810.

Na osnovu člana 11. stav 1. tačka 1, člana 14 i člana 169. stav 6 Zakona o elektronskim komunikacijama ("Sl. list CG" 40/13 i 56/13) Savjet Agencije za elektronske komunikacije i poštansku djelatnost na sjednici održanoj 23.07.2015. godine donio je:

PRAVILNIK

O NAČINU I ROKOVIMA ZA SPROVOĐENJE MJERA ZAŠTITE SIGURNOSTI I INTEGRITETA ELEKTRONSKIH KOMUNIKACIONIH MREŽA I USLUGA

("Službeni list Crne Gore", br. 041/15 od 28.07.2015)

Sadržaj Pravilnika

Član 1

Ovim pravilnikom propisuju se način i rokovi za sprovođenje mjera zaštite sigurnosti i integriteta elektronskih komunikacionih mreža i usluga, kao i način obavještavanja o povredi sigurnosti i integriteta elektronskih komunikacionih mreža i usluga.

Značenje izraza

Član 2

Pojedini pojmovi u smislu ovog pravilnika imaju sljedeće značenje:

1. Integritet mreže: osobina mreže da održi specificirane parametre u dijelu performansi i funkcionalnosti.
2. Kritična sredstva: elementi mreže i infrastruktura čiji bi prekid rada, vjerovatno imao direktan i značajan uticaj na sigurnost mreža i usluga ili direktan uticaj na procesuiranje ličnih podataka.
3. Prijetnja: događaj ili okolnost koja može dovesti do sigurnosnog incidenta.
4. Sigurnosne mjere: skup administrativnih, tehničkih i fizičkih zahtjeva za procese, rad i izmjene u elektronskoj komunikacionoj mreži, u svrhu osiguranja nesmetanog pristupa i upotrebe elektronskih komunikacionih mreža, kao i sigurnosti i integriteta podataka sačuvanih u elektronskoj komunikacionoj mreži.
5. Sigurnosni incident: jedan ili više neželjenih ili neočekivanih događaja koji mogu uticati na sigurnost i integritet mreža i usluga ili sigurnost, integritet i obradu ličnih podataka.

Mjere za zaštitu sigurnosti i integriteta mreža i usluga

Član 3

Mjere za obezbjeđenje integriteta javne elektronske komunikacione mreže, obezbjeđenja neprekidnog pružanja javnih elektronskih komunikacionih usluga, obezbjeđenja sigurnosti ličnih podataka, obezbjeđenja odgovora na sigurnosne incidente, ublažavanja uticaja sigurnosnih incidenata na rad svoje elektronske komunikacione mreže i sa njom povezanih mreža, ublažavanja uticaja prijetnji i sigurnosnih incidenata na korisnike elektronskih komunikacionih usluga, zaštite korisnika od zlonamjernih aktivnosti, elektronskih sabotaža, prevara trećih lica i zloupotreba bilo koje vrste (u daljem tekstu sigurnosne mjere), operator je dužan da primijeni u sljedećim oblastima:

- Upravljanje rizikom;
- Sigurnost ljudskih resursa;
- Sigurnost sistema i objekata;
- Upravljanje operacijama;
- Upravljanje incidentima;
- Upravljanje kontinuitetom poslovanja;
- Nadzor, revizija i testiranje.

U okviru svake oblasti iz stava 1 ovog člana operator je dužan da ispuni odgovarajuće sigurnosne ciljeve, preduzimanjem sigurnosnih mjera koje su navedene u Prilogu 1 ovog pravilnika.

Sigurnosne mjere iz Priloga 1 ovog pravilnika operator je dužan da sprovede u skladu sa odgovarajućim standardima, koji su navedeni u Prilogu 2 ovog pravilnika.

Operator koji pruža usluge telefonskih poziva i pristupa Internetu u fiksnoj elektronskoj komunikacionoj mreži i usluge u mobilnoj elektronskoj komunikacionoj mreži, za više od 10000 korisnika, dužan je da, izgradnjom georedundantne konfiguracije odgovarajućih elemenata mreže i sistema (Disaster Recovery Site) na teritoriji Crne Gore, obezbijedi neprekidnost pružanja telefonske usluge, usluge SMS-a i usluge pristupa Internetu.

