Temeljem članka 12. stavka 1. točke 1. i članka 99. Zakona o elektroničkim komunikacijama („Narodne novine“ br. 73/08, 90/11, 133/12 i 80/13) Vijeće Hrvatske agencije za poštu i elektroničke komunikacije donosi

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 Agencije 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.

POJMOVI I ZNAČENJA

Članak 2.

(1) U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *elektronički podaci*: podaci u obliku pogodnom za obradu putem informacijskog sustava,
2. *hrvatski internetski prostor*: informacijski sustavi koji su u adresnom prostoru hrvatskih operatora koji pružaju uslugu pristupa internetu,
3. *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,
4. *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,
5. *kompromitirani informacijski sustav*: poslužitelj nad kojim treće osobe imaju djelomičnu ili potpunu kontrolu koju najčešće ostvaruju iskorištavanjem ranjivosti sustava,
6. *krivotvorenje elektroničkih podataka*: ilegalno uništavanje, oštećivanje, brisanje, mijenjanje i/ili zamjena elektroničkih podataka s drugim elektroničkim podacima,
7. *nedozvoljeno korištenje informacijskog sustava*: ilegalno korištenje resursa informacijskog sustava i/ili neovlašteno povezivanje s informacijskim sustavom,
8. *preuzimanje kontrole („brute force“)*: pokušaj preuzimanja kontrole nad informacijskim sustavom pogađanjem identifikacijskih, odnosno autorizacijskih podataka korisnika koji su ovlašteni za pristup informacijskom sustavu,
9. *prijevara krivotvorenjem internetskih stranica („phishing“)*: oblik prijevare na internetu koja se najčešće izvodi na kompromitiranom informacijskom sustavu krivotvorenjem internetskih stranica raznih institucija, putem elektroničkih poruka i na druge načine,
10. *sigurnosni incident*: događaj koji može uzrokovati narušavanje sigurnosti i/ili gubitak integriteta mreže koji može utjecati na rad elektroničkih komunikacijskih mreža i/ili usluga,
11. *upravljačko-kontrolni centar mreže zaraženih računala („botnet“)*: informacijski sustav s kojeg je moguće upravljati *mrežom zaraženih računala* („botnet“),
12. *mreža zaraženih računala (»botnet«): veća skupina zaraženih korisničkih računala na kojima je aktivan zlonamjeran kod kojom upravlja upravljačko-kontrolni centar, a koja*

se najčešće koristi kao platforma za slanje neželjene pošte ili za napade uskraćivanjem usluge (»denial of service attacks«),

13. *zlonamjerni kod ili aplikacija*: programski kod s funkcijom nanošenja štete korisnicima i/ili operatorima javnih komunikacijskih usluga koji je instaliran i aktivan na terminalnoj opremi bez znanja korisnika,
14. *zona ukradenih podataka („drop zone")*: informacijski sustav s funkcijom prikupljanja ukradenih podataka.

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.

(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.

(6) Operatori su obvezni kontinuirano provoditi minimalne proaktivne mjere na internetu definirane u Dodatku 4 kako bi se smanjila mogućnost pojave incidenta te se pridržavati

reaktivnih mjera definiranih u Dodatku 5 koje su potrebne za rješenje pojedinog incidenta.

(7) Nadležno tijelo iz dodatka 5 ovog pravilnika može prijaviti otkriveni incident operatoru, ukoliko je isti u nadležnosti operatora. Operator je obvezan u tom slučaju postupati prema reaktivnim mjerama iz dodatka 5 ovog pravilnika.

(NN br. 33/13., 20.3.2013. izmjena stavaka 2. i 3. u članku 3.)

OBAVJEŠTAVANJE AGENCIJE O SIGURNOSNIM INCIDENTIMA

Članak 4.

(1) Operatori su obvezni obavijestiti Agenciju:

1. 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. u slučaju pojave sigurnosnih incidenata vezanih uz internet sukladno kriterijima za izvješćivanje iz Dodatka 2., uzimajući u obzir da se isti odnose na poslužiteljske sustave operatora koji pružaju usluge smještaja informacijskog sadržaja i servisa („hosting services“), vlastite javne usluge te na korisničke sustave za koje je operator zaprimio prijavu o sigurnosnom incidentu.

