PREDLOG!

Na podlagi drugega odstavka 118. člena in drugega odstavka 119. člena Zakona o elektronskih komunikacijah - ZEKom-2 (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) izdaja Agencija za komunikacijska omrežja in storitve Republike Slovenije

SPLOŠNI AKT
o poročanju in vrednotenju varnostnih incidentov

1. člen
(vsebina splošnega akta)

Ta splošni akt podrobneje opredeljuje vrste varnostnih incidentov, ki pomembno vplivajo na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev, metodologijo ter vsebino obvestila ter način poročanja varnostnih incidentov ter podrobneje ureja kriterije za njihovo vrednotenje.

2. člen
(pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu, pomenijo:

1. Kazalniki zlorabe so dejavniki oziroma zaznane aktivnosti, ki bi lahko ali so privedle do zlorabe javnih komunikacijskih omrežij oziroma javnih komunikacijskih storitev operaterja (angl. »IoC-Indicators of Compromise«).

2. Ključni deli nacionalnega varnostnega sistema imajo pomen, kot ga določa zakon, ki ureja informacijsko varnost.

3. Nacionalni CSIRT pomeni nacionalno skupino za obravnavanje incidentov v skladu z zakonom, ki ureja informacijsko varnost.

(2) Preostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen kot je določen v Zakonu o elektronskih komunikacijah – ZEKom-2 (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2).

3. člen
(priglasitev varnostnih incidentov)

(1) Operaterji morajo brez nepotrebnega odlašanja oziroma največ v eni uri po zaznavi varnostnega incidenta, ki pomembno vpliva na delovanje javnih komunikacijskih omrežij (v nadaljnjem besedilu omrežja) ali izvajanje javnih komunikacijskih storitev (v nadaljnjem besedilu: storitve), v skladu z merili iz prvega in drugega odstavka 4. člena tega splošnega akta, obvestiti Agencijo za komunikacijska omrežja in storitve Republike Slovenije (v nadaljnjem besedilu: agencija) in nacionalni CSIRT, če takšni varnostni incidenti vplivajo na:

1. razpoložljivost omrežij, storitev in podatkov (odpoved ali ohromljeno delovanje elementov omrežja, funkcij ali pripadajočih informacijskih sistemov, onemogočen ali ohromljen dostop do elementov omrežja, storitev, podatkov, baz ipd.);
2. upravljanje omrežja ter njegovih nadzornih in varnostnih funkcij;
3. zaupnost, kjer je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, komunikacijskih ali meta podatkov, neavtorizirani osebi, entiteti ali procesu (zlorabljena ali razkrita komunikacija, identiteta in lokacija uporabnika, vdori, ugrabljen promet uporabnikov ipd.);
4. celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih komunikacijskih in metapodatkov (nepooblaščena sprememba konfiguracije, neustrezno usmerjanje, lažno predstavljanje, zloraba klicnih številk ipd.);
5. nastanek znatne materialne ali nematerialne škode, ki jo je, ali bi jo lahko utrpel operater, ali pa njegov uporabnik (fizična ali pravna oseba).

(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 četrtega odstavka 4. člena tega splošnega akta, ki so mu znani, ostale podatke pa najkasneje v roku dveh ur od kar se z njimi seznani. Operater najkasneje v desetih dneh po odpravi varnostnega incidenta poroča agenciji in nacionalnemu CSIRT ostale zahtevane informacije iz tretjega odstavka 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) Poročanje pristojnim organom o varnostnih incidentih se izvaja na način, da se zagotovi varnost prenesenih podatkov, praviloma po elektronski poti, preko elektronske pošte na vnaprej dogovorjeni elektronski naslov oziroma preko enotnega portala za poročanje. Če dejanske in tehnipčne možnosti tega ne dopuščajo, se poročanje izvaja preko glavne pisarne agencije in nacionalnega CSIRT ali na drug primeren način. Če situacija zaradi varnostnega incidenta zahteva takojšnje ukrepanje, lahko operater le-tega izjemoma priglasi tudi na dežurni telefon nacionalnega CSIRT.

