NN br. 109/12, 33/13-ispravak, 126/13 i 67/16

PRAVILNIK
O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA

- neslužbeni pročišćeni tekst -

I. OPĆE ODREDBE

SADRŽAJ PRAVILNIKA

Članak 1.

Ovim Pravilnikom propisuju se način i rokovi u kojima operatori javnih komunikacijskih mreža moraju poduzimati sve odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža, u svrhu osiguravanja neprekinutog obavljanja usluga koje se pružaju putem tih mreža, te uređuje način izvješćivanja Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: Agencija) od strane operatora javnih komunikacijskih mreža i elektroničkih komunikacijskih usluga o povredi sigurnosti ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga.

Ovaj Pravilnik usklađen je s odredbom članka 13.a Direktive 2002/21/EC Europskog parlamenta i Vijeća o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge koja je izmijenjena i dopunjena Direktivom 2009/140/EC.

(NN br. 67/16 – izmjena riječi u prvom odlomku)

POJMOVI I ZNAČENJA

Članak 2.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *informacijski sustav*: komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike,
2. *integritet (cjelovitost) mreže*: skup tehničkih zahtjeva za procese, rad i izmjene u elektroničkoj komunikacijskoj mreži, u svrhu osiguravanja nesmetane uporabe međusobno povezanih elektroničkih komunikacijskih mreža, kao i pristupa tim mrežama te cjelovitosti podataka pohranjenih u elektroničkoj komunikacijskoj mreži,

3. *sigurnosni incident*: događaj koji može uzrokovati narušavanje sigurnosti i/ili gubitak integriteta mreže koji može utjecati na rad elektroničkih komunikacijskih mreža i/ili usluga.

(NN br. 67/16 – izmijenjen cijeli članak)

MJERE ZA ZAŠTITU SIGURNOSTI I INTEGRITETA MREŽA I USLUGA

Članak 3.

(1) Operatori su obvezni provesti odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svojih javnih komunikacijskih mreža i/ili usluga. Te mjere moraju osigurati neprekidno pružanje javnih komunikacijskih usluga putem mreža, kao i stupanj sigurnosti, odgovarajući na prijetnje i sprječavajući sigurnosne incidente ili ublažavajući njihov utjecaj na rad javne komunikacijske mreže, mrežno povezivanje kao i/ili na javne komunikacijske usluge korisnika. Poduzete mjere osobito se provode kako bi se spriječio i umanjio utjecaj sigurnosnih incidenata na korisnike usluga i međusobno povezane elektroničke komunikacijske mreže.

(2) U mjere pod stavkom 1. moraju biti uključene i procedure za upravljanje rizicima, sigurnosni zahtjevi za osoblje, sigurnost sustava i prostora, upravljanje postupcima, upravljanje sigurnosnim incidentima, upravljanje kontinuitetom poslovanja te nadzor i testiranje sigurnosti.

(3) Popis minimalnih mjera iz stavka 1. i 2. ovog članka i referentnih normi za njihovo provođenje prikazan je u Dodatku 1.

(4) Osim navedenih referentnih normi iz Dodatka 1. operatori mogu primijeniti i druge odgovarajuće norme u svrhu ostvarivanja mjera iz ovog članka.

(5) Operatori su obvezni elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja dostaviti Agenciji dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme.

(NN br. 67/16 – u stavku 1. dodana nova rečenica i brisani stavci 6. i 7.)

Članak 3.a.

(1) Operator mora najmanje jednom godišnje provesti reviziju informacijskog sustava kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti iz Dodatka 1 ovog Pravilnika.

(2) Nalaz revizije iz stavka 1. ovog članka, zajedno s planom uklanjanja uočenih nedostataka, potrebno je dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu.

