NEURADNI ČISTOPIS

Na podlagi 86. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 - ZIN-B in 54/14 - odl. US) izdaja direktor Agencije za komunikacijska omrežja in storitve Republike Slovenije

S P L O Š N I A K T

o varnosti omrežij in storitev ter delovanje v izjemnih stanjih

I. SPLOŠNE DOLOČBE

1. člen

(vsebina)

Ta splošni akt določa organizacijske ukrepe, ki jih morajo sprejeti operaterji za ustrezno zagotavljanje varnosti omrežij in storitev, celovitosti omrežij ter delovanja v izjemnih stanjih.

2. člen

(pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu, imajo naslednji pomen:

1. Agencija je neodvisen regulativni organ, katere pristojnosti, organizacija in delovanje določa Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, v nadaljevanju: ZEKom-1).

2. SI-CERT je nacionalni odzivni center za omrežne incidente, ki deluje v okviru javnega zavoda Akademska in raziskovalna mreža Slovenije (ARNES).

3. Sistem upravljanja varovanja informacij (v nadaljevanju: SUVI) je tisti del celotnega sistema upravljanja, ki temelji na pristopu poslovnega tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij.

4. Sistem upravljanja neprekinjenega poslovanja (v nadaljevanju: SUNP) je tisti del celotnega sistema upravljanja, ki temelji na strateški in taktični sposobnost 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.

5. Varnost omrežja in storitev je zmožnost javnega komunikacijskega omrežja, da z določeno stopnjo gotovosti prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo zaupnost, verodostojnost, celovitost ali razpoložljivost shranjenih ali prenesenih podatkov ter s tem povezanih javno dostopnih komunikacijskih storitev, ki jih ponujajo ta omrežja in ali so prek njih dostopne.

6. Celovitost omrežja je zmožnost omrežja, da z veliko verjetnostjo zagotovi neprekinjeno izvajanje storitev prek teh omrežij v primeru incidentov.

7. Sredstvo je vse, kar ima določeno vrednost za operaterja, za njegovo dejavnost ali izvajanje storitev.

8. Incident je eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo ogrozili varnost omrežij in storitev ali celovitost omrežja.

9. Grožnja je možen vzrok za incident, ki lahko povzroči škodo sredstvu, omrežju ali operaterju.

10. Ranljivost je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami.

11. Analiza varnostnih tveganj je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost omrežij in storitev.

12. Analiza vpliva na poslovanje je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za neprekinjeno izvajanje storitev.

13. Obravnava tveganj je proces izbora in vpeljave ukrepov za zmanjševanje tveganj.

14. Preostalo tveganje je tveganje, ki ostane po obravnavi tveganj.

15. Dokumentiran postopek pomeni, da je postopek zapisan.

16. Vodstveni pregled je dokumentiran pregled, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi ustreznost in učinkovitost SUVI in SUNP.

17. Sistem zaščite in reševanja obsega programiranje, načrtovanje, organiziranje, izvajanje, nadzor, financiranje ukrepov ter dejavnosti za varstvo pred naravnimi in drugimi nesrečami.

(2) Ostali pojmi, uporabljeni v tem splošnem aktu, imajo enak pomen, kot je določen v ZEKom-1.

3. člen

(dokumentacija)

(1) Operater mora vzpostaviti in vzdrževati dokumentiran SUVI in SUNP, ki mora obsegati najmanj:

- varnostno politiko in politiko neprekinjenega poslovanja,
- obseg in meje SUVI ter SUNP,
- navodilo za izvajanje analize in obravnave varnostnih tveganj,
- navodilo za izvajanje analize vpliva na poslovanje in obravnave tveganj za neprekinjeno poslovanje,
- varnostni načrt,
- načrt za zagotavljanje celovitosti omrežja,
- zapise o incidentih, notranjih presojah in vodstvenih pregledih SUVI in SUNP.

(2) Za dokumente iz prvega odstavka tega člena mora operater vzpostaviti dokumentiran sistem, ki bo zagotavljal:

- odobritev dokumentov, preden so objavljeni,
- pregledovanje in dopolnjevanje dokumentov,
- uporabo najnovejših verzij ustreznih dokumentov in
- da bodo dokumenti na razpolago tistim, ki jih potrebujejo.

