega akta, obvestiti Agencijo za komunikacijska omrežja in storitve Republike Slovenije (v nadaljnjem besedilu: agencija) in nacionalni CSIRT, če takšni varnostni incidenti vplivajo na:*

V navezavi s predlogom podanim za prvi odstavek 3. člena, kjer predlagamo, da se obveščanje varnostnega incidenta, ki pomembno vpliva na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev določi na 24 ur po zaznavi, za ostale podatke predlagamo, da se podaljša na **najkasneje 72 ur** od kar se z njimi seznanijo.

*(3) Če podatki o vplivu ali obsegu varnostnega incidenta ob zaznavi incidenta še niso znani, operater agenciji in nacionalnemu CSIRT s prvim obvestilom sporoči le tiste podatke iz četrtega odstavka 4. člena tega splošnega akta, ki so mu znani, ostale podatke pa najkasneje v 72 urah od kar se z njimi seznanijo. Operater najkasneje v desetih dneh po odpravi varnostnega incidenta poroča agenciji in nacionalnemu CSIRT ostale zahtevane informacije iz tretjega odstavka 4. člena tega splošnega akta. Če ima dogodek večdnevni pomemben vpliv na omrežje, storitve ali uporabnike, operater vsaj enkrat dnevno poroča agenciji in nacionalnemu CSIRT o dogajanju, o čemer obema v roku desetih dni po vzpostavitvi normalnega delovanja posreduje še končno poročilo.*

Predvsem pa predlagamo, da se obrazec (obstoječi – po 81. členu prej veljavnega ZEKom-1) uporablja v prehodnem obdobju, ko bo agencija vzpostavila avtomatiziran vmesnik za poročanje. Predlagamo, da se v prehodnih določbah opredeli kdaj bo ta avtomatiziran sistem na voljo operaterjem, po potrebi naj bo omogočeno tudi preizkušanje vmesnika.

Nenazadnje pa predlagamo tudi, da organi, ki morajo biti obveščeni o varnostnem incidentu, operaterjem zagotovijo kontaktne podatke, na katere naj jih obveščamo. Predlagamo da se po potrebi doda prehodna določba, s katero naj se tem organom naloži, da v roku 8 dni po uveljavitvi splošnega akta, zagotovijo potrebne podatke, o spremembi katerih nas je seveda treba ustrezno vnaprej obveščati.

#### **K 4. členu**

Ugotavljamo, da se je nabor podatkov ki naj jih operaterji poročamo organom, zelo obsežno povečal, v primerjavi s še veljavnim sistemom obveščanja. Razloga za to, operaterji na posvetu 16.3.2023 nismo izvedeli, zato pozivamo agencijo (oziroma URSIV), da ga obrazloži in pojasni čemu je takšna sprememba potrebna in na čem je utemeljena. Organi bodo zbirali obsežno količino podatkov, vprašanje ali je tak obseg zbiranja res upravičen vin ne bi bil nenazadnje obremenjujoč tudi za organe.

Prva točka 1. odstavka, točka a): Predlagamo, da se spodnja meja trajanja omeji na vsaj 15 minut in bi operaterji poročali o izpadih, ki trajajo 15 minut do 1 ure. Ta predlog smo že podali na javnem posvetu.

#### **K 5. členu**

Na splošno ocenjujemo, da določilo ni potrebno, ker je po naši oceni v nasprotju s 1. odstavkom 118. člena ZEKom-2, ki določa koga naj operaterji v primeru pomembnih incidentov obveščamo, v nasprotju z 2. odstavkom, ki določa obseg urejanja splošnega akta ter poleg tega 6. odstavek istega člena opredeljuje, da o incidentu agencija obvesti zainteresirano javnost ali pa naloži operaterju, da o incidentu obvesti javnost.

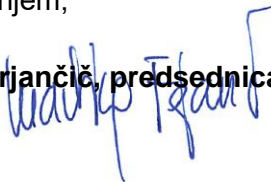
Opozarjamo, da operaterji pričakujemo še objavo splošnega akta po 208. členu ZEKom-2, ki bi utegnil to isto problematiko (obveščanje zaradi napak, ki so posledica incidenta) urediti drugače, kar bo povzročilo nepotrebno zmedo in podvajanje naših obveznosti. Obstaja pa še tretja pravna podlaga obveščanja in sicer 213. člen ZEKom-2, ki nam operaterjem nalaga, da v primeru posebnih tveganj operater takoj, ko za to tveganje izve, z objavo na svojih spletnih straneh in na drugi primeren način obvestiti naročnike o takem tveganju.

Iz besedila predloga 5. člena je tudi mogoče razumeti, da agencija s predlogom celotnega 5. člena uresničuje ureditev 6. odstavka 118. člena ZEKom-2, kar bi bilo napačno, tudi iz razloga, ker 118. člen ZEKom-2 predvideva obveščanja o pomembnih varnostnih incidentih, 5. člen predmetnega splošnega akta pa se je obveščanja razširil na vse varnostne incidente, kar je kot rečeno v nasprotju z zakonom, poleg tega pa za operaterje izredno obremenjujoče. Predlagamo črtanje 4. odstavka.

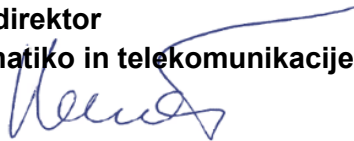
Predlagamo, da se 5. člen kot nepotreben briše oziroma preoblikuje, da bo skladen s 118. členom ZEKom-2.

S spoštovanjem,

**Martina Ferjančič, predsednica SOEK**



**Nenad Šutanovac, direktor  
Združenje za informatiko in telekomunikacije pri GZS**



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