Gospodarska
zbornica
Slovenije

Združenje za informatiko in telekomunikacije

Dimičeva 13 ▪ 1504 Ljubljana ▪ T: (01) 58 98 000, 58 98 474 ▪ F: (01) 58 98 100, (01) 58 98 200 ▪ info@gzs.si ▪ www.gzs.si

Agencija za pošto in elektronske komunikacije Republike Slovenije
Stegne 7, p.p. 418

1001 Ljubljana

Ljubljana, 28. 6. 2013

PREDMET: **Predlogi in pripombe na osnutek predloga Splošnega akta o varnosti omrežij in storitev**

ZVEZA: **Poziv objavljen na spletni strani Agencije, dne 21. 5. 2013, številka 0073-45/2013**

Spoštovani!

Združenje za informatiko in telekomunikacije v okviru Gospodarske zbornice v skladu s pozivom naslovnega organa, podaja predloge in pripombe na Splošni akt o varnosti omrežij in storitev (v nadaljevanju: Splošni akt). Predlogi in pripombe so oblikovani znotraj Sekcije operaterjev elektronskih komunikacij SOEK, ki deluje v okviru Združenja za informatiko in telekomunikacije.

1) Splošni akt o varnosti omrežij in storitev v 15. točki 1. odstavka 2. člena določa, da je vodstveni pregled dokumentiran pregled, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi ustreznost in učinkovitost SUVI in SUNP.

Predlagamo, da se rok za izdelavo vodstvenega pregleda podaljša na dve leti.

Obrazložitev:

Namen vodstvenega pregleda je pregledati rezultate notranjih presoj SUVI in SUNP ter v primeru morebitnih pomanjkljivosti izvesti ustrezne ukrepe za izboljšave. V prejšnji verziji SUVI analize, ki se je izvajala na podlagi Splošnega akta o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov, je bil obseg analize omejen. Na podlagi trenutne verzije Zakona o elektronskih komunikacijah (v nadaljevanju ZEKom-1) pa mora operater zagotoviti pregled vseh sredstev, ki vplivajo na delovanje operaterjevega omrežja in storitev. Podroben pregled teh sredstev zahteva veliko časa, saj je število sredstev zelo obsežno, pri izdelovanju dokumenta pa morajo sodelovati tudi različni zaposleni pri operaterju, ki podrobneje poznajo delovanje in varovanje določenega sredstva. Zaradi velikega števila sredstev, ki jih bo moral operater pregledovati v okviru varnostnega načrta, predlagamo, da se rok za izdelavo vodstvenega pregleda poveča na dve leti.

2) Predlagamo, da se definicije v 2. členu splošnega akta spremenijo in dopolnijo tako:
- da se v definicije celovitosti omrežja briše besedilo »enega ali več«
- da se pri definiciji incidenta doda primeroma naštete dogodke, smiselno enako kot je to v trenutno uporabljanem aktu npr. z besedilom »Za incident se štejejo naravne katastrofe, vojna ali izredna stanja, izpadi električne energije, teroristična dejanja, zlonamerna dejanja posameznikov ali organizacij, okvare na elementih omrežja oziroma informacijskega sistema, človeške napake, delavske stavke itd, vse v kolikor vplivajo na omrežje in storitev.«.

Obrazložitev:

Načrtovanje nepredvidenih dogodkov na predlagani ravni (z veliko verjetnostjo) obravnava vsak predviden incident posebej zato je smiseln poprave definicije, da ne bo nesporazumov da mora operater preigravati scenarije s povezovanjem in nalaganjem incidentov eden na drugega, ker tako (pre)hitro pridemo do nerealnih zahtev. Primeroma našteti dogodki, ki se štejejo za incident pomagajo k lažji razlagi in uporabi splošnega akta.