Praćenje sprovođenja mjera za zaštitu sigurnosti i integriteta mreža i usluga

Član 4

Operator je dužan da, u cilju praćenja sprovođenja sigurnosnih mjera, Agenciji za elektronske komunikacije i poštansku djelatnost (u daljem tekstu Agencija) dostavi:

1) dokumenta kojima se definišu sigurnosne mjere iz člana 3, i postupci za njihovo sprovođenje, u roku 7 dana od njihovog usvajanja;
2) podatke o licu odgovornom za sprovođenje sigurnosnih mjera iz stava 1 člana 3 ovog pravilnika, u roku 7 dana od stupanja ovog pravilnika na snagu;
3) podatke o mjerama nadzora sigurnosti i integriteta mreža i usluga operatora od strane organa državne uprave nadležnog za prevenciju i zaštitu rizika bezbjednosti informacionih sistema odnosno organa uprave nadležnog za oblast računarskog kriminala, u roku 7 dana od vršenja nadzora;
4) izvještaje o interno sprovedenim kontrolama sigurnosti i integriteta elektronskih komunikacionih mreža i usluga i datim preporukama, u roku 7 dana od prijema izvještaja o sprovedenim kontrolama;
5) obavještenja i izvještaje o sigurnosnim incidentima.

Agencija, ili lica angažovana od strane Agencije, će vršiti kontrolu spovođenja sigurnosnih mjera iz člana 3 ovog pravilnika.

Obavještavanje o sigurnosnim incidentima

Član 5

Operator je dužan da, pisanim putem obavijesti Agenciju o sigurnosnom incidentu koji je doveo do prekida u pružanju telefonske usluge, usluge pristupa Internetu ili usluge distribucije audio-vizuelnih medijskih sadržaja u fiksnoj mreži za više od 1000 korisnika, a prekida u pružanju telefonske usluge i usluge SMS-a u mobilnoj mreži na teritoriji većoj od 46 km2 odnosno povrede sigurnosti ličnih podataka korisnika u fiksnim i mobilnim mrežama.

Operator je dužan da obavještenje o sigurnosnom incidentu iz stava 1 ovog člana dostavi Agenciji, u roku od 1 sata nakon pojave sigurnosnog incidenta, u skladu sa Prilogom 3 koji je sastavni dio ovog pravilnika.

Operator je dužan da, pisanim putem Agenciji dostavi izvještaj o sigurnosnom incidentu, koji je značajnije uticao na rad javnih elektronskih komunikacionih mreža ili pružanje elektronskih komunikacionih usluga, u skladu sa kriterijumima za izvještavanje iz Priloga 4 koji je sastavni dio ovog pravilnika.

Operator je dužan da izvještaj o sigurnosnom incidentu iz stava 3 ovog člana dostavi Agenciji, u roku od 3 radna dana od otklanjanja sigurnosnog incidenta, u skladu sa Prilogom 5, koji je sastavni dio ovog pravilnika.

Operator može obavijestiti Agenciju i o drugim važnim sigurnosnim incidentima koji se odnose na sigurnost i integritet javnih elektronskih komunikacionih mreža i usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavova 1. i 3. ovog člana.

Operator je dužan da odmah obavijesti druge operatore u slučaju da povreda sigurnosti i integriteta njegove mreže može značajnije uticati na rad sa njom povezanih mreža.

Prelazne i završne odredbe

Član 6

Operator je dužan da svoj rad uskladi sa ovim pravilnikom u roku od šest mjeseci, a sa odredbom člana 3 stav 4 ovog pravilnika u roku od 18 mjeseci od dana stupanja pravilnika na snagu.

Stupanje na snagu

Član 7

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

Broj: 0402-4628/1

Podgorica, 23.07.2015. godine

Predsjednik Savjeta,

dr Šaleta Đurović, s.r.

