PREDLOG

Na podlagi 86. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/2012) izdaja direktor Agencije za pošto in elektronske komunikacije Republike Slovenije

SPLOŠNI AKT

o varnosti omrežij in storitev

I. SPLOŠNE DOLOČBE

1. člen
(vsebina)

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

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. 109/2012, v nadaljevanju: ZEKom-1).
2. 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.
3. 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.
4. 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.
5. Celovitost omrežja je zmožnost omrežja, da z veliko verjetnostjo zagotovi neprekinjeno izvajanje storitev prek teh omrežij v primeru enega ali več incidentov.
6. Sredstvo je vse, kar ima določeno vrednost za operaterja, za njegovo dejavnost ali izvajanje storitev.
7. Incident je eden ali več neželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo ogrozili varnost omrežij in storitev ali celovitost omrežja.
8. Grožnja je možen vzrok za incident, ki lahko povzroči škodo sredstvu, omrežju ali operaterju.
9. Ranljivost je šibka točka sredstva ali skupine sredstev, ki jo je mogoče izrabiti z eno ali več grožnjami.
10. Analiza varnostnih tveganj je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za varnost omrežij in storitev
11. Analiza vpliva na poslovanje je sistematična uporaba informacij za prepoznavanje virov groženj in ranljivosti sredstev ter ocenjevanje tveganj za neprekinjeno izvajanje storitev.
12. Obravnava tveganj je proces izbora in vpeljave ukrepov za zmanjševanje tveganj.
13. Preostalo tveganje je tveganje, ki ostane po obravnavi tveganj.
14. Dokumentiran postopek pomeni, da je postopek zapisan.
15. Vodstveni pregled je dokumentiran pregled, ki ga vodstvo opravi najmanj enkrat letno, da zagotovi ustreznost in učinkovitost SUVI in SUNP.

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

3. člen

(dokumentacija)

(1) Operater mora vzpostaviti in vzdrževati dokumentiran SUVI, 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,
- izjavo o uporabnosti.

(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,
- da bodo dokumenti na razpolago tistim, ki jih potrebujejo.

4. člen

(varnostna politika in politika neprekinjenega poslovanja)

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

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 ocene varnostnih 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, celovitosti omrežja ali delovanje operaterja v izjemnih stanjih. Operater mora te zapise hraniti najmanj eno leto.

9. člen

(izjava o uporabljenih ukrepih)

(1) Izjava o uporabljenih ukrepih je dokumentiran povzetek odločitev v zvezi z obravnavo tveganj.

(2) Izjava o uporabljenih ukrepih mora vsebovati:
- vse cilje ukrepov in ukrepe, ki so trenutno vpeljani in razloge za izbor,
- spisek ukrepov iz priloge tega splošnega akta, ki niso uporabljeni in obrazložitev razlogov za njihovo izključitev.

10. 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. 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.

11. 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

12. 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 zakona.

13. 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.

14. člen

(obveščanje in poročanje)

(1) Operater mora 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 in so presegli eno od naslednjih referenčnih vrednosti (mejnih parametrov):

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

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

(2) Operater 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,
- 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 xxx in
- medomrežne povezave.

(3) Operater mora za vsak incident, opredeljen v prvem in drugem odstavku tega člena, navesti:

- čas nastanka in trajanja incidenta,
- oceno števila prizadetih uporabnikov,
- 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.

(4) 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.

III. KONČNE DOLOČBE

15. člen

(začetek veljavnosti)

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

(2) Z dnem uveljavitve tega splošnega akta se preneha uporabljati Splošni akt o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov (Uradni list RS št. 126/08).