HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

NACRT PRIJEDLOGA PRAVILNIKA O IZMJENAMA I DOPUNAMA PRAVILNIKA O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA

Zagreb, 8. lipnja 2016.

I. OSNOVA ZA DONOŠENJE PRAVILNIKA

Člankom 12. stavkom 1. točkom 1. i člankom 99. stavkom 9. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13 i 71/14; dalje: ZEK) propisana je ovlast Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: HAKOM) za donošenje Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (dalje: Pravilnik).

II. OCJENA STANJA I OBRAZLOŽENJE IZMJENA

1. Ocjena stanja

Trenutno je vrijedeći Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 109/12, 33/13 i 126/13).

Ovim Pravilnikom se propisuju 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 HAKOM-a 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.

Odlukom o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za njezinu provedbu (NN 108/15), HAKOM je određen nositeljem, između ostalog, mjere *Nadzora tehničkih i ustrojstvenih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga i usmjeravanje operatora javnih komunikacijskih mreža i/ili usluga u cilju osiguranja visoke razine sigurnosti i dostupnosti javnih komunikacijskih mreža i usluga*.
U svrhu ostvarenja navedenog cilja potrebno je poduzeti mjere provođenja nadzora i usmjeravanja operatora javnih komunikacijskih mreža i/ili usluga kojim će se obuhvatiti različiti zahtjevi postavljeni prema operatorima i zahtjevi se odnose na kvalitetu i dostupnost mreža i usluga, zaštitu osobnih podataka, osiguravanje primjerene pažnje u provedbi sigurnosnih mjera na temelju odgovarajućih međunarodnih normi te provedbe zakonske obveze tajnog nadzora elektroničkih mreža i usluga.

S obzirom na gore navedeni cilj Strategije, HAKOM je ovim izmjenama Pravilnika ispunio navedenu zadaću na način da je predvidio za operatore obvezu revizije informacijskog sustava.

Također, HAKOM je unio i izmjene Pravilnika u dijelu koji se odnosi na usklađivanje s novim dokumentima Agencije Europske unije za mrežnu i informacijsku sigurnost (dalje: ENISA), te su jasnije propisane obveze vezano za način obavještavanja krajnjih korisnika o nastalom incidentu.

Sukladno članku 22. stavku 5. ZEK-a, o prijedlogu Pravilnika potrebno je provesti postupak javne rasprave sa zainteresiranom javnošću.

2. Obrazloženje izmjena

2.1. Obveza revizije informacijskog sustava - sukladno članku 99. stavku 10. točki 2. ZEK-a, u svrhu poduzimanja odgovarajućih mjera HAKOM može odrediti operatorima javnih komunikacijskih mreža i operatorima javno dostupnih elektroničkih komunikacijskih usluga, provedbu nadzora sigurnosti mreža i usluga. Navedeni nadzor mora obaviti osposobljeno neovisno interno ili vanjsko tijelo te podatke o obavljenom nadzoru učiniti dostupne HAKOM-u. Troškove nadzora sigurnosti snose operatori javnih komunikacijskih mreža i operatori javno dostupnih elektroničkih komunikacijskih usluga.

2.2. Izmjena Dodatka 2 i obrasca Dodatka 3 Pravilnika - usklađivanje s novim ENISA-inim dokumentima. Ažuriran je Dodatak 2 (kriteriji za izvješćivanje) sukladno ENISA-inom smjernicom (Technical guidline on Incident Reporting). Također, ENISA na svojim internetskim stranicama sadrži obrazac prijave incidenata i s tim obrascem je usklađen Dodatak 3 Pravilnika.

2.3. Brisanje prijave incidenata vezanih za Internet - za ovu vrstu incidenata je nadležan Nacionalni CERT koji je osnovan u skladu sa Zakonom o informacijskoj sigurnosti(NN br. 79/07). Stoga je navedena obveza brisana iz Pravilnika. U slučaju potrebe za postupanjem, HAKOM može na prijedlog CERT-a to riješiti kroz inspekcijski nadzor za što postoji pravna osnova u ZEK-u.