PRILOG 1: Sigurnosne mjere

OBLAST SIGURNOSTI	SIGURNOSNE MJERE
Upravljanje rizikom	Uspostavljanje i održavanje odgovarajućih procedura informacione sigurnosti koja se odnosi na sigurnost mreža, usluga i procesuiranja ličnih podataka; (**Information security policy**) Uspostavljanje i održavanje odgovarajućeg okvira za upravljanje rizikom, koji služi za identifikaciju i adresiranje rizika za mreže, usluge i procesuiranje ličnih podataka; (**Governance and risk management**) Uspostavljanje i održavanje odgovarajuće strukture sigurnosti sa ulogama i odgovornostima; (**Security roles and responsibilities**) Uspostavljanje i održavanje procedura sa zahtjevima koji se tiču sigurnosti za ugovore sa trećim stranama, kako bi se obezbijedilo da zavisnost od trećih strana ne utiče negativno na sigurnost mreža, usluga i procesuiranja ličnih podataka (**Security of third party assets**) .
Sigurnost ljudskih resursa	Obezbijediti odgovarajuću provjeru osoblja (zaposlenih, ugovarača i korisnika treće strane) kada je to potrebno za njihove dužnosti i odgovornosti (**Background checks**); Obezbijediti da osoblje ima dovoljno znanja o sigurnosti, a takođe, obezbijediti i redovnu obuku na temu sigurnosti (**Security knowledge and training**); Uspostaviti i održavati odgovarajuće procedure za upravljanje promjene osoblja ili za promjene njihovih uloga i odgovornosti (**Personnel changes**); Uspostaviti i održavati disciplinske procedure za zaposlene koji prekrše politike sigurnosti ili imati šire procedure koje pokrivaju sigurnosne prekršaje čije kršenje je izazvalo osoblje. (**Handling violations**);
Sigurnost sistema i objekata	Uspostaviti i održavati odgovarajuću fizičku sigirnost i sigurnost uslova u objektima (**Physical and environmental security of facilities**); Uspostaviti i održavati odgovarajuću sigurnost snadbijevanja (električnom energijom, naftnim derivatima-gorivom, klimatizacijom itd) za objekte (**Security of supplies**); Uspostaviti i održavati odgovarajuće (logičke) kontrole pristupa mreži i informacionim sistemima, kako bi se spriječio nedozvoljeni pristup, izmjena ili brisanje podataka na tim sistemima (**Access control to network and information systems**); Uspostaviti i održavati integritet mreže i informacionih sistema, radi zaštite od trojanaca, "code injections" i drugih malvera koji mogu promijeniti njihovu funkcionalnost (**Integrity of network and information systems**); Uspostaviti i održavati odgovarajuće procedure o povjerljivosti i integritetu sadržaja komunikacija i metapodataka o komunikacijama (**Confidentiality of communications**).
Upravljanje operacijama	Uspostaviti i održavati operativne procedure za funkcionisanje kritičnih mrežnih i informacionih sistema od strane osoblja (**Operational procedures**); Uspostaviti procedure za upravljanje promjenama za kritične mrežne i informacione sisteme, kako bi se umanjili incidenti koji su prouzrokovani promjenama (**Change management**); Uspostaviti i održavati procedure za upravljanje sredstvima i kontrolu konfiguracije u cilju upravljanja raspoloživošću kritičnih sredstava i konfiguracija kritičnih mrežnih i informacionih sistema (**Asset management**).
Upravljanje incidentima	Uspostaviti i održavati procedure za upravljanje sigurnosnim incidentima, kao i njihovo prosljeđivanje prema odgovarajućem osoblju (**Incident management procedures**); Uspostaviti i održavati odgovarajuće kapacitete za detekciju sigurnosnih incidentata (**Incident detection capability**); Uspostaviti i održavati odgovarajuće procedure za izvještavanje i objavljivanje o incidentima, uzimajući u obzir nacionalno zakonodavstvo za izvještavanje državnih institucija o incidentima (**Incident reporting and communication**);
Upravljanje kontinuitetom poslovanja	Uspostaviti i održavati planove za vanredne situacije i strategiju za obezbjeđenje kontinuiteta u priužanju mreža i usluga (**Service continuity strategy and contingency plans**);

	Uspostaviti i održavati odgovarajuće "disaster recovery" kapacitete za vraćanje u rad mreža i usluga u slučaju prirodnih i/ili velikih katastrofa (**Disaster recovery capabilities**).
Nadzor, revizija i testiranje	Uspostaviti i održavati sisteme i funkcije nadzora i logovanja kritičnih mrežnih i komunikacionih sistema (**Monitoring and logging policies**); Uspostaviti i održavati procedure za testiranje i uvježbavanje planova za vanredne situacije i obebjeđivanje backupa, kada je potrebno u sardanji sa trećim stranama (**Exercise contingency plans**); Uspostavljanje i održavanje procedura za testiranje mrežnih i informacionih sistema, posebno u slučajevima povezivanja sa novom mrežom ili informacionim sistemom (**Network and information systems testing**); Uspostavljanje i održavanje odgovarajućih procedura za obavljanje sigurnosnih procjena i testova mrežnih i informacionih sistema (**Security assessments**); Uspostaviti i održavati procedure za nadzor usklađenosti sa standardima i zakonskim obavezama (**Compliance monitoring**).

