APEK

Agencija za pošto in elektronske komunikacije Republike Slovenije
Stegne 7, p. p. 418
1000 Ljubljana
telefon: 01 583 63 00, faks: 01 511 11 01
e-naslov: info.box@apek.si, http://www.apek.si
davčna št.: 10482369

Številka: 0073-45/2013/17
Datum: 28.8.2013

Zadeva: **Odgovori na prejete pripombe in mnenja k predlogu Splošnega akta o varnosti omrežij in storitev**

Agencija za pošto in elektronske komunikacije RS (v nadaljevanju: agencija) je do izteka podaljšanega roka (30.7.2013) za oddajo pripomb in mnenj zainteresirane javnosti na predlog Splošnega akta o varnosti omrežij in storitev (v nadaljevanju: Splošni akt) prejela pripombe:

- Slovenskega centra za posredovanje pri omrežnih incidentih (v nadaljevanju: SI-CERT)
- Družbe Gradnje in vzdrževanje telekomunikacijskih omrežij d.o.o. (v nadaljevanju: GVO) in
- Družbe T-2 d.o.o. (v nadaljevanju: T-2) in
- Sekcija operaterjev elektronskih komunikacij SOEK pri Združenju za informatiko in telekomunikacije, ki deluje v okviru GZS (v nadaljevanju: SOEK).

Pripombe in mnenja so bila dne 2.7.2013 objavljena na spletnih straneh agencije, za katere se agencija zainteresirani javnosti zahvaljuje in v nadaljevanju nanje podaja odgovore.

SI-CERT agenciji predlaga, da se k 1. odstavku 2. člena doda opredelitev izraza SI-CERT z naslednjo definicijo: *SI-CERT je nacionalni odzivni center za omrežne incidente, ki deluje v okviru javnega zavoda Akademska in raziskovalna mreža Slovenije (ARNES).*

Agencija se s pripombo strinja in bo dodala predlagano definicijo.

Nadalje SI-CERT predlaga, da se za 14. členom (obveščanje in poročanje) doda nov člen z naslednjo vsebino:

(1) Agencija operativno razreševanje incidenta omrežne in informacijske varnosti preda SI-CERT z namenom strokovne pomoči in svetovanja operaterju, usklajevanja z deležniki znotraj države, ter koordinacijo z odzivnimi CERT centri in drugimi sorodnimi službami v tujini.
(2) Po zaključeni obravnavi incidenta SI-CERT poda poročilo Agenciji o poteku obravnave in rezultatih, skupaj z morebitnimi priporočenimi ukrepi za izboljšanje varnosti omrežja in storitev.
(3) Obveščanje o incidentih omrežne in informacijske varnosti, ter poročanje o rezultatih njihove obravnave se izvaja elektronsko.

Si-CERT v svoji obrazložitvi navaja, da novi Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/2012, v nadaljevanju: ZEKom-1) v drugem odstavku 81. člena določa, da

»Agencija o posameznih kršitvah varnosti omrežij in storitev ter o kršitvah celovitosti omrežij po potrebi in glede na stopnjo kršitve obvešča nacionalno kontaktno točko za obravnavo varnostnih incidentov (SI-CERT)«, v 216. členu pa, da »Zaradi zagotavljanja varnosti in celovitosti omrežij lahko agencija zaprosi za strokovno sodelovanje tudi SI-CERT, ki deluje v okviru javnega zavoda Akademska in raziskovalna mreža Slovenije (ARNES), in druge organe, pristojne za varnost in celovitost omrežij.«

SI-CERT v svojem predlogu nadalje navaja, da je poleg normativne ureditve obveščanja o varnostnih incidentih pomemben tudi primeren odziv v smislu tehnične analize konkretnega incidenta z namenom identifikacije ranljivosti, ki so do njega pripeljale in morebitnega širšega konteksta omrežnih napadov. SI-CERT obravnava incidente omrežne ali informacijske varnosti, tj. dogodke, ki predstavljajo kršitev varnostnih mehanizmov in pravil dopustne uporabe v informacijskih sistemih, računalniških omrežjih in javno dostopnih omrežnih storitvah, oziroma predstavljajo grožnjo za to kršitev. SI-CERT s strokovno podporo operaterju in drugim prizadetim v incidentu lahko v okviru svojih pristojnosti in zmogljivosti pomaga pri zamejitvi škodljivih vplivov incidenta, zbiranju dokazov na računalniških sistemih in v omrežju, odstranitvi škodljivih komponent in povrnitvi v prejšnje stanje. SI-CERT kot član mednarodnih združenj odzivnih CERT centrov po potrebi opravi tudi koordinacijo razreševanja incidenta skupaj s tujimi partnerji. SI-CERT ob zaključenem incidentu s podajo poročila agenciji opiše ugotovljene vzroke za posamezni incident, uporabljene metode v njem in njegove posledice. Na podlagi tega se izoblikuje priporočila, ki jih lahko agencija upošteva pri nadaljnjih dopolnitvah predpisanih ali priporočenih zaščitnih ukrepov za operaterje. Tak proces omogoča, da se ukrepi ščitenja dopolnjujejo skupaj z razvojem storitev in novimi načini zlorab in napadov na informacijske sisteme in storitve na omrežjih.

