TelekomSlovenije

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

info.box@akos-rs.si

Ljubljana, 1. 6. 2023

ZADEVA: **Javna obravnava novega osnutka Splošnega akta o varnosti omrežij, storitev in podatkov**
Zveza: **0073-3/2023**

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 novega osnutka Splošnega akta o varnosti omrežij, storitev in podatkov (v nadaljevanju: Splošni akt), ki je bil dne 19. 5. 2023 objavljen na spletni strani Agencije.

Telekom Slovenije je predloge sprememb in dopolnitev posredoval že k prvotni različici Splošnega akta, ki je bila na spletni strani Agencije objavljena 17. 2. 2023, in sicer smo predloge sprememb in dopolnitev Agenciji posredovali 31. 3. 2023. Agencija je v novi verziji Splošnega akta upoštevala določene predhodno posredovane predloge sprememb in dopolnitev Splošnega akta, na predloge sprememb in dopolnitev Telekoma Slovenije, ki jih Agencija ni upoštevala, pa se Telekom Slovenije v izogib ponovnemu navajanju ponovno sklicuje in Agenciji predlaga, da jih smiselno upošteva v končni verziji Splošnega akta.

Predlogi družbe Telekom Slovenije so sledeči:

2. člen Splošnega akta (pomen izrazov)

Telekom Slovenije predlaga, da se podrobneje opredelita pojma »*veliko število prizadetih uporabnikov*« oziroma »*daljši izpad storitev*«, ki se uporabljata v 6. točki prvega odstavka 2. člena Splošnega akta.

Obrazložitev:
Pojma »*veliko število prizadetih uporabnikov*« oziroma »*daljši izpad storitev*« sta nedefinirana in omogočata različne interpretacije. Zato, da imajo vsi operaterji enaka merila pri presoji navedenih pojmov, predlagamo, da se ju v Splošnem aktu ustrezno definira oziroma določi vrednosti pragov za ti dve merili (npr. nad 25% uporabnikov; nad 12 ur izpada storitev).

3. člen Splošnega akta (varnostna politika)

(i)

Telekom Slovenije predlaga, da se besedilo prvega odstavka 3. člena Splošnega akta, ki se glasi:
»(1) Operater vzpostavi informacijsko varnostno politiko, ki obsega najmanj:«

spremeni tako, da se glasi:
»(1) Operater vzpostavi **varnostno politiko, ki vsebuje informacijsko varnostno politiko in politiko neprekinjenega poslovanja (v nadaljnjem besedilu varnostna politika)**, ki obsega najmanj:«

Skladno z navedenim predlogom se v celotnem Splošnem aktu ustrezno prilagodijo preostali členi Splošnega akta, in sicer na način, da se namesto pojma »*informacijska varnostna politika*« uporablja pojem »*varnostna politika*«.

Obrazložitev:
Naslov predmetnega člena Splošnega akta se glasi »varnostna politika«, nato pa se v besedilu člena uporablja pojem »informacijska varnostna politika«. Tudi pri informacijski varnostni politiki se navaja, da vključuje tako SUVI kot tudi SUNP. Oboje (tako varovanje informacij kot tudi neprekinjeno poslovanje) je sicer lahko del skupne varnostne politike, lahko pa ima operater tudi ločeno politiko informacijske varnosti (varovanja informacij) in politiko neprekinjenega poslovanja. Operater ima lahko še dodatne varnostne politike (npr. politika fizičnega varovanja ...), vse skupaj pa so del krovne varnostne politike.

Predlagamo, da se zaradi poenotenega poimenovanja in neodvisnosti od tega, ali je politika neprekinjenega poslovanja sestavni del informacijske varnostne politike ali pa je ločena politika, spremeni prvi stavek prvega odstavka 3. člena Splošnega akta na način, da se opredeli, da mora varnostna politika vsebovati informacijsko varnostno politiko in politiko neprekinjenega poslovanja (brez opredelitve, ali je to v enem ali več ločenih politikah), vse pa se v nadaljnjem besedilu Splošnega akta referira kot »varnostna politika«. Tudi sedaj se že v nekaterih členih Splošnega akta uporablja zgolj pojem »varnostna politika«, nekonsistentna uporaba pojma »varnostna politika« in »informacijska varnostna politika« pa bi vnašala zmedo v Splošni akt. Prav tako predlagamo, da se v celotnem Splošnem aktu ustrezno prilagodijo preostali členi Splošnega akta, in sicer na način, da se namesto pojma »*informacijska varnostna politika*« uporablja pojem »*varnostna politika*«.

