PREDLOG!

Na podlagi drugega odstavka 118. člena in drugega odstavka 119. člena ter četrtega odstavka 208. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) izdaja Agencija za komunikacijska omrežja in storitve Republike Slovenije

SPLOŠNI AKT
o obveščanju in vrednotenju varnostnih incidentov

1. člen
(vsebina splošnega akta)

(1) Ta splošni akt določa, v katerih primerih gre za pomemben vpliv varnostnih incidentov na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev, glede katerih morajo operaterji obveščati Agencijo za komunikacijska omrežja in storitve Republike Slovenije (v nadaljnjem besedilu: agencija) in nacionalno skupino za obravnavanje incidentov kot je določena v zakonu, ki ureja informacijsko varnost (v nadaljnjem besedilu: nacionalni CSIRT).

(2) Ta splošni akt določa tudi, kdaj gre za majhen, velik ali zelo velik negativen vpliv varnostnih incidentov na varnost omrežij in storitev operaterjev.

(3) Ta splošni akt določa tudi najave dograditev, posodobitev in vzdrževanja omrežja uporabnikom in agenciji ter obveščanje uporabnikov v primeru večjih omejitev ali prekinitev storitev zaradi okvar ali napak.

2. člen
(obveščanje o varnostnih incidentih)

(1) Operaterji morajo brez nepotrebnega odlašanja oziroma največ v 24 urah po zaznavi varnostnega incidenta, če je ta pomembno vplival na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev, v skladu z merili iz prvega odstavka 3. člena tega splošnega akta, obvestiti agencijo in nacionalni CSIRT.

(2) V primeru, da varnostni incident iz prejšnjega odstavka prizadene tudi komunikacije v sili, operater hkrati obvesti tako agencijo in nacionalni CSIRT kot tudi zadevni center za sprejem komunikacije v sili.

(3) Če podatki o vplivu ali obsegu varnostnega incidenta ob zaznavi incidenta še niso znani, operater agenciji in nacionalnemu CSIRT s prvim obvestilom sporoči le tiste podatke iz 4. člena tega splošnega akta, ki so mu znani, ostale podatke pa najkasneje v roku 72 ur, od kar se z njimi seznani. Operater najkasneje v desetih dneh po odpravi varnostnega incidenta obvesti agencijo in nacionalni CSIRT o ostalih zahtevanih informacijah iz 4. člena tega splošnega akta. Če ima dogodek večdnevni pomemben vpliv na omrežje, storitve ali uporabnike, operater vsaj enkrat dnevno poroča agenciji in nacionalnemu CSIRT o dogajanju, o čemer obema v roku desetih dni po vzpostavitvi normalnega delovanja posreduje še končno poročilo.

(4) Obveščanje pristojnih organov o varnostnih incidentih se izvaja praviloma po elektronski poti, agenciji pa preko portala za poročanje. Če dejanske in tehnične možnosti tega ne dopuščajo, se obveščanje izvaja preko glavne pisarne agencije in nacionalnega CSIRT ali na drug primeren način. Če situacija zaradi varnostnega incidenta zahteva takojšnje ukrepanje, operater o njem brez odlašanja dodatno obvesti nacionalni CSIRT še na dežurni telefon.

3. člen
(pomemben vpliv varnostnih incidentov)

(1) Za pomemben vpliv varnostnega incidenta na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev, o katerem mora operater obvestiti agencijo in nacionalni CSIRT gre v primerih, ko so izpolnjena naslednja merila:

1. vpliv na razpoložljivost njegovih omrežij ali storitev ali podatkov (odpoved ali ohromljeno delovanje elementov omrežja, funkcij ali pripadajočih informacijskih sistemov, onemogočen ali ohromljen dostop do elementov omrežja, storitev, podatkov, baz ipd.), ki jih zagotavlja, je presegel enega od naslednjih referenčnih vrednosti, in sicer:

a) varnostni incident je trajal več kot 15 minut in manj kot uro in je prizadel več kot 20% vseh uporabnikov po posamezni storitvi ali
b) varnostni incident je trajal več kot eno uro in je prizadel več kot 15% vseh uporabnikov po posamezni storitvi ter ali
c) varnostni incident je trajal več kot dve uri in je prizadel več kot 10% vseh uporabnikov po posamezni storitvi ali
č) varnostni incident je trajal več kot štiri ure in je prizadel več kot 5% vseh uporabnikov po posamezni storitvi ali
d) varnostni incident je trajal več kot šest ur in je prizadel več kot 2% vseh uporabnikov po posamezni storitvi ali
e) varnostni incident je trajal več kot osem ur in je prizadel več kot 1% vseh uporabnikov po posamezni storitvi ali

2. vpliv varnostnega incidenta na zaupnost komunikacij, in sicer na zaupnost podatkov o prometu iz 218. člena ZEKom-2 ali podatkov o uporabnikih iz 215. člena ZEKom-2, ter na avtentičnost in celovitost omrežja, je nastal zaradi:

a) nepooblaščenega razkritja, spremenjenih ali odtujenih prometnih, lokacijskih podatkov, dnevniških zapisov, gesel ali nastavitev ključnih delov omrežja, ne glede na čas trajanja ali število prizadetih ali
b) nepooblaščenega razkritja vsebine komunikacije (prestrezanje komunikacije) ne glede na število prizadetih ali
c) izvedenega ciljno usmerjenega napada na omrežje ali storitve operaterja kot so določene v 10. točki drugega odstavka 3. člena oziroma njegove uporabnike (DoS, DDoS, sabotaže, itd.), ki je povzročil izpad ali motnje storitev več kot 15 minut ali
č) izvedenega nepooblaščenega vdora ali vpogleda v bazo uporabnikov, v podporne informacijske sisteme ali omrežne elemente operaterja ali
d) varnostnega incidenta ali več ponavljajočih varnostnih incidentov zaradi ranljivosti ali neustreznih nastavitev ali procesov je vplivalo na celovitost ali avtentičnost

omrežja ali uporabnike in je bilo posredno ali neposredno prizadetih več kot 100 uporabnikov (goljufije, zlorabe in kibernetska kriminaliteta) ali

3. vpliv varnostnega incidenta na delovanje oziroma izvajanje:
   a) storitev komunikacij v sili:
      - vpliv na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ ali
      - zaradi nedelovanja ali ohromljenega delovanja omrežja operaterja je prizadetih več kot 100 uporabnikov te storitve ali
   b) storitev upravljavcev kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo kritično infrastrukturo ali
   c) storitev izvajalcev bistvenih storitev (v nadaljnjem besedilu: IBS) ali organov državne uprave (v nadaljnjem besedilu: ODU), kot so določeni v skladu z zakonom, ki ureja informacijsko varnost, če so mu poznani ali
   č) ključnih delov sistema varnosti države, če so mu poznani ali
   d) storitev, ki jih operater zagotavlja drugim operaterjem ali
   e) dostopovnega, agregacijskega vozlišča ali sisteme prenosa in je skupaj prizadeto več kot 1000 uporabnikov ali
   f) upravljanje omrežja ter njegovih nadzornih in varnostnih funkcij.

(2) Ne glede na merila, navedena v prejšnjem odstavku, lahko operater agencijo in nacionalni CSIRT obvesti tudi o drugih o varnostnih incidentih, za katere meni, da vplivajo na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev.

4. člen
(vsebina obvestila)