SI-CERT utemeljuje svojo obrazložitev, da zakon v zgoraj citiranih členih daje pravno podlago za sodelovanje med agencijo in SI-CERT, zato se jim zdi primerno, da se v Splošnem aktu to sodelovanje opiše. Po njihovem mnenju bo Splošni akt s predlagano dikcijo tako pripomogel tudi k odzivanju na incidente, pomoči operaterjem in dolgoročno izboljšanju splošne ravni varnosti računalniških omrežij in storitev v Sloveniji.

Agencija se s predlogi SI-CERT strinja in ga bo z manjšo dopolnitvijo upoštevala.

Generalna pripomba družbe GVO je, da se vsem operaterjem nalagajo enake obveznosti, ne glede na to, ali ti operaterji ponujajo storitve končnim uporabnikom ali zgolj ponujajo pasivno infrastrukturo ponudnikom storitev. Predlagajo, da se določene obveznosti predpiše zgolj operaterjem, ki dejansko ponujajo storitve končnim uporabnikom, saj se da na ta način izogniti nalaganju dvojnih obveznosti za ista omrežja (enkrat gre za obveznost ponudnika pasivne infrastrukture in enkrat za obveznost ponudnika storitev končnim uporabnikom, čeprav gre za isto omrežje). Na ta način je mogoče tudi bolj precizno definirati določene obveznosti in se na ta način izogniti dvomu v to, čigava obveznost je določena zahteva Splošnega akta - ali gre za obveznost ponudnika pasivne infrastrukture ali za obveznost ponudnika storitev končnim uporabnikom.

Agencija na pripombo družbe GVO pojasnjuje, da 79. člen ZEKom-1 v prvem odstavku nalaga vsem operaterjem obveznost, da sprejmejo ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanja tveganja za varnost omrežja in storitev. V skladu z navedenim gre torej za obveznost, ki jo je zakonodajalec naložil tako operaterjem omrežja (ponudniki pasivne infrastrukture) kot operaterjem izvajalcem storitev (ponudniki storitev končnim uporabnikom) in zaradi tega agencija predloga ne bo upoštevala. Predlog splošnega akta je splošne narave in je primeren za vse operaterje. Operater bo z določitvijo obsega in meje sistema upravljanja varovanja informacij ter z analizo tveganj ugotovil kateri ukrepi so za operaterja primerni.

GVO nadalje navaja, da so v predlogu 14. člena Splošnega akta predpisane zahteve glede obveščanja in poročanja agenciji, ko so presežene določene referenčne vrednosti. Te so

predpisane v odstotkih prizadetih končnih uporabnikov glede na vrsto storitve. GVO navaja, da kot ponudnik izključno pasivne infrastrukture ponudnikom storitve nima vpogleda v dejanske storitve, ki jih ponudniki storitev zagotavljajo končnim uporabnikom, zato ne more vedeti, kdaj so te referenčne vrednosti (ki so pogoj za obveščanje in poročanje agenciji) dosežene. Predlagajo, da se 14. člen spremeni oz. dopolni tako, da se dolžnost poročanja omeji izključno na operaterje, ki zagotavljajo storitve končnim uporabnikom. S tem bo zahteva glede poročanja bolj natančno predpisana, hkrati pa bo na ta način izginil dvom glede nosilca obveznosti iz Splošnega akta.

Agencija se ne strinja s predlogom GVO, da se dolžnost poročanja omeji le na operaterje, ki zagotavljajo storitve končnim uporabnikom. ZEKom-1 v VII. poglavju vsem operaterjem brez izjeme nalaga enake obveznosti, pri čemer tudi GVO kot infrastrukturni operater ne more biti izjema. Agencija te pripombe ne bo upoštevala. Kljub temu, agencija se strinja, da je potrebno pri obveščanju in poročanju ločiti med ponudnikom storitev za končne uporabnike in ponudnikom omrežja z vidika tipa podatkov, ki jih operaterji poročajo. Agencija bo upoštevala in ustrezno preoblikovala 14. člen predloga splošnega akta.