(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 su obvezni 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, kako bi se bolje razumjela priroda 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.

OBAVJEŠTAVANJE DRUGIH SUBJEKATA O SIGURNOSNIM INCIDENTIMA

Članak 5.

(1) Operatori su obvezni :

1. odmah obavijestiti korisnike javnih komunikacijskih usluga o značajnijem prekidu pružanja javnih komunikacijskih mreža i/ili usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2,

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 IZMJENI 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“.

DODATAK 1

MINIMALNE MJERE SIGURNOSTI

Minimalne mjere sigurnosti	Referentne norme	Opis
Procedure za upravljanje rizicima	ISO 27001/2 i ISO 27005	ISO 27005 opisuje procedure za upravljanje rizicima. ISO 27002 u poglavlju 5. opisuje politiku informacijske sigurnosti, procedure za upravljanje rizicima i kontrolu trećih strana (dobavljače usluga (hardvera i softvera)), kao što su sigurnosni zahtjevi i postupak nabave za nadogradnju ili kupovinu informacijskog sustava.
Sigurnosni zahtjevi za osoblje	ISO 27001/2	ISO 27001/2 u poglavlju 8. opisuje sigurnosne provjere osoblja, sigurnosne uloge i odgovornosti, sigurnosno znanje i osposobljavanje te promjene osoblja.
Sigurnost sustava i prostora	ISO 27001/2	ISO 27001 u poglavlju 9. opisuje fizičku sigurnost prostora, IT opreme i kontrolu okoline.

Upravljanje postupcima	ISO 27001/2	ISO 27001 u poglavlju 10. opisuje operativne procedure, uloge, klasifikaciju, kontrolu pristupa i kontrolu promjene.
Upravljanje sigurnosnim incidentima	ISO 27001/2	ISO 27002 u poglavlju 13. opisuje upravljanje sigurnosnim incidentima
Upravljanje kontinuitetom poslovanja	ISO 22301	ISO 22301 opisuje upravljanje kontinuitetom poslovanja
Nadzor i testiranje sigurnosti	ISO 27001/2	Nadzor je opisan u poglavlju 10. ISO 27001/2, dok su testiranje sigurnosti, usklađenost nadzora i obavještavanje opisani u poglavlju 15. ISO 27001/2.

DODATAK 2

SIGURNOSNI INCIDENTI VEZANI UZ INTERNET

Sigurnosni incidenti	Opis sigurnosnih incidenata
Upravljačko-kontrolni centar mreže zaraženih računala („botnet“)	Uspostavljanje upravljačko-kontrolnog centara mreže zaraženih računala („botnet“) na informacijskom sustavu. Informacijski sustav može biti kompromitiran ili nekompromitiran.
Kompromitirani informacijski sustav	Informacijski sustav s funkcijom prikupljanja ukradenih podataka, odnosno zona ukradenih podataka („drop zone“). Informacijski sustav može biti kompromitiran ili nekompromitiran
	Kompromitirani informacijski sustav s uslugom distribucije zlonamjernog koda putem internetskih stranica ili na druge načine
	Kompromitirani informacijski sustav s krivotvorenim stranicama za krađu osobnih ili drugih podataka, odnosno prijevara krivotvorenjem internetskih stranica („phishing“)

Nedozvoljene mrežne aktivnosti	Neovlašteni pokušaji korištenja usluga na informacijskim sustavima pogađanjem identifikacijskih korisničkih podataka preuzimanjem kontrole („brute force“)
Napadi uskraćivanjem usluge („denial of service attacks“)	Napadi uskraćivanjem usluge na javne informacijske sustave, pojedine usluge ili mrežnu infrastrukturu operatora
Korisnička računala u sustavu mreže zaraženih računala („botnet“)	Sudjelovanje zaraženog korisničkog računala u hrvatskom adresnom prostoru operatora koji pruža uslugu pristupa internetu u ulozi člana mreže zaraženih računala („botnet“)
Ostali sigurnosni incidenti	Neovlaštene promjene stranica i ostali sigurnosni incidenti vezani uz kompromitirane informacijske sustave