4. člen

(varnostna politika in politika neprekinjenega poslovanja)

Varnostna politika in politika neprekinjenega poslovanja je dokument ali zbirka dokumentov, s katerim operater uradno izraža splošen namen in usmeritev SUVI in SUNP. Politika ravnanja v izjemnih stanjih je del politike neprekinjenega poslovanja. Operater mora v varnostni politiki in politiki neprekinjenega poslovanja (v nadaljevanju: politika) določiti cilje in načela za ukrepanje pri zagotavljanju varnosti omrežij in storitev, celovitosti omrežij in delovanja v izjemnih stanjih. Najvišje vodstvo operaterja mora odobriti politiko. Politika mora upoštevati poslovne, pravne in zakonodajne zahteve ter pogodbene obveznosti pri zagotavljanju varnosti omrežja in storitev, celovitosti omrežja ter delovanja v izjemnih stanjih.

5. člen

(obseg in meje SUVI ter SUNP)

Operater mora opredeliti obseg in meje SUVI in SUNP z vidika značilnosti svojega poslovanja, organizacije, lokacije, velikosti, tehnologije in zahtev VII. poglavja ZEKom-1.

6. člen

(navodilo za izvajanje analize in obravnave varnostnih tveganj)

(1) Navodilo za izvajanje analize in obravnave varnostnih tveganj opredeljuje metodologijo, ki jo je operater izbral za izvajanje analize varnostnih tveganj, kriterije za izbor varnostnih ukrepov, sprejemljivo raven tveganja ter postopek obravnave preostalih tveganj.

(2) Metodologija za oceno varnostnih tveganj mora biti izbrana tako, da bodo rezultati ocene varnostnih tveganj primerljivi in ponovljivi.

(3) Operater mora v rednih časovnih intervalih analizirati in obravnavati varnostna tveganja.

7. člen

(navodilo za izvajanje analize vpliva na poslovanje)

(1) Navodilo za izvajanje analize vpliva na poslovanje opredeljuje metodologijo, ki jo je operater izbral za izvajanje analize tveganj za neprekinjeno izvajanje storitev prek svojega omrežja, kriterije za izbor ukrepov in sprejemljivo raven tveganja.

(2) Metodologija za oceno tveganj za neprekinjeno poslovanje mora biti izbrana tako, da bodo rezultati te ocene tveganj primerljivi in ponovljivi.

(3) Operater mora v rednih časovnih intervalih analizirati in obravnavati tveganja za neprekinjeno izvajanje storitev prek svojega omrežja.

8. člen

(zapisi o incidentih)

Operater mora voditi zapise o vseh incidentih, ki so vplivali na varnost omrežij in storitev ali celovitost omrežja. Operater mora te zapise hraniti najmanj eno leto.

9. člen

(notranje presoje SUVI in SUNP)

(1) Operater mora najmanj enkrat letno izvajati notranje presoje SUVI in SUNP, da ugotovi ali so cilji ukrepov, ukrepi, procesi in postopki:

- v skladu z zakonskimi zahtevami,
- ustrezno in učinkovito vpeljani in vzdrževani.

(2) Program notranjih presoj je potrebno načrtovati ob upoštevanju položaja in pomembnosti procesov in področij, ki so predmet notranje presoje, kot tudi ob upoštevanju rezultatov predhodnih presoj. Program notranjih presoj mora zagotoviti, da se v treh letih pregledajo vsi cilji ukrepov, ukrepi, procesi in postopki. Notranje presoje sistema morajo opraviti posamezniki, ki niso povezani s področjem podvrženem pregledu. Posamezniki morajo za izvajanje tovrstnih pregledov imeti ustrezno znanje in izkušnje.

(3) O rezultatih notranjih presoj je potrebno voditi zapise. Operater mora te zapise hraniti najmanj pet let.

10. člen

(vodstveni pregled SUVI in SUNP)

(1) Vodstvo operaterja mora najmanj enkrat letno pregledovati rezultate notranjih presoj, oceniti možnosti za izboljšave in potrebe po spremembi SUVI in SUNP.

(2) Rezultat vodstvenega pregleda so odločitve in ukrepi za izboljšanje učinkovitosti SUVI in/ali SUNP ali morebitne spremembe SUVI in/ali SUNP.

(3) O rezultatih vodstvenega pregleda je potrebno voditi zapise. Operater mora te zapise hraniti najmanj pet let.

II. VARNOST OMREŽIJ IN STORITEV

11. člen

(varnostni načrt)

(1) Varnostni načrt je dokumentirana zbirka ukrepov, postopkov in informacij, ki so izdelani, zbrani in pripravljeni za:

- zmanjševanje varnostnih tveganj in
- uporabo v primeru incidenta z namenom zmanjšanja negativnih učinkov in omilitev posledic.