(5) Pri prijavi varnostnega incidenta iz prejšnjega odstavka, operater do vzpostavitve enotnega portala iz prejšnjega odstavka uporabi veljaven obrazec za priglasitev varnostnih incidentov, ki ga agencija objavi na svoji spletni strani.

4. člen
(kriteriji za poročanje in vsebina poročila)

(1) Pri presoji velikosti in pomembnosti varnostnega incidenta iz prvega odstavka 3. člena tega splošnega akta operater upošteva naslednje kriterije:

1. vpliv na razpoložljivost njegovih omrežij ali na razpoložljivost storitev, ki jih zagotavlja, je presegel enega od naslednjih referenčnih vrednosti, in sicer:
   a) vpliv je trajal manj kot uro in je prizadel več kot 20% vseh naročnikov po posamezni storitvi,

b) vpliv je trajal več kot eno uro in je prizadel več kot 15% vseh naročnikov po posamezni storitvi,
c) vpliv je trajal več kot dve uri in je prizadel več kot 10% vseh naročnikov po posamezni storitvi,
č) vpliv je trajal več kot štiri ure in je prizadel več kot 5% vseh naročnikov po posamezni storitvi,
d) vpliv je trajal več kot šest ur in je prizadel več kot 2% vseh naročnikov po posamezni storitvi,
e) vpliv je trajal več kot osem ur in je prizadel več kot 1% vseh naročnikov po posamezni storitvi;

2. vpliv na zaupnost komunikacij, in sicer na zaupnost podatkov o prometu iz 218. člena ZEKom-2 ali podatkov o naročnikih iz 215. člena ZEKom-2 ter na avtentičnost in celovitost omrežja:
a) nepooblaščeno so bili razkriti, spremenjeni ali odtujeni prometni, lokacijski podatki, dnevniški zapisi, gesla ali nastavitve ključnih delov omrežja, ne glede na čas trajanja ali število prizadetih,
b) nepooblaščeno je bila razkrita vsebina komunikacije (prestrezanje komunikacije) ne glede na število prizadetih,
c) izveden je bil ciljno usmerjen napad na omrežje ali storitve operaterja oziroma njegove uporabnike (DoS, DDoS, sabotaže, itd.), ne glede na čas trajanja ali število prizadetih, kjer se sproži ukrep preusmeritve oziroma čiščenja prometa bodisi lokalno ali z zunanjo podporo (angl. »blackholing«),
č) izveden je bil nepooblaščen vdor ali vpogled v bazo uporabnikov, podporne informacijske sisteme ali omrežne elemente operaterja,
d) dogodek ali več ponavljajočih dogodkov zaradi ranljivosti ali neustreznih nastavitev, 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).

(2) Ne glede na kriterije iz prvega odstavka tega člena operater, ki zagotavlja storitve končnim uporabnikom, nemudoma poroča pristojnim organom o varnostnih incidentih iz prvega odstavka 3. člena tega splošnega akta, ki so negativno vplivali na delovanje oziroma izvajanje:
1. storitev komunikacij v sili:
   - vpliv na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ ali
   - zaradi nedelovanja ali ohromljenega delovanja omrežja je prizadetih več kot 100 uporabnikov te storitve,
2. storitve upravljavcev kritične infrastrukture, ki so določeni v skladu s predpisi, ki urejajo kritično infrastrukturo,
3. storitve 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,
4. ključnih delov sistema varnosti države,
5. storitev, ki jih operater zagotavlja drugim operaterjem,
6. dostopovnega, agregacijskega vozlišča ali sisteme prenosa in je skupaj prizadeto več kot 1.000 uporabnikov.

(3) Ne glede na kriterije, navedene v prvem in drugem odstavku tega člena, lahko operater tudi prostovoljno poroča varnostne incidente, za katere meni, da vplivajo na varnost omrežij in storitev.