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 (npr. 112, 193)	1 korisnik	neovisno o trajanju
Onemogućena govorna usluga u nepokretnoj mreži	80 000 korisnika	4 sata
Onemogućena govorna usluga u nepokretnoj mreži	240 000 korisnika	1 sat
Onemogućena govorna usluga u pokretnoj mreži	255 000 korisnika	4 sata
Onemogućena govorna usluga u	765 000 korisnika	1 sat

pokretnoj mreži		
Onemogućena usluga pristupa internetu	60 000 korisnika	4 sata
Onemogućena usluga pristupa internetu	180 000 korisnika	1 sat

(NN br. 126/13., 16.10.2013. izmjena u Dodatku 2. brišu se sigurnosni incidenti »Onemogućena SMS usluga u pokretnoj mreži« i »Onemogućena usluga elektroničke pošte«)

KRITERIJI ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA VEZANIH UZ INTERNET

Sigurnosni incidenti	**Minimalno trajanje sigurnosnog incidenta**
Upravljačko-kontrolni centar mreže zaraženih računala („botnet“)	Potrebno je prijaviti svaki upravljačko-kontrolni centar neovisno o trajanju
Kompromitirani informacijski sustav	Zlonamjerna funkcionalnost je aktivna duže od 12 sati
Prijevara krivotvorenjem internetskih stranica („phishing“)	Zlonamjerna aktivnost je prisutna duže od 8 sati
Nedozvoljene mrežne aktivnosti	Potrebno je prijaviti svaki slučaj uspješnog kompromitiranja informacijskog sustava neovisno o trajanju
Napadi uskraćivanjem usluge („denial of service attacks“)	Potrebno je prijaviti napade na terminalnu opremu korisnika koji traju duže od 30 minuta, a neovisno o trajanju napade na infrastrukturu operatora koji pruža uslugu pristupa internetu
Korisnička računala u sustavu mreže zaraženih računala („botnet“)	Potrebno je jednom mjesečno prijaviti prosječan broj zaraženih računala za prethodni mjesec
Ostali sigurnosni incidenti	Prijava po procjeni operatora davatelja usluga

DODATAK 3

PREDLOŽAK ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA

Potrebni podaci	**Popunjava operator**
Naziv operatora	
Datum podnošenja izvještaja	
Datum i vrijeme nastanka/otkrivanje sigurnosnog incidenta	
Vrsta usluge koju obuhvaća sigurnosni incident	☐ Nepokretna telefonija: ☐ PSTN ☐ DSL ☐ OPTIKA ☐ KABELSKA ☐ DRUGO___ ☐ Nepokretni Internet: ☐ DSL ☐ OPTIKA ☐ KABELSKA ☐ DRUGO _____ ☐ Pokretna telefonija: ☐ GSM ☐ UMTS ☐ LTE ☐ DRUGO _____ ☐ Pokretni Internet: ☐ GPRS/EDGE ☐ UMTS ☐ LTE ☐ DRUGO _____ ☐ Drugo _____
Vrijeme trajanja sigurnosnog incidenta i broj obuhvaćenih korisnika	TRAJANJE / BROJ OBUHVAĆENIH KORISNIKA Nepokretna telefonija: _____ _____ Nepokretni internet:_____ _____ Pokretna telefonija:_____ _____ Pokretni internet:_____ _____ Drugo:_____ _____
Utjecaj na hitne službe	☐ DA ☐ NE
Utjecaj na međupovezivanje (u tuzemstvu i	☐ DA ☐ NE

inozemstvu)	
Izvorni uzrok	☐ Sistemske greške ☐ Ljudska greška ☐ Zlonamjerne radnje ☐ Prirodni fenomen ☐ Greška treće strane
Početni uzrok	☐ Presjek kabela ☐ Krađa kabela ☐ Poplava ☐ Obilne snježne padaline ☐ Oluja ☐ Prekid napajanja ☐ Električni udar ☐ Fizički napad ☐ Kibernetički napad ☐ Loša promjena ☐ Loše održavanje ☐ Preopterećenje ☐ Iscrpljene zalihe goriva ☐ Proceduralna greška ☐ Greška hardvera ☐ Programska greška ☐ Ljudska greška ☐ Ništa ☐ Bez informacija ☐ Drugo_____