Družba T-2 d.o.o. predlaga, da se v Splošnem aktu bolj določno in natančno opredeli terminologija ter, da se v čim večji meri poenoti z terminologijo, ki je že uporabljena v zakonu. Kot navajajo, iz definiciji predloga Splošnega akta izhaja, da sta Sistem upravljanja varovanja informacij (SUVI) kot Sistem neprekinjenega poslovanja (SUNP) vsak zase del celotnega sistema upravljanja, pri čemer prvi temelji na pristopu poslovnega tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij, drugi pa na strateški in taktični sposobnosti operaterja, da pripravi načrt za primere incidentov in motenj pri poslovanju ter se nanje odzove, da lahko zagotovi neprekinjeno izvajanje storitev prek svojega omrežja na sprejemljivi vnaprej določeni ravni. Glede na navedeno in glede na določila zakona družba T-2 sklepa, da gre za ločeni področji, ki se v določeni meri prekrivata. Iz 3. člena predloga pa izhaja podrejenost SUNP SUVI, saj SUNP v začetku prvega odstavka člena ni omenjen. Glede na to, da se v nadaljevanju splošnega akta omenjata oba termina, T-2 predlaga uporabo enotne terminologije tudi v tem delu.

Agencija na pripombo družbe T-2 pojasnjuje, da so SUVI, SUNP in drugi morebitni sistemi upravljanja (kakovost, okolje itd.) del enotnega sistema upravljanja in se med seboj dopolnjujejo. Agencija se strinja s pripombo, da tako kot se sedaj glasi 3. člen splošnega akta, kaže na podrejenost SUNP SUVI, kar pa ne drži. Agencija bo upoštevala pripombo družbe T-2.

Nadalje T-2 navaja, da so v 14. členu predloga Splošnega akta zapisani pogoji, ob katerih mora operater obvestiti agencijo in jih poročati o vseh kršitvah varnosti omrežij in storitev. Predlagajo, da bi bilo potrebno dodatno določiti ali so navedene referenčne vrednosti določene glede na dejansko število uporabnikov v trenutku, ko pride do incidenta ali glede na neko povprečno ocenjeno vrednost. Smatrajo, da je v posameznem trenutku pri določenih storitvah dejansko število uporabnikov zelo težko, če že ne nemogoče določiti. Zaradi morebitnim nejasnostim v tem delu in potencialnim težavam, predlagajo, da se Splošni akt v tem delu dopolni.

Agencija bo predlog delno upoštevala in ustrezno spremenila 14. člen predloga splošnega akta.

SOEK predlaga, da se rok za izdelavo vodstvenega pregleda, ki je opredeljen v 15. točki 1. odstavka 2. člena, podaljša za dve leti. V svoji obrazložitvi navajajo, da se je v primerjavi s predhodnim Splošnim aktom o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov obseg SUVI analize razširil, saj je potrebno 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 različni zaposleni pri operaterju, ki podrobneje poznajo delovanje in varovanje določenega sredstva. Ker je teh sredstev veliko, ki bi jih operater moral pregledovati v okviru varnostnega načrta, predlagajo, da se rok za izdelavo vodstvenega pregleda poveča na dve leti.

Agencija na pripombo SOEK pojasnjuje, da se s tem splošnim aktom obseg zahtev SUVI v primerjavi s Splošnim aktom o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov ni bistveno spremenil. Novost je sistem upravljanja neprekinjenega poslovanja (SUNP) in se agencija strinja s SOEK, da bo potrebno za implementacijo ukrepov SUNP prehodno obdobje in bo to upoštevala.

Agencija na pripombo SOEK v zvezi z rokom za izvedbo vodstvenega pregleda pojasnjuje, da so zahteve predloga splošnega akta povzete po standardu SIST ISO/IEC 27001, ki predstavlja dobro prakso na področju zagotavljanja varnosti. Omenjeni standard priporoča izvajanje vodstvenega pregleda najmanj enkrat letno oz. ob vsaki spremembi poslovanja, organizacije itd. Vodstveni pregled, za razliko od notranjih presoj, ni tako zahtevna naloga saj pomeni le-to, da mora operater najmanj enkrat letno pregledati rezultate notranjih presoj, oceniti možnost za izboljšave in morebitne potrebe po spremembi sistema upravljanja, in zaradi tega agencija predloga za spremembo roka ne bo upoštevala.