(3) Postupak revizije treba provoditi tako da se u obzir uzme značaj pojedinih dijelova informacijskog sustava za funkcioniranje cijelog sustava te rezultate prethodnih

revizija. Reviziju mogu obavljati zaposlenici operatora koji nisu vezani za područje revizije i koji imaju odgovarajuće znanje i iskustvo ili vanjsko revizorsko tijelo.

(NN br. 67/16 – dodan novi članak 3.a.)

OBAVJEŠTAVANJE AGENCIJE O SIGURNOSNIM INCIDENTIMA

Članak 4.

(1) Operatori su obvezni obavijestiti Agenciju u slučaju neovlaštenog povezivanja s javnom komunikacijskom mrežom ili dijelom mreže te u slučaju kršenja sigurnosti ili integriteta javnih komunikacijskih usluga, koji su značajnije utjecali na obavljanje djelatnosti javnih komunikacijskih mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2.

(2) O sigurnosnim incidentima iz stavka 1. operatori moraju obavijestiti Agenciju bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. ovog Pravilnika:

1. u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2,
2. u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta,
3. u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta.

(3) Operatori moraju osigurati Agenciji podatke za kontakt sukladno Dodatku 3 u svrhu brze razmjene informacija o sigurnosnim incidentima između operatora i Agencije, te pružiti potrebne tehničke informacije Agenciji radi praćenja sigurnosti i integriteta javnih komunikacijskih mreža.

(4) Sve obavijesti o sigurnosnim incidentima moraju se dostavljati Agenciji upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način sukladno obrascu iz Dodatka 3.

(5) Agencija može zatražiti dopunu izvješća iz stavka 2. u svrhu praćenja određenog sigurnosnog incidenta te boljeg razumijevanja prirode nastalog sigurnosnog incidenta.

(6) Operator može obavijestiti Agenciju i o drugim, po mišljenju operatora, važnim sigurnosnim incidentima koji se odnose na sigurnost i integritet javnih komunikacijskih mreža i/ili usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavka 1.

(NN br. 67/16 – izmijenjen stavak 1. i 5.)

OBAVJEŠTAVANJE DRUGIH SUBJEKATA O SIGURNOSNIM INCIDENTIMA

Članak 5.

Operatori su obvezni bez odgode:

1. na odgovarajući način obavijestiti korisnike javnih komunikacijskih usluga o značajnijem prekidu pružanja javnih komunikacijskih mreža i/ili usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2. Ako su ugrožene osnovne usluge kao što su glasovna usluga, SMS usluga ili usluga pristupa internetu, operatori moraju bez odgode objaviti informacije o nastalom značajnom incidentu na službenoj stranici. Informacije o značajnom incidentu moraju sadržavati opis područja obuhvaćenog incidentom, koji može biti prikazan i u kartografskom obliku
2. obavijestiti druge operatore o mjerama koje mogu biti poduzete od strane korisnika javnih komunikacijskih usluga kako bi se uklonila prijetnja sigurnosnog incidenta, koje se odnose na terminalnu opremu korisnika, navodeći moguće troškove vezane uz provođenje takvih mjera.

ZAVRŠNE ODREDBE

Članak 6.

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga stupa na snagu šest (6) mjeseci od dana objave u „Narodnim novinama“.

PRIJELAZNE I ZAVRŠNE ODREDBE
PRAVILNIKA O IZMJENAMA PRAVILNIKA O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA
(NN br. 126/13)

Ovaj Pravilnik stupa na snagu osmog (8) dana od dana objave u „Narodnim novinama“.

PRIJELAZNE I ZAVRŠNE ODREDBE
PRAVILNIKA O IZMJENMA I DOPUNAMA PRAVILNIKA O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA
(NN br. 67/16)

Ovaj Pravilnik stupa na snagu 1. siječnja 2017.

