TelekomSlovenije

Agencija za komunikacijska omrežja in storitve Republike Slovenije
Stegne 7
1001 Ljubljana

info.box@akos-rs.si

Ljubljana, 30. 3. 2023

ZADEVA: **Javna obravnava osnutka Splošnega akta o poročanju in vrednotenju varnostnih incidentov**
Zveza: **0073-1/2023**

Spoštovani,

Telekom Slovenije, d.d. (v nadaljevanju: Telekom Slovenije), naslovni Agenciji za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: Agencija) v roku posreduje predloge sprememb in dopolnitev osnutka Splošnega akta o poročanju in vrednotenju varnostnih incidentov (v nadaljevanju: Splošni akt), ki je bil dne 27. 2. 2023 objavljen na spletni strani Agencije.

Uvodoma Telekom Slovenije poudarja, da mora biti Splošen akt jasen in racionalen ter usklajen z direktivo NIS 2[1]. Ključnega pomena je, da se z namenom učinkovitosti poročanja ter v izogib nepotrebnemu obremenjevanju operaterjev s poročanjem številnim različnim organom oziroma institucijam, vzpostavi enotna platforma za poročanje s strani operaterjev, v katero bi bili povezani vsi pristojni organi oziroma institucije, ki bi morali zaradi obveščenosti imeti vzpostavljene tudi medsebojne povezave.

Predlogi družbe Telekom Slovenije, vezani na Splošni akt, so sledeči:

3. člen Splošnega akta (priglasitev varnostnih incidentov)

(i)

Telekom Slovenije predlaga, da se besedilo v prvem odstavku 3. člena Splošnega akta, ki se glasi:
»Operaterji morajo brez nepotrebnega odlašanja oziroma največ v eni uri po zaznavi varnostnega incidenta, ki pomembno vpliva …«

spremeni, tako da se glasi:
»Operaterji morajo brez nepotrebnega odlašanja oziroma največ v štiriindvajsetih urah po zaznavi in potrditvi varnostnega incidenta, ki pomembno vpliva …«

Obrazložitev:
Predlagamo podaljšanje roka za posredovanje obvestila Agenciji na 24 ur po zaznavi varnostnega incidenta. Poročanje v roku 1 ure je neizvedljivo, saj se v tem času v večini primerov še določajo obseg dogodka, njegove posledice in vzroki. V prvi uri po zaznavi dogodka le-tega pogosto ni možno niti ustrezno klasificirati kot incidenta, glede na 6. člen tega Splošnega akta. Predlog podaljšanja roka na 24 ur je skladen s 23. členom (4. odstavek točka a) NIS 2 direktive.
Potrebna je tudi jasna definicija pojma »*zaznava varnostnega incidenta*«, zato predlagamo dodatno dopolnitev, in sicer, da mora biti incident tudi potrjen. Predpisan rok za poročanje začne teči, ko varnostni dogodek prekvalificiramo v varnostni incident. Varnostni dogodek je zaznan takrat, ko se zgodi oziroma ko ga nadzorni sistemi zaznajo in s tem zabeležijo. Takrat se sproži proces preiskovanja varnostnega dogodka, ki se ga časovno ne da definirati. Na podlagi preiskovanja varnostnega dogodka, se ta tekom preiskave, ko so potrjeni indici, da ne gre zgolj za dogodek, prekvalificira v varnostni incident.

(ii)

Telekom Slovenije predlaga, da se 3. in 5. točka prvega odstavka 3. člena Splošnega akta, ki se glasita:
»3. zaupnost, kjer je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, komunikacijskih ali meta podatkov, neavtorizirani osebi, entiteti ali procesu (zlorabljena ali razkrita komunikacija, identiteta in lokacija uporabnika, vdori, ugrabljen promet uporabnikov ipd.);«
»5. nastanek znatne materialne ali nematerialne škode, ki jo je, ali bi jo lahko utrpel operater, ali pa njegov uporabnik (fizična ali pravna oseba).«