Agencija na pripombo SOEK v zvezi z zahtevnostjo pregleda vseh sredstev (notranja presoja) pojasnjuje, da je program notranjih presoj potrebno načrtovati ob upoštevanju položaja in pomembnosti procesov in področij, ki so predmet notranjih presoj (2. odstavek 10. člena splošnega akta). To pomeni, da je potrebno določiti kriterije, obseg, pogostost in metode presoje. Pogostost notranjih presoj je s splošnim aktom določena na najmanj enkrat letno, obseg letnih notranjih presoj pa ni določen. Agencija bo delno upoštevala predlog in bo v splošnem aktu bolj natančno pojasnila načrtovanje notranjih presoj.

Nadalje SOEK predla, da se definicije v 2. členu Splošnega akta spremenijo in dopolnijo tako:

- da se v definiciji celovitosti omrežja briše besedilo »enega ali več«
- da se pri definiciji incidenta doda primeroma naštete dogodke, smiselno enako, kot je to v trenutno uporabljenem 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 omrežje oz. informacijskega sistema, človeške napake, delavske stavke itd., vse v kolikor vplivajo na omrežje in storitev«

V svoji obrazložitvi navajajo, da se načrtovanje nepredvidenih dogodkov na predlagani ravni (z veliko verjetnostjo) obravnava vsak predviden incident posebej zato je smiseln popravek 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.

Agencija bo upoštevala pripombo SOEK v zvezi s predlogom, da se v definiciji celovitosti omrežja briše besedilo »enega ali več«, ker je že po definiciji incident eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, varnost omrežij in storitev ali celovitost omrežja.

Agencija ne bo upoštevala pripombo SOEK v zvezi s predlogom, da se pri definiciji incidenta doda primeroma naštete dogodke, ker bi bil že nabor možnih skupin dogodkov izredno obsežen in nikoli v popolnosti zajet.

Nadalje SOEK predlaga, da se doda nov člen, ki bi jasno določil minimalni nabor storitev pri katerih morajo biti zagotovljeni organizacijski ukrepi iz tega Splošnega akta – smiselno je uporabiti kriterije podobno kot pri 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).*

Agencija na pripombo SOEK pojasnjuje, da ZEKom-1 zahteva od operaterjev sprejetje ustreznih tehničnih in organizacijskih ukrepov za ustrezno obvladovanje tvegana za varnost omrežij in storitev. Agencija pripombe SOEK ne bo upoštevala, ker se ZEKom-1 ne omejuje na kakšno specifično omrežje ali storitev. V zvezi s komentarjem, da bi določil minimalni nabor storitev za SUVI in SUNP podobno kot za obveščanje in poročanje, agencija pojasnjuje, da se ti podatki zbirajo za potrebe Evropske komisije in ENISE, ki je priporočila o katerih kršitvah varnosti in celovitosti je treba poročati. V tem smislu je bil tudi oblikovan 14. člen splošnega akta.

Nadalje SOEK predlaga, 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. SOEK v svoji obrazložitvi navaja, da 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 kolikšnem 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.

Agencija na pripombo SOEK pojasnjuje, da je oblikovanje varnostnega načrta in načrta za zagotavljanje celovitosti omrežja prepuščena operaterju, to se pravi lahko sta ločena dokumenta ali združena. Pomembno je, da ta dokument oz. dokumenta vsebujejo zahteve iz 12. oz. 13. člena splošnega akta. Pričakovano je, da bo veliko incidentov skupnih, ki bodo imeli negativni vpliv tako na varnost omrežij in storitev kakor na celovitost omrežja. Pri ukrepih bo potrebno načrtovati in obravnavati dva vidika: kako v primeru incidenta zmanjšati varnostna tveganja (varnost omrežij in storitev) in kako ravnati oz. katere ukrepe je potrebno sprejeti, da se v najkrajšem možnem času ponovno zagotovi izvajanje storitev (celovitost omrežja). Agencija v splošnem aktu ne bo predpisala obliko dokumenta (samostojen, ločen obliko itd.).

SOEK predlaga, da se določila o izdelavi dokumenta – izjavi o uporabnosti, ki ga je potrebno pripraviti v okviru dokumentacije SUVI, odstrani iz Splošnega akta oz. smiselno vključi

znotraj dokumentov notranje presoje in vodstvenega pregleda SUVI in SUNP. Iz besedila Splošnega akta domnevajo, da je izjava o uporabnosti podrobneje opredeljena v 9. členu, v katerem je opisana vsebina izjave o uporabljenih ukrepih. Kot navajajo, 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.

Agencija se strinja s pripombo SOEK in jo bo upoštevala.