(4) Operater mora glede varnostnega incidenta v poročilu navesti tiste podatke iz spodnjega seznama, ki so relevantni za konkretni varnostni incident:

1. naziv operaterja;
2. identifikacijsko oznaka, 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 posamezni storitvi iz 10. točke tretjega odstavka 4. člena tega splošnega akta;
8. skupno ocenjeno število vseh prizadetih uporabnikov;
9. skupno ocenjeno število vseh prizadetih uporabnikov zaradi razlogov, navedenih v 2. točki prvega odstavka tega člena;
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),
    g) zagotavljanje storitev podatkovnega centra,
    h) zagotavljanje storitev računalništva v oblaku;
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,
    c) ključne dele sistema varnosti države,
    č) IBS ali ODU, kot so določeni v skladu z zakonom, ki ureja informacijsko varnost,
    d) zagotavljanje storitev drugim operaterjem,
    e) druge države Evropske unije.
15. opis in analizo varnostnega incidenta, vključno z navedbo kazalnikov zlorabe in druge tehnične podrobnosti o dogodku, če ti obstajajo;
16. izvedene ukrepe po 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.

(5) Kjer je to zahtevano, operater poroča oceno števila prizadetih oziroma potencialno prizadetih uporabnikov po posamezni storitvi ob upoštevanju realnih podatkov. Če to ni izvedljivo ali če bi bilo povezano z dolgotrajnimi postopki ali večjimi stroški, število prizadetih operater poroča 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 na svojih spletnih straneh na hitro in enostavno dostopnem ter jasno razvidnem mestu brez nepotrebnega odlašanja obvešča javnost in svoje uporabnike o vseh varnostnih incidentih, ki pomembno vplivajo na kakovost ali razpoložljivost njegovih storitev. Operater vodi evidenco vseh spletnih objav o nastalih incidentih. Vsako objavo iz te evidence lahko izbriše po preteku 12 mesecev.

(2) Operater v primeru posebne in resne grožnje varnostnega incidenta iz 4. člena tega splošnega akta nemudoma in brezplačno obvesti svoje uporabnike o morebitnih zaščitnih in popravnih ukrepih, če obstaja verjetnost, da bi jih taka grožnja lahko prizadela. Operater uporabnike seznani tudi o sami grožnji, kadar oceni, da je to potrebno.

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

(4) Ne glede na prvi odstavek tega člena se operater, ki oceni, da je varnostni incident posledica zlonamernih aktivnosti tretjih oseb, pred vsakim obvestilom javnosti o vsebini obvestila posvetuje z agencijo, ki upošteva šesti odstavek 118. člena ZEKom-2.

6. člen
(vrednotenje varnostnega incidenta)

(1) Varnostni incidenti se razvrščajo glede na negativni vpliv, ki ga imajo na varnost omrežij in storitev operaterja, na nemoteno delovanje operaterja in škodo, ki mu jo povzročijo ter glede na negativni vpliv na delovanje upravljalcev kritične infrastrukture, na delovanje IBS ali ODU, na delovanje storitev komunikacij v sili ali na delovanje ključnih delov sistema varnosti države.

(2) Varnostni incidenti se skladno s prejšnjim odstavkom razvrščajo v tri glavne skupine: lažji, težji in kritični varnostni incident:

1. Lažji varnostni incident je enkraten varnostni incident oziroma dogodek, ki ima majhen negativen vpliv na varnost omrežij in storitev operaterja ali pripadajoče informacijske sisteme ter nima večjega vpliva na nemoteno delovanje operaterja in mu ne povzroča večje škode, pri čemer varnostni incident:

a) nima negativnega vpliva na delovanje upravljavcev kritične infrastrukture ali delovanje na delovanje IBS ali ODU,

b) nima negativnega vpliva na delovanje ključnih delov sistema varnosti države,

c) nima negativnega vpliva na delovanje storitev komunikacij v sili:

- ne vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ,
- motnja ne traja več kot 15 minut in ni prizadetih več kot 100 uporabnikov pri operaterju hkrati,

č) pri zagotavljanju omrežij in storitev operaterja:

- nima vpliva ali ima zanemarljiv vpliv na upravljanje omrežja operaterja, njegovih nadzornih ali varnostnih funkcij,
- nima vpliva na zaupnost komunikacij na podlagi prvega odstavka 214. člena ZEKom-2,
- nima vpliva na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih podatkov o prometu,

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,
- varnostni incident trajal več kot dve uri in manj kot štiri ure in je prizadel do 10% uporabnikov po posamezni storitvi operaterja,
- varnostni incident trajal več kot štiri ure in manj kot šest ur in je prizadel do 5% uporabnikov po posamezni storitvi operaterja;

e) obstaja možnost gospodarske škode ali pride do izpada dnevnega dohodka operaterja, ki ne presega 10% njegovega povprečnega dnevnega dohodka.