[1] DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148

Spremenita oziroma dopolnita, tako da se glasita:
»3. zaupnost, kjer je bila zaradi varnostnega incidenta na javnem komunikacijskem omrežju ali pri delovanju javnih komunikacijskih storitev ogrožena, razkrita ali zlorabljena zaupnost komunikacije, komunikacijskih ali meta podatkov, neavtorizirani osebi, entiteti ali procesu (zlorabljena ali razkrita komunikacija, identiteta in lokacija uporabnika, vdori, ugrabljen promet uporabnikov ipd.);«
»5. nastanek znatne materialne ali nematerialne škode, ki jo je, ali bi jo lahko, zaradi varnostnega incidenta na javnem komunikacijskem omrežju ali pri delovanju javnih komunikacijskih storitev, utrpel operater, ali pa njegov uporabnik (fizična ali pravna oseba).«

Obrazložitev:
Predlagamo jasnejšo opredelitev obsega poročanja v tem delu. Zaupnost podatkov je lahko (oziroma je) tipično najpogosteje ogrožena zaradi razlogov, ki se ne tičejo oziroma niso povezani z omrežjem in storitvami operaterja (npr. z zlorabo ukradenih/izgubljenih dokumentov pri sklepanju poslov, neustrezno hrambo uporabniških imen in gesel s strani strank, …). Menimo, da tovrstni incidenti niso in naj ne bi bili predmet poročanja po ZEKom-2.

(iii)

Telekom Slovenije predlaga, da se besedilo v tretjem odstavku 3. člena Splošnega akta, ki se glasi:
»(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 roku dveh ur 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.«

spremeni, tako da se glasi:
»(3) Če podatki o vplivu ali obsegu varnostnega incidenta ob zaznavi in potrditvi 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 roku štiriindvajsetih ur od kar se z njimi seznani. Operater najkasneje v treh mesecih po odpravi varnostnega incidenta poroča agenciji in nacionalnemu CSIRT ostale zahtevane informacije iz tretjega odstavka 4. člena tega splošnega akta.«

Obrazložitev:
Sklicujemo se na zgornjo obrazložitev predloga k prvemu odstavku tega člena Splošnega akta. Ko je potrjeno, da gre za varnostni incident, se vse vpletene ekipe trudijo, da se v najkrajšem možnem času vzpostavi prvotno stanje. Zato ni primerno, da se v teh kritičnih trenutkih ukvarjajo še s tem, koliko časa je še do poročanja o različnih podatkih vsem organom, katerim je potrebno poročati. V primeru izpadov komunikacije v sili je najprej potrebno obvestiti centre za sprejem komunikacije v sili in v dogovoru z njimi zagotoviti ponovno delovanje v najkrajšem možnem času.
Dodatno v drugem stavku tretjega odstavka 3. člena Splošnega akta predlagamo podaljšanje roka za poročanje po odpravi varnostnega incidenta. Po vzpostavitvi delovanja je potrebna temeljita analiza, preko katere se odkrije vektor napada in sprejme ukrepe za izboljšanje. Analiza v zgolj 10 dneh bi lahko v veliki meri temeljila na ugibanju, zaključki pa bi lahko bili napačni, zato predlagamo, da se rok za poročanje podaljša na tri mesece.

(iv)

Telekom Slovenije predlaga, da se besedilo v prvem stavku četrtega odstavka 3. člena Splošnega akta, ki se glasi:
» (4) Poročanje pristojnim organom o varnostnih incidentih se izvaja na način, da se zagotovi varnost prenesenih podatkov, praviloma po elektronski poti, preko elektronske pošte na vnaprej dogovorjeni elektronski naslov oziroma preko enotnega portala za poročanje.«

spremeni, tako da se glasi:
»(4) Poročanje pristojnim organom o varnostnih incidentih se izvaja na način, da se zagotovi varnost prenesenih podatkov, praviloma po elektronski poti, preko elektronske pošte na vnaprej dogovorjeni skupni elektronski naslov oziroma preko enotnega portala za poročanje.«

Obrazložitev:
Predlagamo uporabo enotnega portala za poročanje ali skupni elektronski naslov za vse pristojne organe, ki jih je potrebno obveščati oziroma jim poročati. Tako ne bo prišlo do primera, da bi katerega od pristojnih organov pomotoma izpustili pri izvedbi obveščanja.