(1) Operater mora glede varnostnega incidenta v obvestilu navesti vse podatke, s katerimi razpolaga in se nanašajo na konkretni varnostni incident, in sicer:
   1. naziv operaterja,
   2. identifikacijsko oznako, pod katero operater sam vodi varnostni incident,
   3. kontaktne podatke odgovorne osebe na strani operaterja v zvezi z varnostnim incidentom,
   4. datum in čas nastanka varnostnega incidenta,
   5. celotno trajanje od nastanka oziroma prepoznave varnostnega incidenta do obnove normalnega delovanja,
   6. kateri ključni elementi varnosti so bili kršeni oziroma ogroženi v skladu s prvim odstavkom tretjega člena tega splošnega akta,
   7. oceno števila prizadetih oz. potencialno prizadetih uporabnikov po posameznih storitvah iz 10. točke tega odstavka,
   8. skupno ocenjeno število vseh prizadetih uporabnikov,
   9. skupno ocenjeno število vseh prizadetih uporabnikov zaradi razlogov, navedenih v 2. točki tega odstavka,
   10. opredelitev storitev, na katere je varnostni incident negativno vplival:
      a) zagotavljanje medosebne komunikacijske storitve na podlagi številke,
      b) zagotavljanje medosebne komunikacijske storitve, neodvisne od številke (OTT storitve),
      c) zagotavljanje storitev dostopa do interneta,
      č) zagotavljanje storitev komunikacij stroj – stroj (M2M),
      d) zagotavljanje storitev komunikacij v sili,

e) zagotavljanje ali uporaba storitev medomrežne povezave (npr. z drugimi operaterji, lastne ali najete povezave med vozlišči, tranzit),
f) zagotavljanje storitev domenskih imen (avtoritativni ali rekurzivni DNS strežniki),

11. oceno geografske razširjenosti območja, ki ga je prizadel varnostni incident (vsaj na nivoju prizadete statistične regije, po možnosti s pripadajočimi kraji in ulicami, kjer to primerno),
12. opredelitev primarnega vzroka varnostnega incidenta: naravna nesreča, človeška napaka na strani operaterja, zlonamerne aktivnosti, sistemska okvara ali napaka osebe izven neposrednega nadzora operaterja,
13. vrsto omrežja (fiksno, mobilno) in sredstva oziroma podatke, na katere je dogodek negativno vplival,
14. vpliv varnostnega incidenta na:
    a) storitve komunikacij v sili,
    b) upravljalce kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo kritično infrastrukturo, če mu je to poznano,
    c) ključne dele sistema varnosti države,
    č) IBS ali ODU, kot so določeni v skladu z zakonom, ki ureja informacijsko varnost, če so mu poznani,
    d) zagotavljanje storitev drugim operaterjem,
    e) druge države Evropske unije,
15. opis in analizo varnostnega incidenta, vključno z navedbo dejavnikov oziroma zaznanih aktivnosti, ki bi lahko ali so privedle do zlorabe javnih komunikacijskih omrežij oziroma javnih komunikacijskih storitev operaterja (angl. »IoC-Indicators of Compromise«) in druge tehnične podrobnosti o dogodku, če obstajajo,
16. izvedene ukrepe po varnostnem incidentu z namenom vzpostavitve normalnega stanja ter ukrepe, da se dogodek ne ponovi,
17. pomembnost varnostnega incidenta v skladu z lastno klasifikacijo operaterja,
18. navedbo, ali so bili zaradi posebne in resne grožnje varnostnega incidenta obveščeni uporabniki in na kakšen način,
19. navedbo, ali kdaj in na kakšen način so bili o varnostnem incidentu obveščeni drugi prizadeti operaterji,
20. navedbo, ali je bila zaradi varnostnega incidenta obveščena splošna javnost (navedba spletnega mesta ali drugi način obveščanja),
21. navedba, ali operater potrebuje oziroma je potreboval pomoč nacionalnega CSIRT,
22. dolgoročne pomembne ugotovitve v zvezi z varnostnim incidentom.

(2) Kjer je to zahtevano v skladu s tem splošnim aktom, operater obvesti agencijo in nacionalni CSIRT o oceni števila prizadetih oziroma potencialno prizadetih uporabnikov posamezne storitve ob upoštevanju razpoložljivih podatkov. Če to ni izvedljivo ali če bi bilo povezano z dolgotrajnimi postopki ali večjimi stroški, število prizadetih operater obvešča na podlagi ocene iz lastnih historičnih (statističnih) podatkov (npr. povprečno število uporabnikov, ki je uporabljalo izpadlo storitev v času dogodka v zadnjih treh mesecih).