(ii)
Telekom Slovenije predlaga, da se 3. točka prvega odstavka 3. člena Splošnega akta, ki se glasi:
»3. navedbo tveganj, nevarnosti in groženj, ki bi lahko ogrozile njegovo delovanje,«

spremeni tako, da se glasi:
»3. navedbo tveganj, nevarnosti in groženj, ki bi lahko ogrozile **izvajanje storitev elektronskih komunikacij,**«

Obrazložitev:
Uporabljena dikcija »*ogrozile njegovo delovanje*« je zelo široka in se nanaša na celotno poslovanje družbe, ne pa zgolj na izvajanje storitev elektronskih komunikacij, na kar se nanaša Splošni akt, zaradi česar predlagamo ustrezno spremembo dikcije navedene 3. točke prvega odstavka 3. člena Splošnega akta.

(iii)
Telekom Slovenije predlaga, da se drugi odstavek 3. člena Splošnega akta, ki se glasi:
»(2) Informacijsko varnostno politiko in ukrepe za obvladovanje tveganj za informacijsko varnost odobri vodstvo, objavi in sporoči zaposlenim ter relevantnim pogodbenim partnerjem.«

spremeni tako, da se glasi:
»(2) Informacijsko varnostno politiko in ukrepe za obvladovanje tveganj za informacijsko varnost **sprejme vodstvo. Operater mora varnostno politiko in ukrepe za obvladovanje tveganj sporočiti zaposlenim ter relevantnim pogodbenim partnerjem.**«

Obrazložitev:
Menimo, da mora varnostno politiko vodstvo operaterja sprejeti, ne zgolj odobriti. Naveden odstavek 3. člena Splošnega akta v predlagani obliki je tudi dvoumen, saj se lahko razume, da mora vodstvo operaterja, poleg sprejetja (odobritve) varnostne politike, to tudi objaviti/sporočiti zaposlenim in relevantnim pogodbenim partnerjem. Slednje aktivnosti so lahko z interno organizacijo operaterja urejene na drug način. Pomembno je, da operater sledi zastavljenemu cilju, to je sporočanje varnostne politike znotraj organizacije kot tudi po potrebi zainteresiranim strankam (pogodbenim partnerjem).

<u>6. člen Splošnega akta (vsebina SUNP)</u>

(i)
Telekom Slovenije predlaga, da se prvi odstavek 6. člena Splošnega akta, ki se glasi:
»(1) Operater v okviru SUNP ob upoštevanju njegovih lokacij, njegove velikosti in kompleksnosti, pripravi strateški in taktični načrt in postopke za zagotavljanje neprekinjenega poslovanja ter izvede oceno vpliva na poslovanje, ki zajema navedbo možnih dogodkov in varnostnih incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi elementov omrežij, informacijskih sistemov, kadrovskih razlogov, odpovedi oskrbe z energenti, dobave opreme oziroma storitev podpore tretje ravni.«

spremeni tako, da se glasi:
»(1) Operater v okviru SUNP ob upoštevanju njegovih lokacij, njegove velikosti in kompleksnosti, pripravi strateški in taktični načrt in postopke za zagotavljanje neprekinjenega poslovanja ter izvede oceno vpliva na poslovanje **in oceno tveganja**, ki zajema navedbo možnih dogodkov in varnostnih incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi elementov omrežij, informacijskih sistemov, kadrovskih razlogov, odpovedi oskrbe z energenti, dobave opreme oziroma storitev podpore tretje ravni.«