4. člen Splošnega akta (kriteriji za poročanje in vsebina poročila)

Vezano na 4. člen Splošnega akta uvodoma poudarjamo oziroma predlagamo, da bi bilo potrebno izrecno zapisati oziroma določiti, da je v primeru, ko operater omrežje daje v najem, odgovornost za poročanje na najemniku.

(i)

Telekom Slovenije predlaga, da se točka 1. a) prvega odstavka 4. člena Splošnega akta, ki se glasi:
»a) vpliv je trajal manj kot uro in je prizadel več kot 20% vseh naročnikov po posamezni storitvi,«

spremeni tako, da se glasi:
»a) vpliv je trajal več kot 15 minut in je prizadel več kot 20% vseh naročnikov po posamezni storitvi,«

Dodatno predlagamo, da se jasno opredeli vsebina pojma »*posamezne storitve*«, ki se uporablja v navedeni določbi.

Obrazložitev:
Predlagamo spremembo kriterija, po katerem bi morali obveščati o čisto vseh incidentih, tudi če so trajali manj kot minuto, in jih ogromna večina uporabnikov sploh ni mogla zaznati. Po do sedaj veljavnem splošnem aktu o takšnih dogodkih sploh ni bilo potrebno obveščati, saj kratkotrajni izpadi nimajo večjega vpliva na nemoteno delovanje operaterja.
Prav tako je smiselno bolj jasno definiranje pojma »*posamezne storitve*« - določene storitve nimajo bistvenega pomena in je zato obveščanje nesmiselno (npr. izpad HBO Max).

(ii)

Telekom Slovenije predlaga, da se besedilo točke 2. prvega odstavka 4. člena Splošnega akta, ki se glasi:
»(2) vpliv na zaupnost komunikacij, in sicer na zaupnost podatkov o prometu iz 218. člena ZEKom-2 ali podatkov o naročnikih iz 215. člena ZEKom-2 ter na avtentičnost in celovitost omrežja: …«

spremeni tako, da se glasi:
»(2) vpliv na zaupnost komunikacij, in sicer na zaupnost podatkov o prometu iz 218. člena ZEKom-2 ali podatkov o naročnikih iz 215. člena ZEKom-2 ter na avtentičnost in celovitost omrežja, kjer so bili zaradi varnostnega incidenta na javnem komunikacijskem omrežju ali pri delovanju javnih komunikacijskih storitev: …«

Obrazložitev:
Predlagamo uskladitev z obsegom poročanja glede na predlog predhodno navedenega popravka prvega odstavka 3. člena Splošnega akta.

(iii)

Telekom Slovenije predlaga, da se točke 2.c), 2.č) in 2.d) prvega odstavka 4. člena Splošnega akta, ki se glasijo:
»c) izveden je bil ciljno usmerjen napad na omrežje ali storitve operaterja oziroma njegove uporabnike (DoS, DDoS, sabotaže, itd.), ne glede na čas trajanja ali število prizadetih, kjer se sproži ukrep preusmeritve oziroma čiščenja prometa bodisi lokalno ali z zunanjo podporo (angl. »blackholing«),«
»č) izveden je bil nepooblaščen vdor ali vpogled v bazo uporabnikov, podporne informacijske sisteme ali omrežne elemente operaterja,«
»d) dogodek ali več ponavljajočih dogodkov zaradi ranljivosti ali neustreznih nastavitev, procesov je vplivalo na celovitost ali avtentičnost omrežja ali uporabnike in je bilo posredno ali neposredno prizadetih več kot 100 uporabnikov (goljufije, zlorabe in kibernetska kriminaliteta).«