(2) Operater mora izdelati, izvajati, spremljati in izboljševati varnostni načrt v skladu z navodili za izvajanje analize varnostnih tveganj in tretjim odstavkom 79. člena ZEKom-1.

12. člen

(načrt za zagotavljanje celovitosti omrežja)

(1) Načrt za zagotavljanje celovitosti omrežja je dokumentirana zbirka ukrepov, postopkov in informacij, ki so izdelani, zbrani in pripravljeni za:

- zagotavljanje neprekinjenega izvajanja storitev in
- uporabo v primeru incidenta z namenom, da se v najkrajšem možnem času zagotovi ponovno izvajanje storitev.

(2) Operater mora izdelati, izvajati, spremljati in izboljševati načrt za zagotavljanje celovitosti omrežja na podlagi analize vpliva na poslovanje in zajema najmanj:

- opredelitev vseh tveganj in groženj znotraj in zunaj operaterja, ki bi lahko ogrozili neprekinjeno izvajanje storitev,
- opredelitev verjetnosti pojava vseh groženj, ki bi lahko ogrozile neprekinjeno izvajanje storitev,
- opredelitev verjetnosti, da bo grožnja izrabila ranljivost,
- opredelitev pričakovanega časa za ponovno vzpostavitev izvajanja storitev za vsa prepoznana tveganja,
- določitev ukrepov za zmanjšanje tveganj na sprejemljivo raven.

13. člen

(obveščanje in poročanje)

(1) Operater mora takoj, ko to zazna, obvestiti agencijo o vseh kršitvah varnosti omrežij in storitev ali celovitosti omrežij, če te lahko pomembno vplivajo na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev. V kolikor ob sami zaznavi incidenta vsi relevantni podatki še niso znani, se le-te pošlje agenciji najkasneje v treh delovnih dneh po odpravi incidenta.

(2) Operater mora za vsak incident poročati:

- čas nastanka in trajanja incidenta,
- oceno števila prizadetih naročnikov po posamezni storitvi,
- statistično regijo prizadetih uporabnikov,
- vpliv na omrežje in storitve,
- vpliv na druga povezana omrežja in operaterje,
- popis vzrokov in posledic incidenta,
- izvedeni ukrepi po incidentu.

(3) Operater, ki zagotavlja storitve končnim uporabnikom, obvešča agencijo, ko je incident presegel enega od naslednjih referenčnih vrednosti:

- vpliv je trajal več kot eno uro in je prizadel več kot 15 % vseh naročnikov po posamezni storitvi,

- vpliv je trajal več kot dve uri in je prizadel več kot 10 % vseh naročnikov po posamezni storitvi,
- vpliv je trajal več kot štiri ure in je prizadel več kot 5 % vseh naročnikov po posamezni storitvi,
- vpliv je trajal več kot šest ur in je prizadel več kot 2 % vseh naročnikov po posamezni storitvi,
- vpliv je trajal več kot osem ur in je prizadel več kot 1 % vseh naročnikov po posamezni storitvi.

(4) Operater, ki zagotavlja storitve končnim uporabnikom najmanj beleži in poroča kršitve iz prvega odstavka tega člena, ki so vplivale na:

- govorne storitve na fiksni lokaciji,
- govorne storitve v javnih brezžičnih omrežjih,
- širokopasovne storitve na fiksni lokaciji,
- širokopasovne 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.

(5) Operater omrežja najmanj beleži in obvešča agencijo, ko je incident pomembno vplival na zagotavljanje komunikacijskih storitev prek teh omrežij.

(6) Operater omrežja namesto števila prizadetih naročnikov poroča o številu prizadetih medomrežnih aktivnih ali pasivnih povezav in pripadajočih zmogljivosti.

(7) Pri storitvah, ki se zagotavljajo na fiksni lokaciji se ob incidentu poroča število nedelujočih priključkov oziroma število nedelujočih medomrežnih (aktivnih/pasivnih) povezav.

(8) V javnih brezžičnih omrežjih se ob incidentu poroča število prizadetih aktivnih uporabnikov. Podatek števila prizadetih je ocena in temelji na podlagi statistike in meritev, ki so bile opravljene na posamezni javni brezžični dostopovni točki (bazni postaji, WLAN itd.) pred incidentom za dobo zadnjih treh mesecev.