5. člen
(obveščanje uporabnikov in drugih operaterjev)

(1) Operater v primeru posebne in resne grožnje varnostnega incidenta iz 3. člena tega splošnega akta nemudoma na svojih spletnih straneh na hitro in enostavno dostopnem ter

jasno razvidnem mestu obvešča uporabnike, ki bi jih taka grožnja lahko prizadela o morebitnih zaščitnih in popravnih ukrepih, ki jih lahko sprejmejo uporabniki. Operater uporabnike seznani tudi o sami grožnji, kadar oceni, da je to potrebno.

(2) Operater na svojih spletnih straneh na hitro dostopnem in jasno razvidnem mestu nemudoma obvesti uporabnike o večjih omejitvah in prekinitvah dostopa do svojih storitev zaradi okvar, napak in drugih varnostnih incidentov ter o tem vodi evidenco.

(3) Operater o varnostnem incidentu nemudoma obvesti tudi druge operaterje, če ta posredno ali neposredno vpliva na delovanje ali zagotavljanje njihovih storitev.

6. člen
(vrednotenje varnostnega incidenta)

Priglašeni varnostni incident se vrednoti glede na negativen vpliv, ki ga ima na varnost omrežij in storitev operaterjev, in sicer:

1. za majhen negativen vpliv na varnost omrežij in storitev operaterjev gre, če:
   a) nima negativnega vpliva na delovanje upravljavcev kritične infrastrukture ali delovanje na delovanje IBS ali ODU ali
   b) nima negativnega vpliva na delovanje ključnih delov sistema varnosti države ali
   c) nima negativnega vpliva na delovanje storitev komunikacij v sili, in sicer:
      - ne vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ ali
      - motnja ne traja več kot 15 minut in hkrati ni prizadetih več kot 500 uporabnikov pri operaterju ali
   č) pri zagotavljanju omrežij in storitev operaterja:
      - nima vpliva ali ima zanemarljiv vpliv na upravljanje omrežja operaterja, njegovih nadzornih ali varnostnih funkcij ali
      - nima vpliva na zaupnost komunikacij na podlagi prvega odstavka 214. člena ZEKom-2 ali
      - nima vpliva na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih podatkov o prometu ali
   d) ima negativni vpliv na razpoložljivost njegovih omrežij, na razpoložljivost ali kakovost njegovih storitev, pri čemer je:
      - varnostni incident trajal manj kot dve uri in je prizadel do 15% uporabnikov po posamezni storitvi operaterja ali
      - varnostni incident trajal več kot dve uri in manj kot štiri ure in je prizadel do 10% uporabnikov po posamezni storitvi operaterja ali
      - varnostni incident trajal več kot štiri ure in manj kot šest ur in je prizadel do 5% uporabnikov po posamezni storitvi operaterja ali
   e) obstaja možnost gospodarske škode ali pride do izpada dnevnega dohodka operaterja, ki ne presega 10% njegovega povprečnega dnevnega dohodka;

2. za velik negativen vpliv na varnost omrežij in storitev operaterjev gre, če:
   a) vpliva na vsaj en sektor kritične infrastrukture ali delovanje vsaj enega IBS ali ODU ali
   b) ima pomemben vpliv na varnost omrežja ali njegovih ključnih storitev upravljanja in nadzora ali

c) ima pomemben vpliv na zaupnost, kjer je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, podatkov o prometu, nepooblaščeni osebi ali procesu, pri čemer je prizadetih do 10 000 uporabnikov ali
č) ima pomemben vpliv na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih komunikacijskih podatkov, pri čemer je prizadetih do 10 000 uporabnikov ali
d) je ob dogodku nastala pomembna materialna škoda, ki znaša od 10% do 50% povprečnega dnevnega dohodka ali
e) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih več kot 10 000 uporabnikov teh storitev pri operaterju ali
f) ima pomemben negativni vpliv na razpoložljivost njegovih omrežij, ki služijo zagotavljanju neprekinjenega poslovanja, ali na razpoložljivost ali kakovost njegovih storitev, pri čemer je varnostni incident:
   - trajal več kot uro in manj kot dve in je prizadel med 10 in 15% uporabnikov operaterja po posamezni storitvi ali
   - trajal več kot dve uri in manj kot štiri ure in je prizadel med 5 in 10% uporabnikov operaterja po posamezni storitvi ali
   - trajal več kot štiri ure in manj kot šest ur in je prizadel med 2 in 5% uporabnikov operaterja po posamezni storitvi ali
   - trajal šest ali več ur in je prizadel med 1 in 2% uporabnikov operaterja po posamezni storitvi;

