telemach

Agencija za komunikacijska omrežja in storitve RS
Stegne 7
1000 Ljubljana

info.box@akos-rs.si

Ljubljana, 7. 4. 2023

Zadeva: **Pripombe in predlogi družbe Telemach Slovenija d.o.o. k osnutku predloga Splošnega akta o poročanju in vrednotenju varnostnih incidentov**

Zveza: **Objava na spletni strani agencije z dne 27.2.2023[1], opr. št. 0073-1/2023**

Spoštovani.

V družbi Telemach Slovenija d.o.o. (v nadaljevanju Telemach Slovenija), smo preučili objavljen osnutek Splošnega akta o poročanju in vrednotenju varnostnih incidentov, storitev in podatkov (v nadaljevanju splošni akt), ter v nadaljevanju podajamo pripombe in predloge k posameznim členom.

Prvi odstavek 3. člena

Predlagana 1 ura (po zaznavi) obveščanja varnostnega incidenta, ki pomembno vpliva na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev predstavlja za operaterje absolutno premalo časa. V kolikor se zgodi varnostni incident, ki pomembno vpliva na delovanje omrežja, operaterji vse svoje resurse usmerimo v reševanje nastalega incidenta, ki bi v večini primerov presegel predlagani čas obveščanja. **Predlagamo, da se obveščanje varnostnega incidenta, ki pomembno vpliva na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev podaljša na 24 ur po zaznavi.**

*(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:*

Nadalje predlagamo, da se pri prijavljanju varnostnih incidentov vzpostavi **enotna/skupna digitalna vstopna točka (portal)**, kjer bi z enkratnim digitalnim vnosom podatkov obvestili vse relevantne deležnike. Trenutni način obveščanja, s pošiljanjem »word« dokumenta na elektronske naslove je v dobi digitalizacije zamuden in zastarel postopek.

[1] https://www.akos-rs.si/javna-posvetovanja-in-razpisi/novica/agencija-objavlja-predlog-splosnega-akta-o-porocanju-in-vrednotenju-varnostnih-incidentov

telemach

Drugi odstavek 3. člena

V zvezi z obveščanjem o varnostnih incidentih ponavljamo predlog podan v prvem odstavku 3. člena. Vzpostavi se naj **enotna/skupna digitalna vstopna točka (portal)**, kjer bi z enkratnim digitalnim vnosom podatkov obvestili vse relevantne deležnike.

Tretji odstavek 3. člena

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 seznani**.

*(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 seznani. 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.*

Prvi odstavek 4. člena (točka 2. c.)

Glede na to, da so dandanes ciljno usmerjeni napadi na omrežje ali storitve operaterja oziroma njegove uporabnike (DoS, DDoS, sabotaže, itd.) že skoraj vsakodnevni, **predlagamo, da se za tovrstne varnostne napade poroča tedensko in ne ob vsakem napadu.** Namreč krajših incidentov uporabniki ne zaznavajo oziroma na uporabnike nimajo večjega vpliva, zato njihova obravnava ni smiselna.

Predlagamo, da se 2. c) točka prvega odstavka 4. člena briše, saj je takih napadov (DoS, DDos) zoper uporabnike preveliko število.

V kolikor zahteve ni moč izbrisati, upoštevajte predlagano tedensko poročanje ali pa se dikcija spremeni na način, da se prijavlja samo napade, ki so vplivali na delovanje storitev.

Drugi odstavek 4. člena

V drugem odstavku 4. člena je navedeno, da mora operater, ki zagotavlja storitve končnim uporabnikom, nemudoma poročati pristojnim organom o varnostnih incidentih, ki so negativno vplivali na delovanje oziroma izvajanje, poleg ostalih storitev tudi storitve upravljavcev kritične infrastrukture, storitve izvajalcev bistvenih storitev (IBS) ali organov državne in ključnih delov sistema varnosti države. Za poročanje slednjih bi morali operaterji imeti točne in vsakokrat posodobljene sezname kritične infrastrukture, IBS in ključnih delov sistema države. Postavlja se vprašanja kdo nam bo posredoval sezname in skrbel za njihovo aktualnost?

telemach

Prvi odstavek 5. člena

Predlagamo črtanje prvega odstavek 5. člena, ki predvideva, da operater obvešča javnost in svoje uporabnike o vseh varnostnih incidentih, ki pomembno vplivajo na kakovost ali razpoložljivost njegovih storitev. Menimo, da je obveščanje uporabnikov o vseh incidentih povsem nepotrebno, saj bo to privedlo zgolj do objave velike količine podatkov, ki po vsej verjetnosti za javnost in uporabnike ne bo zanimiva ali koristna. Za uporabnike je bolj pomembno in koristno obveščanje o morebitnih zaščitnih in popravnih ukrepih, kar pa je že predvideno v drugem odstavku istega člena.

V primeru vprašanj ali nejasnosti ostajamo na voljo.

S spoštovanjem,

Martina Denovnik
Vodja službe za regulativo