PRILOG 2: Standardi za sprovođenje sigurnosnih mjera

OBLAST SIGURNOSTI	REFERENTNI STANDARDI
Upravljanje rizikom	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27005 MEST ISO/IEC 27011
Sigurnost ljudskih resursa	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27011
Sigurnost sistema i objekata	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27011
Upravljanje operacijama	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27011
Upravljanje incidentima	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27011
Upravljanje kontinuitetom poslovanja	ISO/IEC 22301 MEST ISO/IEC 27011
Nadzor, revizija i testiranje	MEST ISO/IEC 27001 MEST ISO/IEC 27002 MEST ISO/IEC 27011

PRILOG 3:

Obavještenje o sigurnosnom incidentu

Operator	
Datum i vrijeme nastanka sigurnosnog incidenta	
Datum i vrijeme utvrđivanja sigurnosnog incidenta	
Način utvrđivanja sigurnosnog incidenta	
Vrsta usluge koju obuhvata sigurnosni incident	Fiksna telefonija: □ PSTN □ IMS □ VoIP □ DRUGO _____ Fiksni Internet: □ xDSL □ FTTx □ KDS □ DRUGO _____ Mobilna telefonija: □ GSM □ UMTS □ LTE □ DRUGO _____ Mobilni Internet: □ GPRS/EDGE □ UMTS □ LTE □ DRUGO _____ Zemaljska radiodifuzija: □ Zemaljska TV □ Zemaljski radio Distribucija AVM sadžaja: □ KDS □ IPTV □ Satelitski □ MMDS □ DRUGO Drugo _____
Opis sigurnosnog incidenta	
Broj obuhvaćenih korisnika	BROJ OBUHVAĆENIH KORISNIKA Fiksna telefonija: _____ Fiksni Internet: _____ Mobilna telefonija: _____ Mobilni Internet: _____ Zemaljska radiodifuzija: _____ Distribucija AVM sadžaja: _____ Drugo: _____
Uticaj na hitne službe	□ DA □ NE
Uticaj na interkonekciju (u zemlji i inostranstvu)	□ DA □ NE
Da li je došlo do povrede ličnih podataka korisnika?	□ DA □ NE U slučaju da je odgovor DA, opisati prirodu i sadržaj otkrivenih ličnih podataka korisnika
Aktivnosti koje su preduzete za rješavanje sigurnosnog incidenta	
Subjekti koji su obavješteni o sigurnosnom incidentu	
Procijenjeno vrijeme otklanjanja sigurnosnog incidenta	
Ostale važne informacije	
Ime i kontakt podaci lica koje je zaduženo za davanje informacija o incidentu (tel., e-mail)	
Datum i vrijeme dostave obavještenja	

PRILOG 4:

Kriterijumi za izvještavanje o sigurnosnom incidentu

Sigurnosni incident	Minimum krajnjihkorisnika/po-vršina teritorije obuhvaćenih sigurnosnim incidentom	Minimalno trajanje sigurnosnog incidenta
Nemogućnost mreže da prima, ili usmjerava pozive prema brojevima hitnih službi	1 korisnik	nezavisno od trajanja
Onemogućena usluga telefonskih poziva u fiksnoj mreži	1 000 korisnika	4 sata
Onemogućena usluga telefonskih poziva u fiksnoj mreži	5 000 korisnika	1 sat
Onemogućena usluga telefonskih poziva i SMS u mobilnoj mreži	46 km²	4 sata
Onemogućena usluga telefonskih poziva i SMS u mobilnoj mreži	138 km²	1 sat
Onemogućena usluga pristupa internetu	1 000 korisnika	4 sata
Onemogućena usluga pristupa internetu	5 000 korisnika	1 sat
Onemogućena usluga distribucije audio vizuelnih sadržaja	1 000 korisnika	4 sata
Onemogućena usluga distribucije audio vizuelnih sadržaja	5 000 korisnika	1 sat
Povreda ličnih podataka korisnika	1 korisnik	nezavisno od trajanja