(9) Operater izvajalec storitev število prizadetih uporabnikov pripravi ob upoštevanju realnih podatkov. V kolikor to ni izvedljivo ali če bi bilo povezano z dolgotrajnimi postopki ali večjimi stroški, število prizadetih temelji na podlagi ocene operaterja.

(10) Poročanje o incidentih se izvaja elektronsko. Če dejanske in tehnične možnosti tega ne dopuščajo, se poročanje izvaja preko glavne pisarne agencije ali na drug primeren način.

14. člen

(obravnava incidenta omrežne in informacijske varnosti)

(1) Agencija operativno razreševanje incidenta omrežne in informacijske varnosti preda po potrebi in glede na kršitev 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 operaterju in Agenciji o poteku obravnave in rezultatih, skupaj z morebitnimi priporočenimi ukrepi za izboljšanje varnosti omrežja in storitev.

II.a DELOVANJE V IZJEMNIH STANJIH

14.a člen

(obseg in meje SUNP v izjemnih stanjih)

(1) Operater, ki ima sklenjeno pogodbo ali dogovor z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja, in operater, ki z njim sodeluje po prvem odstavku 14.b člena tega

splošnega akta, mora identificirati tiste dele omrežja, ki so nujni za nemoteno delovanje omrežij nosilcev varnostnega in obrambnega sistema ter sistema zaščite in reševanja v izjemnih stanjih.

(2) Operater, ki zagotavlja javna telefonska omrežja, mora identificirati omrežne priključne točke, ki jim je dodeljena funkcija prednosti v skladu z uredbo, ki ureja pravice do omrežnih priključnih točk s prednostjo.

14.b člen

(ukrepi za zagotavljanje celovitosti omrežja v izjemnih stanjih)

(1) Operater, ki ima sklenjeno pogodbo ali dogovor z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja mora načrt za zagotavljanje celovitosti omrežja iz 12. člena tega splošnega akta dopolniti z relevantnimi ukrepi iz tretjega odstavka tega člena. V primeru sodelovanja z ostalimi operaterji je dolžan te ukrepe medsebojno uskladiti na način, da se zagotovi nemoteno delovanje omrežij nosilcev varnostnega in obrabnega sistema ter sistema zaščite in reševanja v izjemnih stanjih. Ukrepi za ravnanje v izjemnih stanj se morajo predhodno uskladiti z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja.

(2) Operater, ki zagotavlja javna telefonska omrežja, mora načrt za zagotavljanje celovitosti omrežja iz 12. člena tega splošnega akta dopolniti z ukrepi iz tretjega odstavka tega člena, s katerimi se bo zagotovila funkcija prednosti komunikacije.

(3) Ukrepi za zagotavljanje celovitosti omrežja v izjemnih stanjih obsegajo najmanj:

- postopek dodeljevanja funkcije prednosti komunikacije določenega operaterja, postopek ohranjanja prednosti v omrežjih drugih operaterjev in postopek omejevanja ali prekinjanja preostalih telefonskih priključkov v omrežju operaterja,
- postopek vzpostavitve nadomestnih ter obhodnih poti v čim krajšem možnem času z minimalnim časom aktiviranja poti, določitve rezervnih naprav ter vseh potrebnih protokolov za uporabo,
- postopek vzpostavitve ustreznih varnostnih ukrepov na nadomestnih poteh,
- postopek usklajenega ukrepanja in medsebojni pomoči v primeru velikih naravnih in drugih nesreč,
- spisek vseh operaterjev, ki operaterju, ki ima sklenjeno pogodbo ali dogovor z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja, zagotavlja nadomestne ter obhodne poti ali katere koli druge povezave,
- določitev vseh nadomestnih, obhodnih poti in drugih povezav, ki operaterju, ki ima sklenjeno pogodbo ali dogovor z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja, zagotavljajo drugi operaterji,
- določitev odgovornih oseb operaterja in njihovih nalog glede poročanja o izrednih dogodkih, povezanih z zagotavljanjem funkcije prednosti in
- protokol obveščanja Nacionalnega centra za krizno upravljanje in protokol obveščanja Centra za obveščanje Republike Slovenije.

III. PREHODNA IN KONČNA DOLOČBA

15. člen

(uskladitev SUNP)

Operaterji morajo svoj SUNP uskladiti z določbami tega splošnega akta v roku 3 mesecev od začetka veljavnosti tega splošnega akta.

16. člen

(začetek veljavnosti)

Ta splošni akt začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.