3. za zelo velik negativen vpliv na varnost omrežij in storitev operaterjev gre, če:
a) lahko delno ali v celoti onemogoči delovanje vsaj treh področij kritične infrastrukture, ali več izvajalcev IBS ali ODU ali bistvenih storitev ali
b) neposredno in znatno ogroža varnost omrežja ali njegovih ključnih storitev upravljanja in nadzora ali
c) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih 10 000 ali več uporabnikov teh storitev pri operaterju ali
č) vpliva na zaupnost, tako da je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, pri čemer je prizadetih 20 000 ali več uporabnikov ali
d) vpliva na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih podatkov, pri čemer je prizadetih 20 000 ali več več uporabnikov ali
e) operaterju povzroči materialno škodo, ki znaša več kot 50 % njegovega povprečnega dnevnega dohodka oziroma mu nastane tudi pomembna nematerialna škoda ali
f) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih več kot 20 000 uporabnikov teh storitev pri operaterju ali
g) vpliva na razpoložljivost njegovih omrežij, vključno z redundantnimi povezami in elementi, s katerimi zagotavlja neprekinjeno poslovanje, ali na razpoložljivost ali kakovost njegovih storitev pri čemer je varnostni incident:
   - trajal več kot eno in manj kot dve uri in je prizadel več kot 100 000 uporabnikov ali
   - trajal več kot dve uri in manj kot štiri ure in je prizadel več kot 200 000 uporabnikov ali
   - trajal več kot štiri ure in manj kot šest ur in je prizadel več kot 300 000 uporabnikov ali
   - trajal šest ali več ur in je prizadel več kot 400 000 uporabnikov.

7. člen

(najave omejitev ali prekinitev)

(1) Operater mora najaviti omejitve ali prekinitve javnih komunikacijskih storitev zaradi dograditve, posodobitve ali vzdrževanja javnih komunikacijskih omrežij vsaj 24 ur pred nameravano izvedbo, tako da navede točen datum in uro predvidenega posega in dejanski predviden oziroma potencialno možen vpliv del na izvajanje storitev, zadevno geografsko območje ter čas trajanja izvajanja del.

(2) Operater mora najave o omejitvah in prekinitvah iz prejšnjega odstavka objaviti v sredstvih javnega obveščanja oziroma vsaj na svojih spletnih straneh, kjer morajo biti dostopne najmanj dva meseca, in sicer na hitro in enostavno dostopnem mestu in na pregleden način.

(3) Operater mora v istem časovnem roku in z enako vsebino, kot je navedeno v prvem odstavku tega člena, seznaniti tudi agencijo preko portala za poročanje.

(4) Dela iz prvega odstavka tega člena morajo biti izvedena na način, da je čas omejitve ali prekinitve čim krajši in da prizadene čim manj uporabnikov.

PREHODNA IN KONČNA DOLOČBA

8. člen
(obveščanje agencije)

Do vzpostavitve portala agencije, ki je naveden v četrtem odstavku 2. člena in v tretjem odstavku 7. člena tega splošnega akta, operaterji za obveščanje agencije uporabljajo veljavna obrazca, objavljena na spletni strani agencije, ki ju izpolnjena pošljejo preko elektronske pošte na vnaprej dogovorjena elektronska naslova.

9. člen
(začetek veljavnosti)

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

Št. _____ mag. Tanja Muha

Ljubljana, dne _____ v.d. direktorja

EVA _____