3) Predlagamo da se doda nov člen nov člen, ki bi jasno določil minimalni nabor storitev pri katerih morajo biti zagotovljeni organizacijski ukrepi iz tega splošnega akta – smiselno je uporabiti kriterije podobne kot pri zahtevi o obveščanju, npr. tako da se vstavi nov člen z besedilom:
»Operater mora organizacijske ukrepe iz tega splošnega akta zagotoviti najmanj pri naslednjih storitvah:
• govorne storitve na fiksni lokaciji,
• govorne storitve v javnih brezžičnih omrežjih,
• podatkovne storitve v javnih fiksnih omrežjih,
• podatkovne storitve v javnih brezžičnih omrežjih,
• zagotavljanje klica na enotno evropsko številko za klic v sili 112, številko policije 113 in številko za prijavo pogrešanih otrok 116 000 in
• medomrežne povezave (zaključevanje klicev končnih uporabnikov, zaključevanje mednarodnih klicev, zaključevanje na številke nujnih služb, posredovanje klicev na končne uporabnike operaterja).• medomrežne povezave.«

4) Splošni akt določa, da mora operater poleg varnostnega načrta izdelati tudi načrt za zagotavljanje celovitosti omrežja.

Predlagamo, da se določila iz načrta za zagotavljanje celovitosti omrežja lahko obravnava samostojno ali v okviru varnostnega načrta, ter se v tem primeru obveznosti znotraj varnostnega načrta nekoliko dopolni.

Obrazložitev:

Splošni akt v 1. odstavku 3. člena določa, da morajo operaterji poleg varnostnega načrta izdelati tudi načrt za zagotavljanje celovitosti omrežja. Znotraj načrta za zagotavljanje celovitosti omrežja mora operater na podlagi 2. odstavka 13. člena Splošnega akta med drugim opredeliti vsa tveganja, ki bi lahko ogrozili neprekinjeno izvajanje storitev. Operaterji že v okviru varnostnega načrta v zvezi z vsakim tveganjem opredelijo verjetnost nastanka posameznega varnostnega incidenta in stopnjo posledic, če do varnostnega incidenta pride, ter pri tej oceni upoštevajo tudi dejstvo, da določen incident lahko vpliva na začasno prekinitev izvajanja storitev. Načrt za zagotavljanje celovitosti omrežja bo torej znotraj dodatnega dokumenta posebej opredelil vsa varnostna tveganja, ki lahko povzročijo začasno neizvajanje storitev. Prav tako znotraj načrta za zagotavljanje celovitosti omrežja trenutno ni jasno opredeljeno ob kolikšnemu obsegu nedelovanja storitev se posamezno tveganje obravnava (storitev lahko ne deluje le za nekatere uporabnike –npr. motnje znotraj omrežja, odpoved baznih postaj, ipd.), ter na katere storitve se ta odpoved nanaša (npr. ali tudi za storitev polnjenja uporabniških računov preko SMS sporočil, telefonsko glasovanje, ipd). Ker vsebina načrta za zagotavljanje celovitosti omrežja ni podrobneje določena ter so tveganja, ki lahko povzročijo nedelovanje storitev že opredeljena v varnostnem načrtu, bi bilo primerno, da se lahko načrt za zagotavljanje celovitosti omrežja pripravi kot samostojen dokument ali združi z varnostnim načrtom, ter te obveznosti znotraj varnostnega načrta ustrezno dopolni.

Dimičeva 13 ▪ 1504 Ljubljana ▪ T: (01) 58 98 000, 58 98 474 ▪ F: (01) 58 98 100, (01) 58 98 200 ▪ info@gzs.si ▪ www.gzs.si

5) Splošni akt določa, da mora operater v okviru dokumentacije SUVI izdelati tudi izjavo o uporabnosti.