spremenijo tako, da se glasijo:
»c) izveden je bil ciljno usmerjen napad na omrežje ali storitve operaterja oziroma njegove uporabnike (DoS, DDoS, sabotaže, itd.) in so bile storitve motene, ne glede na število prizadetih, kjer se proži ukrep preusmeritve, oziroma čiščenja s pomočjo ponudnika telekomunikacijskih storitev operaterja (uplink providerja)«,«
»č) izveden je bil nepooblaščen vdor ali vpogled v bazo uporabnikov, podporne informacijske sisteme ali omrežne elemente operaterja, razen če ni verjetno, da bi bile s tem ogrožene pravice in svoboščine naročnikov oziroma uporabnikov,«
»d) incident ali več ponavljajočih incidentov zaradi ranljivosti ali neustreznih nastavitev, procesov je vplivalo na celovitost ali avtentičnost omrežja ali uporabnike in je bilo posredno ali neposredno prizadetih več kot 100 uporabnikov (goljufije, zlorabe in kibernetska kriminaliteta).«

Obrazložitev:
K točki c): Pri ciljno usmerjenih napadih se vse odvija samodejno. Smiselno je, da so izvzeti primeri, ko storitev ni bila motena, ker je operater poskrbel za nemoteno delovanje (redundančni sistemi niso napadeni). Prav tako je smiselno izvzeti krajše napade, ki so trajali manj kot 15 minut, če niso imeli večjega vpliva na nemoteno delovanje operaterja. Predlagamo tudi, da se jasneje definira, kaj pomeni zunanja podpora (»blackholing«). Blackholing je namreč osnovna funkcionalnost DDoS orodja in ni merodajen podatek, saj je odvisen od zakupljene licence DDoS orodja posameznega operaterja.

K točki č): Za sorazmerno ureditev administrativnih bremen operaterjev naj se v tem primeru postopki poročanja, ki jih mora izvajati operater kot ponudnik elektronskih komunikacijskih storitev, uskladijo z obveznostmi poročanja, ki jih ima operater kot obdelovalec osebnih podatkov. Predlagamo, da se obveznost poročanja uskladi z obveznostmi iz Splošne uredbe o varstvu podatkov.

K točki d): Po naši oceni je zapisana preveč splošno in bi jo bilo potrebno jasneje opredeliti. Tudi če je prizadetih več kot 100 uporabnikov, obveščanje ni možno, če npr. SPAM filter ni zaznal *phishing-a*. Gre za zasebne poštne predale in zasebne končne naprave, zato je to neizvedljivo. Predlagamo še, da se namesto besede »dogodek« uporablja »incident« - na podlagi preiskovanja varnostnega dogodka, se ta tekom preiskave, ko so potrjeni indici, da ne gre zgolj za dogodek, prekvalificira v varnostni incident.

(iv)

Telekom Slovenije predlaga, da se druga alineja 1. točke drugega odstavka 4. člena Splošnega akta, ki se glasi:
»- zaradi nedelovanja ali ohromljenega delovanja omrežja je prizadetih več kot 100 uporabnikov te storitve,«, črta.

Obrazložitev:
Predlagamo, da se naveden kriterij črta. Že prva alineja 1. točke drugega odstavka 4. člena Splošnega akta namreč nalaga obveznost obveščanja ob vplivu na delovanje storitev komunikacij v sili.

(v)

Telekom Slovenije predlaga, da se točke 10.b), 10.g) in 10.h) četrtega odstavka 4. člena Splošnega akta, ki se glasijo:
»b) zagotavljanje medosebne komunikacijske storitve, neodvisne od številke (OTT storitve),«,
»g) zagotavljanje storitev podatkovnega centra,«
»h) zagotavljanje storitev računalništva v oblaku;«
črtajo.

Obrazložitev:
Za storitve, opredeljene v točkah 10.b), 10.g) in 10.h) četrtega odstavka 4. člena Splošnega akta ZEKom-2 ne predpisuje nobenih obveznosti, zato ne bi smele biti predmet predmetnega Splošnega akta.