Obrazložitev:
Predlagamo dopolnitev določbe na način, da se doda oziroma upošteva tudi ocena tveganj. V sedanji obliki je pomen določbe takšen, da mora ocena vpliva na poslovanje upoštevati možne dogodke in varnostne incidente, kar pa ni običajna praksa. ISO 22301 definira analizo vpliva na poslovanje (»*business impact analysis: process of analysing the impact over time of a disruption on the organization*«) kot analiziranje vpliva izpada na poslovanje operaterja (storitve) in se ne nanaša na vzrok izpada, ampak na posledice izpada. S procesom ocenjevanja tveganj se identificira, analizira in obravnava vzroke, ki lahko pripeljejo do izpada. Tako kot pri SUVI je tudi pri SUNP ocenjevanje tveganj bistven proces, ki mora biti ustrezno vključen v SUNP.

(ii)

Telekom Slovenije predlaga, da se (sicer napačno številčena) 7. točka drugega odstavka 6. člena Splošnega akta, ki se glasi:
»7. vzpostavi učinkovit proces shranjevanja oziroma varnostnega arhiviranja (po potrebi na potresno varno rezervno lokacijo) in obnove podatkov v primeru izgube ali zlorabe, ki se periodično preverja,«

spremeni tako, da se glasi:
»7. vzpostavi učinkovit proces shranjevanja oziroma varnostnega arhiviranja (po potrebi na potresno varno rezervno lokacijo) in obnove podatkov v primeru izgube, ki se periodično preverja,«

Obrazložitev:
Obnova podatkov se izvede v primeru, če so bili podatki na operativnih sistemih pobrisani, uničeni zaradi kateregakoli razloga, nenadzorovano spremenjeni – torej z eno besedo izgubljeni, saj v operativnih sistemih nimamo več (dela ali vseh) podatkov. O zlorabi podatkov pa govorimo, če so bili podatki razkriti ali uporabljeni za druge namene, kot pa se jih hrani, sami podatki pa pri tem niso bili izgubljeni. V tem primeru nam obnovitev podatkov iz varnostnega kopiranja oziroma arhiviranje ne rešita težav zlorabe osebnih podatkov oziroma obnova podatkov sploh ni potrebna, saj imamo v operativnih sistemih že veljavne podatke. Glede na navedeno predlagamo, da se v navedeni določbi črta del besedila »*ali zlorabe*«.

(iii)

Telekom Slovenije predlaga, da se pojem »*učinkovit/-a/-o*«, ki se uporablja v (napačno številčeni) 9. točki drugega odstavka 6. člena Splošnega akta ter v nadaljevanju tudi v preostalih določbah splošnega akta (tretji in četrti odstavek 6. člena Splošnega atka, 7. člen Splošnega akta), zamenja s pojmom »*uspešen/-a/-o*«.

Obrazložitev:
V navedeni določbi Splošnega akta ter tudi v nadaljevanju le-tega se uporabljajo besedne zveze »učinkovita obnova«, »učinkovitost ukrepov«, »učinkovitost SUNP« … Standardi ISO/IEC 27001 in ISO 22301 uporabljajo pojem »*uspešnost*« (angl. »*effectiveness*«), ki pomeni, da so načrtovane aktivnosti izvedene in doseženi načrtovani rezultati (angl. »*planned activities are realized and planned results achieved*«). Primeri uporabe v navedenih standardih: »uspešnost sprejetih ukrepov« (angl »*effectiveness of the actions taken*«), »uspešnost sistema upravljanja informacijske varnosti« (angl. »*effective information security management*«), … V navedenih standardih se ne pojavlja beseda »učinkovitost« (angl. »*efficiency*«), ki pove, kako dobro se izkoriščajo sredstva za doseganje ciljev, torej razmerje med vloženimi viri (kot so čas, denar, energija, materiali, …) in doseženimi rezultati. Učinkovitost je povezana z optimizacijo in racionalno uporabo virov. Seveda je cilj vsakega operaterja učinkovito izvajaje zahtevanih aktivnosti, vendar pa mora Splošni akt slediti temu, da so izvedene načrtovane aktivnosti in doseganje načrtovanih rezultatov, torej da se od operaterjev zahteva uspešnost. Učinkovitost operaterjev je interni poslovni cilj in ne more biti predmet zahtev Splošnega akta, še manj pa predmet nadzora. Glede na navedeno predlagamo, da se v vseh delih Splošnega akta, kjer je uporabljen pojem »*učinkovitost*«, le-ta zamenja s pojmom »*uspešnost*«.