2. Težji varnostni incident je enkraten varnostni incident oziroma zaporedje večjega števila varnostnih incidentov v kratkem obdobju, ki ima velik negativen vpliv na varnost omrežij in storitev operaterja, vključno s pripadajočimi informacijskimi sistemi. Takšen incident ima pomemben vpliv na nemoteno delovanje operaterja in mu povzroči večjo škodo, pri čemer:

a) vpliva na vsaj en sektor kritične infrastrukture, delovanje vsaj enega IBS ali ODU,

b) ima pomemben vpliv na upravljanje omrežja, njegovih nadzornih ali varnostnih funkcij,

c) ima pomemben vpliv na zaupnost, kjer je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, podatkov o prometu, nepooblaščeni osebi, entiteti ali procesu, pri čemer je prizadetih do 10 000 uporabnikov,

č) ima pomemben vpliv na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih komunikacijskih podatkov, pri čemer je prizadetih do 10 000 uporabnikov,

d) je ob dogodku nastala pomembna materialna škoda, ki znaša od 10% do 50 % povprečnega dnevnega dohodka operaterja oziroma mu nastane lahko tudi nematerialna škoda,

e) je novico o varnostnem incidentu objavilo več medijskih hiš ali spletnih portalov v državi,

f) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih več kot 10 000 uporabnikov teh storitev pri operaterju,

g) 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,
   - trajal več kot dve uri in manj kot štiri ure in je prizadel med 5 in 10% uporabnikov operaterja po posamezni storitvi,
   - trajal več kot štiri ure in manj kot šest ur in je prizadel med 2 in 5% uporabnikov operaterja po posamezni storitvi;
   - trajal šest ali več ur in je prizadel med 1 in 2% uporabnikov operaterja po posamezni storitvi.

3. Kritični varnostni incident je varnostni incident, ki ima zelo velik negativen vpliv na varnost omrežij in storitev operaterja, vključno s pripadajočimi informacijskimi sistemi. Ob tem takšen incident povzroči tudi oteženo delovanje države, še posebej ključnih delov sistema varnosti države, komunikacij v sili ter IBS in ODU, pri čemer varnostni incident:
   a) lahko delno onemogoči delovanje vsaj treh področij kritične infrastrukture ali bistvenih storitev, določenih v skladu s področno zakonodajo, ali enega v celoti,
   b) neposredno in znatno ogroža varnost omrežja ali njegovih ključnih storitev upravljanja,
   c) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih 10 000 ali več uporabnikov teh storitev pri operaterju,
   č) vpliva na zaupnost, tako da je bila ogrožena, razkrita ali zlorabljena zaupnost komunikacije, pri čemer je prizadetih 20 000 ali več uporabnikov,
   d) vpliva na celovitost in avtentičnost omrežja, shranjenih, obdelanih ali prenesenih podatkov, pri čemer je prizadetih 20 000 ali več več uporabnikov,
   e) operaterju povzroči materialno škodo, ki znaša 50 % ali več njegovega povprečnega dnevnega dohodka oziroma mu nastane tudi pomembna nematerialna škoda,
   f) vpliva na posredovanje oziroma usmerjanje komunikacij v sili na pristojni organ oziroma je prizadetih več kot 20 000 uporabnikov teh storitev pri operaterju,
   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,
      - trajal več kot dve uri in manj kot štiri ure in je prizadel več kot 200 000 uporabnikov,
      - trajal več kot štiri ure in manj kot šest ur in je prizadel več kot 300 000 uporabnikov;
      - trajal šest ali več ur in je prizadel več kot 400 000 uporabnikov.

KONČNA DOLOČBA

7. člen
(začetek veljavnosti)

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

PREDLOG!

Št. _____ mag. Tanja Muha

Ljubljana, dne _____ v.d. direktorja

EVA _____