Predlagamo, da se določila o izdelavi tega dokumenta odstranijo iz Splošnega akta oz. smiselno vključijo znotraj dokumentov notranje presoje in vodstvenega pregleda SUVI *in SUNP.*

Obrazložitev:

Iz besedila Splošnega akta domnevamo, da je izjava o uporabnosti podrobneje opredeljena v 9. členu, v katerem je opisana vsebina izjave o uporabljenih ukrepih. Splošni akt določa, da je izjava o uporabljenih ukrepih dokumentiran povzetek odločitev v zvezi z obravnavo tveganj. Povzetki odločitev operaterja so navedeni znotraj varnostnega načrta in notranje presoje ter vodstvenega pregleda SUVI in SUNP. Izjava o uporabljenih ukrepih povečuje število dokumentov, ki jih mora operater izdelati, ter hkrati pomeni podvajanje istih podatkov znotraj različnih dokumentov. Izdelovanje dodatne izjave o uporabnosti je po našem mnenju torej nepotrebno ter ne daje dodane vrednosti za operaterja ter nadzorne organe, zato bi bilo primerno, da se ta dokument iz dokumentacije SUVI bodisi odstrani ali pa smiselno uredi znotraj notranje presoje ter vodstvenega pregleda SUVI in SUNP.

6) 8. člen predloga Splošnega akta določa, da mora operater voditi zapise o vseh incidentih, ki so vplivali na varnost omrežij in storitev, celovitost omrežja ali delovanje operaterja v izrednih razmerah, ter te zapise hraniti 1 leto.

Predlagamo, da operaterji vodijo zapise le o tistih incidentih, ki so vplivali na varnost omrežij in storitev, celovitost omrežja ali delovanje operaterja v izrednih razmerah in o katerih morajo v skladu s splošnim aktom obveščati Agencijo.

Obrazložitev:

Operaterji se zavedajo svojih dolžnost, da je potrebno Agenciji Republike Slovenije za pošto in elektronske komunikacije (v nadaljevanju Agenciji) poročati v vseh kršitvah, ki so pomembno vplivale na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev. Ob izvajanju storitev lahko prihaja do določenih napak pri njihovem delovanju (npr. daljše pošiljanje določenih podatkov), ki lahko vplivajo na varnost omrežja ali storitev. Nekateri operaterji zagotavljajo več telekomunikacijskih storitev ter imajo za zagotavljanje teh storitev znotraj svojega podjetja tudi veliko sredstev, ki vplivajo na njihovo delovanje. Redno beleženje vsake napake bodisi znotraj posamezne strojne ali programske naprave ali pa na podlagi npr. tipkarske napake zaposlenega, bi operaterju povzročala veliko stroškov dela, izdelan zapis incidentov pa tako Agenciji kot tudi operaterju ne bi prispeval k večji varnosti omrežij in storitev.

7) 1. odstavek 14. člena Splošnega akta določa, da mora operater takoj, ko to zazna, obvestiti Agencijo o vseh kršitvah varnosti omrežij in storitev ali celovitosti omrežij, če so te pomembno vplivale na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev.

Predlagamo, da se besedilo 1. odstavka 14 člena Splošnega akta spremeni v smislu, da se loči začetno obveščanje, ki ga mora operater izvesti takoj ko je to mogoče in podrobnejše poročanje, ki ga mora operater izvesti najpozneje v 3 delovnih dneh po zaključku incidenta.

Dimičeva 13 ▪ 1504 Ljubljana ▪ T: (01) 58 98 000, 58 98 474 ▪ F: (01) 58 98 100, (01) 58 98 200 ▪ info@gzs.si ▪ www.gzs.si

Obrazložitev:

Ob zaznavi kršitve varnosti omrežja oz. storitev bo operater posvetil vsa svoja razpoložljiva sredstva k čimprejšnji odpravi varnostnega incidenta ter zmanjšanju posledic, ki v zvezi s posamezno kršitvijo nastanejo. Ob odpravi kršitve bo operater najverjetneje izvedel interni nadzor zakaj je do določene kršitve varnosti omrežja oz. storitve prišlo. Ob sami zaznavi kršitve varnosti omrežja oz. storitev nekateri podatki, ki bi jih moral operater posredovati Agenciji, na podlagi 3. odstavka 14. člena Splošnega akta, še niso znani, zato menimo, da bi bilo primerneje, da se operaterju omogoči določen rok za izdelavo poročila. Operater bo v nekaj dneh po ugotovitvi kršitve varnosti razpolagal z natančnejšimi informacijami o varnostnem incidentu, ter na tej podlagi Agenciji lahko posredoval podrobnejše informacije.