10. člen Splošnega akta (upravljanje tveganj v zvezi z oskrbo električne energije)

(i)

Telekom Slovenije predlaga, da se tretji odstavek 10. člena Splošnega akta, ki se glasi:
»(3) Operater mora imeti v času največje obremenitve vsaj dvourno avtonomijo (rezervno napajanje), ki omogoča več kot 500 naročnikom delovanje vsaj javno dostopne medosebne komunikacijske storitve na podlagi številke, SMS sporočil, javnega alarmiranja in obveščanja ter storitev komunikacij v sili, na vseh večjih dostopovnih vozliščih ter baznih postajah, ki pokrivajo naselja s statusom mesta z več kot 3 000 prebivalci.«

spremeni tako, da se glasi:
»(3) Operater mora imeti v času največje obremenitve vsaj dvourno avtonomijo (rezervno napajanje), ki omogoča več kot 500 **uporabnikom** delovanje vsaj javno dostopne **govorne** komunikacijske storitve na podlagi številke, javnega alarmiranja in obveščanja ter storitev komunikacij v sili, na vseh večjih dostopovnih vozliščih ter baznih postajah.«

Obrazložitev:
Predlagamo, da se namesto na »javno dostopne medosebne komunikacijske storitve« (govorne storitve, SMS, MMS,...), ki je zelo širok pojem, obveznost nanaša na »govorne komunikacijske storitve na podlagi številke«. Predlagani kriteriji so zelo kompleksni, zato predlagamo, da se obveznost nanaša na dostopovna vozlišča in bazne postaje, na katerih je hkrati več kot 500 uporabnikov. Namesto pojma »*naročniki*« predlagamo uporabo pojma »*uporabniki*«, saj so na baznih postajah tudi drugi uporabniki, ki niso naročniki operaterja (predplačniki, roaming uporabniki).

(ii)

Telekom Slovenije predlaga, da se v celoti črta četrti odstavek 10. člena Splošnega akta, ki se glasi:
»(4) Operater mora imeti v času največje obremenitve vsaj dve urno avtonomijo (rezervno napajanje), ki omogoča več kot 250 naročnikom delovanje vsaj javno dostopne medosebne komunikacijske storitve na podlagi številke, SMS sporočil, javnega alarmiranja in obveščanja ter storitev komunikacij v sili, na vseh večjih dostopovnih vozliščih ter baznih postajah, ki pokrivajo naselja brez statusa mesta z manj kot 3 000 prebivalci.«

Obrazložitev:
Predlagamo črtanje določbe, saj so predlagani kriteriji pretirano kompleksni oziroma zahtevni.

14. člen Splošnega akta (certificiranje)

Telekom Slovenije predlaga, da se prvi odstavek 14. člena Splošnega akta, ki se glasi:
»(1) Operater, ki izvaja storitve za kritične subjekte ali ima več kot 100 000 uporabnikov, vzpostavi, izvaja, vzdržuje in nenehno izboljšuje vzdržuje SUVI in SUNP v skladu s priznanimi veljavnimi mednarodnimi standardi v obsegu, kot je določen v zakonu in tem »splošnem aktu.«

spremeni tako, da se glasi:
»(1) Operater vzpostavi, izvaja, vzdržuje in nenehno izboljšuje SUVI in SUNP v skladu s priznanimi veljavnimi mednarodnimi standardi v obsegu, kot je določen v zakonu in tem »splošnem aktu.«

Podredno predlagamo črtanje celotnega 14. člena Splošnega akta.