2.4. Pobliže određivanje načina obavještavanja krajnjih korisnika o nastalom incidentu - budući da do sada nije bio propisan način obavještavanja krajnjih korisnika o incidentu, izmjenom Pravilnika će se ovaj dio detaljnije definirati pa će operatori biti dužni, u slučaju da su ugrožene osnovne usluge kao što su glasovna usluga, SMS usluga ili usluga pristupa internetu, bez odgode objaviti informacije o nastalom značajnom incidentu s kartografskim prikazom područja ugroza na službenoj stranici.

III. TEKST NACRTA PRIJEDLOGA PRAVILNIKA

Prilaže se tekst Nacrta Pravilnika.

HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

Na temelju članka 12. stavka 1. točke 1. i članka 99. stavka 9. Zakona o elektroničkim komunikacijama (»Narodne novine« 73/08, 90/11, 133/12, 80/13 i 71/14), Vijeće Hrvatske regulatorne agencije za mrežne djelatnosti na sjednici održanoj _____ 2016. donosi

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

Članak 1.

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 109/12, 33/13 i 126/13; dalje: Pravilnik), mijenja se na način da se u članku 1. riječ *„Agencije“* zamjenjuje se riječima *„Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: Agencija)“*.

Članak 2.

Članak 2. mijenja se i glasi:

„*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.“*

Članak 3.

(1) U članku 3. na kraju stavka 1. dodaje se nova rečenica koja glasi:
„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 članku 3. stavak 6. i stavak 7. se brišu.

Članak 4

Iza članka 3. dodaje se novi članak 4. koji glasi:
„(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 obavljaju osobe koje nisu vezane za područje revizije te moraju imati odgovarajuće znanje i iskustvo.“

Članak 5.

(1) Dosadašnji članak 4. postaje članak 5.

(2) U dosadašnjem članku 4. stavak 1. mijenja se i glasi:
„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.“

(3) U dosadašnjem članku 4. stavak 5. mijenja se i glasi:
„Agencija može zatražiti dopunu izvješća iz stavka 2. u svrhu praćenja određenog sigurnosnog incidenta te boljeg razumijevanja prirode nastalog sigurnosnog incidenta.“

Članak 6.

(1) Dosadašnji članak 5., koji postaje članak 6., mijenja se na način da se iza riječi *„obvezni“* dodaju riječi *„bez odgode“* te se točka 1. mijenja i glasi:

„

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 javno dostupna telefonska usluga, SMS usluga, ili usluga pristupa internetu, operatori moraju bez odgode objaviti informacije o nastalom značajnom incidentu s kartografskim prikazom područja ugroza na službenoj stranici.“*

Članak 7.

Dodatak 1 mijenja se i glasi:

„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

Članak 8.

Dodatak 2 mijenja se i glasi:

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	14 200 korisnika	8 sati
Onemogućena govorna usluga u nepokretnoj mreži	28 500 korisnika	6 sati
Onemogućena govorna usluga u nepokretnoj mreži	71 300 korisnika	4 sata
Onemogućena govorna usluga u nepokretnoj mreži	142 600 korisnika	2 sata
Onemogućena govorna usluga u nepokretnoj mreži	214 000 korisnika	1 sat
Onemogućena govorna usluga u nepokretnoj mreži	44 100 korisnika	8 sati
Onemogućena govorna usluga u	88 300 korisnika	6 sati

pokretnoj mreži		
Onemogućena govorna usluga u pokretnoj mreži	22 000 korisnika	4 sata
Onemogućena govorna usluga u pokretnoj mreži	441 500 korisnika	2 sata
Onemogućena govorna usluga u pokretnoj mreži	662 300 korisnika	1 sat
Onemogućena govorna usluga u pokretnoj mreži	9 800 korisnika	8 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	19 700 korisnika	6 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	49 400 korisnika	4 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	98 800 korisnika	2 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	148 200 korisnika	1 sat
Onemogućena usluga pristupa internetu u nepokretnoj mreži	32 000 korisnika	8 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	64 100 korisnika	6 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	160 400 korisnika	4 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	320 900 korisnika	2 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	481 400 korisnika	1 sat

Članak 9.

Dodatak 3 mijenja se i glasi:

„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 interkonekciju	☐ 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	

Članak 10.

Dodatak 4 i 5 se brišu.

Članak 10.

Ovaj Pravilnik stupa na snagu 1. siječnja 2017.

KLASA: 011-02/16-02/05
URBROJ: 376-04-16-1
Zagreb,

PREDSJEDNIK VIJEĆA

dr. sc. Dražen Lučić