PRILOG 5:
Izvještaj o sigurnosnom incidentu

Operator	
Datum i vrijeme nastanka sigurnosnog incidenta	
Datum i vrijeme utvrđivanja sigurnosnog incidenta	
Način utvrđivanja sigurnosnog incidenta	
Opis sigurnosnog incidenta	
Vrsta usluge koju obuhvata sigurnosni incident	Fiksna telefonija: □ PSTN □ IMS □ VoIP □ DRUGO _____ Fiksni Internet: □ xDSL □ FTTx □ KDS □ DRUGO _____ Mobilna telefonija: □ GSM □ UMTS □ LTE □ DRUGO _____ Mobilni Internet: □ GPRS/EDGE □ UMTS □ LTE □ DRUGO _____ Zemaljska radiodifuzija: □ Zemaljska TV □ Zemaljski radio Distribucija AVM sadžaja: □ KDS □ IPTV □ Satelitski □ MMDS □ DRUGO Drugo _____

Vrijeme trajanja sigurnosnog incidenta i broj obuhvaćenih korisnika	TRAJANJE BROJ OBUHVAĆENIH KORISNIKA Fiksna telefonija: _____ _____ Fiksni Internet: _____ _____ Mobilna telefonija: _____ _____ Mobilni Internet: _____ _____ Zemaljska radiodifuzija: _____ _____ Distribucija AVM sadžaja: _____ _____ Drugo: _____ _____
Uticaj na hitne službe	□ DA □ NE
Uticaj na interkonekciju (u zemlji i inostranstvu)	□ DA □ NE
Da li je došlo do povrede ličnih podataka korisnika?	□ DA □ NE U slučaju da je odgovor DA, opisati prirodu i sadržaj otkrivenih ličnih podataka korisnika
Osnovni uzrok	□ Sistemske greške □ Ljudske greške □ Zlonamjerne radnje □ Prirodni fenomeni □ Greška treće strane □ Uzrok nije utvrđen
Početni uzrok	□ Prekid kabla □ Krađa kabla □ Poplava □ Obilne snježne padavine □ Oluja □ Prekid napajanja □ Električni udar □ Fizički napad □ Kibernetički napad □ Loše održavanje □ Preopterećenje □ Iscrpljene zalihe goriva □ Proceduralna greška □ Greška hardvera □ Programska greška □ Ljudska greška □ Drugo _____ □ Uzrok nije utvrđen

Sistemi obuhvaćeni početnim uzrokom	□ Bazne stanice i upravljački sistemi (npr. BTS, NodeB, RNC) □ Mobilni komutacioni sistemi (npr. MSC, VLR, SGSN, GGSN) □ Korisnički i lokacioni registri (npr. HLR, HSS, AuC) □ Komutacioni sistemi (npr. lokalne centrale, svičevi, DSLAM) □ Sistemi prenosa (npr. SDH, WDM) □ Interkonekcija □ Međunarodna mreža □ Sistem napajanja (npr. transformatori, mreža napajanja) □ Rezervno napajanje (npr. dizel generatori, baterije) □ Sistemi hlađenja □ Ulični kabineti □ Centar za razmjenu poruka □ Adresni serveri (DHCP, DNS) □ Backbone mreža □ Lokalna mreža (npr. optička, bakarna) □ Drugo _____
Rješavanje sigurnosnog incidenta i opis preduzetih mjera (opis aktivnosti koje su preduzete nakon utvrđivanja incidenta za rješavanje incidenta)	
Mjere preduzete nakon otklanjanja sigurnosnog incidenta (opis preduzetih aktivnosti od strane operatora za smanjivanje vjerovatnoće ponavljanja incidenta ili uticaja incidenta)	Katalog
Dugoročne mjere	propisa
Ostale važne informacije	©2015
Ime i kontakt podaci lica koje je zaduženo za davanje informacija o incidentu (tel., e-mail)	
Datum dostave izvještaja	