(vi)

Telekom Slovenije predlaga, da se v točki 14. četrtega odstavka 4. člena Splošnega akta opredeli, kako lahko operaterji zaznavajo vpliv na subjekte, ki so navedeni v tej točki. Opredeli se naj tudi, kako naj operaterji pridobijo seznam upravljalcev kritične infrastrukture (b) in IBS (č), saj seznami teh subjektov niso javno dostopni.

(vii)

Telekom Slovenije vezano na točko 17. četrtega odstavka 4. člena Splošnega akta predlaga, da se zaradi dejstva, da bodo operaterji zapadli pod NIS 2 direktivo, uporablja enotno klasifikacijo (ki bo skladna z NOKI, kot navedeno v 6. členu Splošnega akta).

5. člen Splošnega akta (Obveščanje uporabnikov in drugih operaterjev)

V četrtem odstavku 5. člena Splošnega akta je pred obvestilom javnosti o incidentu predvideno posvetovanje z Agencijo. Menimo, da je potrebno bolj jasno navesti v katerih primerih je posvetovanje potrebno oziroma je takšna vsebina smiselna zgolj v primeru, če bo Agencija zagotavljala ustrezno odzivnost v režimu 24/7. V nasprotnem primeru lahko pride do tega, da bo obvestilo do uporabnikov prišlo z zamudo, kar lahko pri uporabnikih povzroči dodatne posledice in nepopravljivo škodo, zaradi posledic varnostnega incidenta. Zaradi navedenega bi bilo treba četrti odstavek 5. člena Splošnega akta ustrezno prilagoditi oziroma črtati.

6. člen Splošnega akta (vrednotenje varnostnega incidenta)

(i)

Telekom Slovenije predlaga, da se besedilo drugega odstavka 6. člena Splošnega akta, ki se glasi:
»(2) Varnostni incidenti se skladno s prejšnjim odstavkom razvrščajo v tri glavne skupine: lažji, težji in kritični varnostni incident:«

spremeni tako, da se glasi:
»(2) Varnostni incidenti se skladno s 119. členom ZEKom-2 razvrščajo v tri glavne skupine: lažji, težji in kritični varnostni incident:«

Obrazložitev:
Delitev varnostnih incidentov na tri različne skupine je predpisana v 119. členu ZEKom-2. Agencija naj v tem Splošnem aktu opredeli predvsem, kdaj gre za majhen, velik ali zelo velik negativen vpliv, pri tem pa naj upošteva merila, ki so določena v 3. odstavku 118. člena ZEKom-2: *število uporabnikov, trajanje incidenta, geografsko razširjenost območja in obseg prizadetosti delovanja omrežja ali storitve, obseg vpliva na kritično infrastrukturo, izvajanje bistvenih storitev, storitve komunikacije v sili, delovanja ODU in nosilcev ključnih delov sistema varnosti države.* Pri tem agencija sodeluje z organom, pristojnim za informacijsko varnost. Potrebno je torej poenotenje in odprava neskladij. Ob tem se je potrebno zavedati, da različne klasifikacije znotraj istega primera niso smiselne in povzročajo le dodatno nepotrebno delo na obsežnih analizah.

(ii)

Telekom Slovenije predlaga, da se točka 2.e) drugega odstavka 6. člena Splošnega akta, ki se glasi: »e) je novico o varnostnem incidentu objavilo več medijskih hiš ali spletnih portalov v državi,« črta.

Obrazložitev:
Menimo, da navedena določba ne predstavlja ustrezne metodologije za določanje klasifikacije varnostnega incidenta in jo je potrebno črtati.

S spoštovanjem.

Pripravili:

Sašo Potočnik
Pravne zadeve in regulativa

Boštjan Vrečko
Korporativna varnost

Tatjana Savić
IKT in storitve omrežja

Jernej Nemec
Skladnost poslovanja in upravljanje tveganj

Telekom Slovenije, d.d.
mag. Vesna Prodnik
članica uprave

Poslati:
- priporočeno s povratnico na naslov Agencije
- na e-mail naslov info.box@akos-rs.si