8) 14. člen Splošnega akta določa mejne parametre: vpliv je trajal več kot eno uro in je prizadel več kot 15% vseh uporabnikov po posamezni storitvi...

Opozarjamo, da so mejni parametri v tem členu pisani splošno in jih je težko definirati in določiti. Prav tako bo potrebna dodatna obdelava podatkov naročnikov zato, da bomo lahko definirali npr. kriterij, da je bilo prizadetih več kot 15% vseh uporabnikov po določeni storitvi, saj le tako lahko ugotovimo lokacijo uporabnikov na določenem območju (ko npr. pride do izpada določene bazne postaje bi potemtakem morali določiti oz. ugotoviti koliko uporabnikov je bilo prizadetih, kar je v določenih situacijah nemogoče). Predlagamo jasnejše in racionalnejše opredelitve.

9) 2. odstavek 14. člena Splošnega akta opredeljuje dolžnost beleženja in poročanja kršitev ter vpliv na storitve.

Opozarjamo, da ponudniki pasivne infrastrukture ne smejo biti izvzeti (primeri odprtih širokopasovnih omrežij).

Ker ni povsem jasno ali so ti ponudniki zajeti z medomrežnimi povezavami (ponudniki namreč ne nudijo storitev glede na definicijo 32. tč. 3. člena ZEKom-1), predlagamo, da se po potrebi 2. odstavek ustrezno dopolni.

10) 3. odstavek 14. člena Splošnega akta določa, da je potrebno navesti tudi oceno števila prizadetih uporabnikov.

Opozarjamo, da je ocena števila prizadetih uporabnikov res zelo približna, saj na njen izračun vpliva več dejavnikov, ki jih nimamo pod nadzorom. Pride tudi do situacij, ko ocene niti ne moremo pridobiti. Zato predlagamo, da se to ustrezno tudi zapiše v Splošni akt (da se oceno predloži le ko je to mogoče).

11) Predlagamo, da se v 14. člen doda nov odstavek, ki bi določal, da »Operater oceno o % prizadetih uporabnikov in oceno števila prizadetih uporabnikov pripravi ob upoštevanju realnih podatkov ali če to praktično ni izvedljivo ali če bi bilo povezano z dolgotrajnimi postopki ali večjimi stroški, na podlagi ocene operaterja.«.

Obrazložitev:

kot izhaja iz pripomb 8) in 9) je predlog akta v tem delu nejasen. S predlagano spremembo se lahko akt po našem mnenju uporablja in izvaja tudi v praksi brez nepotrebnih zapletanj s tolmačenjem.

Gospodarska zbornica Slovenije

Združenje za informatiko in telekomunikacije

Dimičeva 13 ▪ 1504 Ljubljana ▪ T: (01) 58 98 000, 58 98 474 ▪ F: (01) 58 98 100, (01) 58 98 200 ▪ info@gzs.si ▪ www.gzs.si

12) 1. odstavek 15. člena Splošnega akta določa, da akt začne veljati naslednji dan po objavi v Uradnem listu.

Zaradi ustrezne uskladitve z zadevnim Splošnim aktom, predlagamo, da je vacatio legis vsaj 6 mesecev oziroma 1 leto za vzpostavitev SUNP oz. politike neprekinjenega poslovanja. Uskladitev na strani operaterja terja večje in zamudne logistične postopke in prilagoditve sistemov, zato bi bila uskladitev z aktom v tako kratkem času, kot ga sedaj določa predlog Splošnega akta, nemogoča.

Lep pozdrav!

Dušan Zupančič
Direktor Združenja za informatiko in telekomunikacije pri GZS

Špela Dekleva
Predsednica Sekcije operaterjev elektronskih komunikacij SOEK pri ZIT, GZS