Obrazložitev:
Kot že v predlogih k prvemu osnutku Splošnega akta opozarjamo, da ustrezno izkazovanje varnosti ne more biti odvisno od tega, komu ali koliko uporabnikom določen operater ponuja svoje storitve. Vsi uporabniki storitev morajo biti s stališča varnosti v enakovrednem položaju, torej smejo pričakovati in morajo biti glede varnosti omrežij, storitev in podatkov deležni enake obravnave, ne glede na to ali so pri operaterju, ki izvaja storitve tudi za kritične subjekte ali ne oziroma ali ima ta operater več kot 100.000 uporabnikov ali ne.

Trenutno predlagana določba neutemeljeno razlikuje med operaterji glede na to, za koga izvajajo storitve ter glede na število njihovih uporabnikov in jih postavlja v neenakopraven položaj ter povečuje varnostna tveganja, saj operaterji, ki ne izvajajo storitev za kritične subjekte oziroma imajo manj kot 100.000 uporabnikov, ne bodo zavezani certificiranju SUVI in SUNP. Posledično se varnostna tveganja prenaša na uporabnike teh operaterjev in jih s tem postavlja v slabši položaj (zaradi slabših standardov varnosti omrežij, storitev, storitev in podatkov, saj ti operaterji ne bodo vsakoletno podvrženi zunanjim in neodvisnim pregledom SUVI in SUNP). Obveznosti bi morale biti za vse

operaterje enake, ne glede na to, komu nudijo javne storitve in ne glede na število njihovih uporabnikov – vsi operaterji bi morali zagotoviti enake standarde varnosti vsem svojim uporabnikom.

Opozarjamo, da bi opustitev obveznosti certificiranja za operaterje, ki imajo manj kot 100.000 uporabnikov, lahko tudi privedla do načrtnega »drobljenja« števila uporabnikov na različne MVNO, še posebej v segmentu rezidenčnih uporabnikov. V tem primeru bi lahko bil cilj operaterja, da ima posamezne MVNO, ki vsak zase ne dosega merila 100.000 uporabnikov in zato zanj ni zahtevana certifikacija SUVI in SUNP. Takšno ravnanje oziroma izigravanje določb Splošnega atka s strani operaterjev bi nedvomno imelo tudi negativne posledice na varnost omrežij, storitev in podatkov uporabnikov teh omrežij.

Iz zgoraj navedenih razlogov predlagamo, da se v 1. odstavku 14. člena Splošnega akta črtata kriterija izvajanja storitev kritičnim subjektom in števila uporabnikov. Certificiranje naj bo obvezno za vse operaterje ali pa naj se navedeni člen Splošnega akta črta v celoti, certificiranje pa se v tem primeru ne zahteva od nobenega operaterja.

Splošni predlog

Telekom Slovenije predlaga, da naj Agencija na svojem spletnem mestu vodi in objavlja seznam relevantnih priporočil Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA) in drugih relevantnih organizacij (npr. Skupina NIS), ki jim naj sledijo operaterji.

Obrazložitev:
V Splošnem aktu se na več mestih (npr. prvi odstavek 4. člena, tretji odstavek 5. člena, peti odstavek 6. člena …) od operaterjev pričakuje upoštevanje določenih standardov in priporočil raznih agencij. V izogib morebitnemu upoštevanju različnega nabora relevantnih dokumentov (sedaj je določitev nabora teh dokumentov prepuščena operaterju in njegovim merilom in kriterijem) predlagamo, da Agencija na svojih spletnih straneh objavlja in sprotno ažurira sezname dokumentov relevantnih priporočil ENISA ali drugih organizacij. Na ta način imajo vsi operaterji enakovreden nabor zunanjih dokumentiranih informacij.

Prav tako predlagamo, da se v določbah Splošnega akta izpusti konkretno navajanje dokumentov z datumi izdaje, ki bi s časom lahko zastarali oziroma bi v primeru izdanih novejših dokumentov ne bile upoštevane dodatne zahteve oziroma priporočila.

S spoštovanjem.

Pripravili:

Sašo Potočnik
Pravne zadeve

Boštjan Vrečko
Korporativna varnost
za

Tatjana Savić
IKT in storitve omrežja

Telekom Slovenije, d.d.
Boštjan Košak
predsednik uprave

TelekomSlovenije d.d.

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