SOEK predlaga, da se v okviru zahtev 9. člena Splošnega akta, ki obravnava zapisa o incidentih, vodijo le zapisi o tistih incidentih, ki so vplivali na varnost omrežij in storitev, celovitost omrežja ali delovanje operaterja v izrednih razmerah, ne pa zapise o vseh incidentih, kot je zapisano v predlogu Splošnega akta. V svoji obrazložitvi predlog utemeljujejo, da operaterji zagotavljajo več telekomunikacijskih storitev, ter da bi redno beleženje vsake napake bodisi znotraj posamezne strojne ali programske naprave ali pa na podlagi npr. tiskarske napake zaposlenega operaterju povzročilo veliko stroškov dela, izdelan zapis incidentov pa tako agenciji kot operaterju ne bi prispeval v večji varnosti omrežij in storitev.

Agencija pojasnjuje, da splošni akt ne obravnava izjemnih stanj, tako da bo v 8. členu brisala »ali delovanje operaterja v izjemnih stanjih«. Agencija na pripombo SOEK pojasnjuje, da zaznavanje incidentov in beleženje le-teh koristi predvsem operaterju. Obravnava teh zapisov, v okviru analize tveganja, bodo koristili operaterju pri dopolnjevanju morebiti neprepoznanih ali neupoštevanih grožnjah in ranljivostih sistema ter implementaciji morebitnih novih ukrepih, ki bodo zmanjšali vpliv teh dogodkov na varnost omrežij in storitev ter celovitost omrežja. Ker operaterju ni treba voditi zapise o vseh incidentih, temveč le o incidentih, ki so vplivali na varnost omrežij in storitev ter celovitost omrežja, agencija pripombe SOEK ne bo upoštevala.

SOEK predlaga, da se 1. odstavek 14. člena splošnega akta, ki obravnava čas obveščanja incidenta, spremeni v smislu, da se loči začetno obveščanje, ki ga mora operater izvesti takoj, ko je mogoče in podrobnejše poročanje, ki ga mora operater izvesti najpozneje v treh delovnih dneh po zaključku incidenta. V obrazložitvi svoj predlog utemeljujejo, da ob zaznavi kršitve varnosti omrežja oz. storitev operater vsa svoja razpoložljiva sredstva posveti 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 zaznav kršitve varnosti omrežja oz. storitev, vsi relevantni podatki še niso znani, zato menijo, da je 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 podlagi teh agenciji posredoval podrobnejše informacije.

SOEK nadalje v zvezi z 14. členom splošnega akta, ki določa mejne parametre poročanja ugotavlja, da so mejni parametri v tem členu pisani splošno in jih je težko definirati in določiti. Prav tako smatrajo, da 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 ugotovijo 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). Predlagajo jasnejše in racionalnejše opredelitve.

Nadalje 2. odstavek 14. člena Splošnega akta opredeljuje dolžnost beleženja in poročanja kršitev ter vpliv na storitve. V zvezi s tem členom SOEK opozarja, da ponudniki pasivne infrastrukture ne smejo biti izvzeti (primeri odprtih širokopasovnih omrežij). Ker ni povsem jasno ali ti ponudniki zajeti z medomrežnimi povezavami (ponudniki namreč ne nudijo storitev glede na definicijo 32. točke 3. člena zakona), predlagajo, da se po potrebi 2. odstavek 14. člena ustrezno dopolni.

SOEK opozarja, da je ocena števila prizadetih uporabnikov res zelo približna, saj na njen izračun vpliva več dejavnikov, ki jih nimajo pod nadzorom. Navajajo, da pride tudi do situacij, ko ocene niti ne morejo pridobiti, zato predlagajo, da se to ustrezno zapiše v Splošni akt in da se oceno predloži le, ko je to mogoče. Predlagajo, da se v 14. člen Splošnega akta doda nov odstavek, ki bi določal, da »Operater oceno % prizadetih uporabnikov in oceno števila prizadetih uporabnikov pripravi ob upoštevanju realnih podatkov ali če to ni praktično izvedljivo ali če bi bilo povezano z dolgotrajnimi postopki ali večjimi stroški, na podlagi ocene operaterja«. Kot je navedeno v pripombah v zvezi s poročanjem in mejnimi parametri SOEK smatra, da je predlog akta v tem delu nejasen. S predlagano spremembo se lahko akt po njihovem mnenju uporablja in izvaja tudi v praksi brez nepotrebnih zapletanj s tolmačenjem.

Agencija bo predloge delno upoštevala in ustrezno spremenila 14. člen predloga splošnega akta.

V predlogu splošnega akta je predlagano, da akt začne veljati naslednji dan po objavi v Uradnem listu. SOEK predlaga, da zaradi ustrezne uskladitve z zadevnim Splošnim aktom, 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.

Agencija se strinja s pripombo SOEK in jo bo upoštevala.

Franc Dolenc
Direktor