DODATAK 1

MINIMALNE MJERE SIGURNOSTI

Minimalne mjere sigurnosti	Referentne norme
Procedure za upravljanje rizicima	ISO 27001:2013 ISO 27002:2015 ISO 27005:2011
Sigurnosni zahtjevi za osoblje	ISO 27001:2013 ISO 27002:2015
Sigurnost sustava i prostora	ISO 27001:2013 ISO 27002:2015
Upravljanje postupcima	ISO 27001:2013 ISO 27002:2015
Upravljanje sigurnosnim incidentima	ISO 27001:2013 ISO 27002:2015
Upravljanje kontinuitetom poslovanja	ISO 22301:2012
Nadzor i testiranje sigurnosti	ISO 27001:2013 ISO 27002:2015

DODATAK 2

KRITERIJI ZA IZVJEŠĆIVANJE

Sigurnosni incidenti	**Minimum krajnjih korisnika obuhvaćenih sigurnosnim incidentom**	**Minimalno trajanje sigurnosnog incidenta**
Mrežno onemogućavanje, primanja, ostvarivanja ili točnog usmjeravanja poziva prema hitnim službama	10 000 korisnika	neovisno o trajanju
Onemogućena govorna usluga u nepokretnoj mreži	14 000 korisnika	8 sati
Onemogućena govorna usluga u nepokretnoj mreži	28 000 korisnika	6 sati
Onemogućena govorna usluga u nepokretnoj mreži	71 000 korisnika	4 sata
Onemogućena govorna usluga u nepokretnoj mreži	142 000 korisnika	2 sata
Onemogućena govorna usluga u nepokretnoj mreži	214 000 korisnika	1 sat
Onemogućena govorna usluga u pokretnoj mreži	44 000 korisnika	8 sati
Onemogućena govorna usluga u pokretnoj mreži	88 000 korisnika	6 sati
Onemogućena govorna usluga u pokretnoj mreži	220 000 korisnika	4 sata
Onemogućena govorna usluga u	441 000 korisnika	2 sata

pokretnoj mreži		
Onemogućena govorna usluga u pokretnoj mreži	662 000 korisnika	1 sat
Onemogućena usluga pristupa internetu u nepokretnoj mreži	9 000 korisnika	8 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	19 000 korisnika	6 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	49 000 korisnika	4 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	98 000 korisnika	2 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	148 000 korisnika	1 sat
Onemogućena usluga pristupa internetu u pokretnoj mreži	32 000 korisnika	8 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	64 000 korisnika	6 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	160 000 korisnika	4 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	320 000 korisnika	2 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	481 000 korisnika	1 sat

DODATAK 3

PREDLOŽAK ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA

Potrebni podaci	**Popunjava operator**
Naziv operatora	
Datum podnošenja izvještaja	
Datum i vrijeme nastanka/otkrivanje sigurnosnog incidenta	
Mreža	☐ podzemni kabel ☐ zračni kabel ☐ podmorski kabel ☐ svjetlosni kabel ☐ radio mreža (zemaljska) ☐ satelitska mreža
Vrsta usluge koju obuhvaća sigurnosni incident	☐ Nepokretna telefonija: ☐ VoIP ☐ DSL ☐ OPTIKA ☐ KABELSKA ☐ DRUGO ☐ Nepokretni Internet: ☐ DSL ☐ OPTIKA ☐ KABELSKA ☐ DRUGO ☐ Sustav energetske mreže ☐ DRUGO ☐ Pokretna telefonija: ☐ GSM ☐ UMTS ☐ LTE ☐ DRUGO ☐ Pokretni Internet: ☐ GPRS/EDGE ☐ UMTS ☐ LTE ☐ DRUGO ☐ SMS ☐ MMS ☐ DRUGO

	☐ Satelitske komunikacijske usluge	☐ DRUGO
	☐ Međunarodni roaming	☐ DRUGO
	☐ Glasovne poruke	☐ DRUGO
	☐ Radio prijenos	☐ DRUGO
	☐ TV prijenos	☐ DRUGO
	☐ Kabelska televizijska mreža	☐ DRUGO

Vrijeme trajanja sigurnosnog incidenta i broj obuhvaćenih korisnika		VRIJEME TRAJANJA	BROJ OBUHVAĆENIH KORISNIKA
	Nepokretna telefonija		
	Nepokretni internet		
	Sustav energetske mreže		
	Pokretna telefonija		
	Pokretni internet		
	SMS		
	MMS		
	Satelitske usluge		
	Međunarodni roaming		
	Govorna usluga :		
	Radio prijenos		
	TV prijenos		
	IPTV		
	Drugo:		

Utjecaj na međupovezivanje	☐ DA ☐ NE
Utjecaj na hitne službe	☐ DA ☐ NE
Izvorni uzrok	☐ Sistemske greške ☐ Ljudska greška ☐ Zlonamjerne radnje ☐ Prirodni fenomen ☐ Greška treće strane
Početni uzrok	☐ Obilne snježne padaline ☐ Oluja ☐ Poplava ☐ Požar ☐ Zemljotres ☐ Prekid napajanja ☐ Električni udar ☐ Presjek kabela ☐ Krađa kabela ☐ Elektromagnetska interferencija ☐ DoS napad ☐ Krađa hardvera ☐ Pogrešna nadogradnja/zamjena hardvera ☐ Pogrešna nadogradnja/zamjena softvera ☐ Preopterećenje ☐ Iscrpljene zalihe goriva

	☐ Proceduralna greška ☐ Sigurnosna greška ☐ Ništa ☐ Drugo
Naknadni uzrok	☐ Obilne snježne padaline ☐ Oluja ☐ Poplava ☐ Požar ☐ Zemljotres ☐ Prekid napajanja ☐ Električni udar ☐ Presjek kabela ☐ Krađa kabela ☐ Elektromagnetska interferencija ☐ DoS napad ☐ Krađa hardvera ☐ Pogrešna nadogradnja/zamjena hardvera ☐ Pogrešna nadogradnja/zamjena softvera ☐ Preopterećenje ☐ Iscrpljene zalihe goriva ☐ Proceduralna greška ☐ Sigurnosna greška ☐ Ništa ☐ Drugo_____

Imovina obuhvaćena incidentom	☐ Pretplatnička oprema ☐ Bazne stanice i upravljački sklopovi (npr. BTS, NodeB, RNC) ☐ Mobilno prospajanje (npr. MSC, VLR, SGSN, GGSN) ☐ Korisnički i lokacijski registri (npr. HLR, HSS, AuC) ☐ Prospojnici (npr. lokalne centrale, usmjerivači, DSLAM) ☐ Prijenosni čvorovi (npr. SDH, WDM) ☐ Kabeli (npr. morski, zračni, podzemni) ☐ Međukonekcijske točke (npr. IXPs, IP transit) ☐ Sustav napajanja (npr. transformatori, mreža napajanja) ☐ Rezervno napajanje (npr. dizel generatori, baterije) ☐ Sustav hlađenja ☐ Ulični kabineti ☐ Centar za razmjenu poruka ☐ Prospojni centar (npr. MSC, VLR) ☐ Sustav naplate ☐ Adresni serveri (DHCP, DNS) ☐ Inteligentni mrežni uređaji ☐ Zgrade i fizički sigurnosni sustavi ☐ Operativni sustavi potpore ☐ Ništa ☐ Drugo_____
Opis sigurnosnog incidenta	
Rješavanje sigurnosnog incidenta i opis	

poduzetih mjera (opis aktivnosti koje su poduzete nakon otkrića incidenta za rješavanje incidenta)	
Mjere poduzete nakon otklanjanja sigurnosnog incidenta (opis poduzetih aktivnosti od strane operatora za smanjivanje vjerojatnosti ponavljanja incidenta ili utjecaja incidenta)	
Dugoročne mjere	
Kontakt podaci za praćenje procesa	
Ostale važne informacije	

(NN br. 67/16 – izmjena Dodataka 1, 2 i 3 te brisanje Dodataka 4 i 5.)