Posljedični uzrok	☐ Presjek kabela ☐ Krađa kabela ☐ Poplava ☐ Obilne snježne padaline ☐ Oluja ☐ Prekid napajanja ☐ Električni udar ☐ Fizički napad ☐ Kibernetički napad ☐ Loša promjena ☐ Loše održavanje ☐ Preopterećenje ☐ Iscrpljene zalihe goriva ☐ Proceduralna greška ☐ Greška hardvera ☐ Programska greška ☐ Ljudska greška ☐ Ništa ☐ Bez informacija ☐ Drugo _____
Imovina obuhvaćena početnim uzrokom	☐ 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) ☐ Jezgrena mreža (npr. svjetlovodna jezgra, agregacijska mreža)

	☐ Međukonekcije (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) ☐ Internacionalna temeljna mreža (npr. podvodni kabeli, internetske točke razmjene, internacionalne međukonekcije) ☐ Adresni serveri (DHCP, DNS) ☐ Mrežna okosnica operatora (backbone) (npr. svjetlovodna, bakrena) ☐ Područna mreža (npr. svjetlovodna) ☐ Bez informacija ☐ 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. 126/13., 16.10.2013. izmijenjen Dodatak 3.)

DODATAK 4

MINIMALNE PROAKTIVNE MJERE KOJE JE POTREBNO PROVODITI PRIJE POJAVE SIGURNOSNIH INCIDENATA NA INTERNETU

Sigurnosni incidenti	Proaktivna mjera
Upravljačko-kontrolni centar mreže zaraženih računala („botnet“)	1. Redovno informiranje krajnjih korisnika na vidnom mjestu o načinima zaraze i ulozi upravljačko-kontrolnog centra mreže zaraženih računala („botnet“)
Kompromitirani informacijski sustav	1. Kontinuirano ažurirati operativni sustav i instalirane aplikacije koje su u vlasništvu operatora i za koje korisnik nema administratorske ovlasti 2. Onemogućiti sve mrežne usluge koje nisu neophodne za rad informacijskog sustava

	3. Operator mora redovito informirati korisnika, koji je vlasnik virtualnog privatnog sustava, o potrebi provođenja mjera navedenih u točkama 1 i 2 na informacijskim sustavima na kojima korisnik ima administratorske ovlasti 4. Opcionalno implementirati tehničke mjere za zaštitu web sjedišta od mogućih kompromitacija WAF (Web Application Firewall) i/ili IPS (Intrusion Prevention System) za zaštitu svih usluga
Nedozvoljene mrežne aktivnosti	1. Implementacija mjera zaštite od automatiziranog napada pogađanjem lozinki
Napadi uskraćivanjem usluge („denial of service attacks“)	1. Implementacija tehničkih mjera za mjerenje i analizu strukture i anomalija prometa u mreži 2. Razrađen plan o načinima filtriranja zlođudnog prometa pri napadima uskraćivanjem usluge
Korisnička računala u sustavu mreže zaraženih računala („botnet“)	1. Redovno informiranje krajnjih korisnika na vidnom mjestu o načinima zaraze, ulozi mreže zaraženih računala („botnet“) i načinima zaštite od zaraze zlođudnim kodom

DODATAK 5

MINIMALNE REAKTIVNE MJERE KOJE JE POTREBNO PROVODITI NAKON POJAVE SIGURNOSNIH INCIDENATA NA INTERNETU

Tip sigurnosnog incidenta	Reaktivna mjera
Upravljačko-kontrolni centar mreže zaraženih računala (»botnet«)	1. U suradnji sa nadležnim tijelom sukladno važećem Zakonu o informacijskoj sigurnosti analizirati i ukloniti kontrolno-upravljački centar

Kompromitirani informacijski sustav	1. Ukloniti zlonamjernu aplikaciju i po potrebi u skladu sa Zakonom o informacijskoj sigurnosti u suradnji s nadležnim tijelom analizirati kompromitirani sustav i zlonamjernu aplikaciju.
Nedozvoljene mrežne aktivnosti	1. U slučaju uspješnog napada, odnosno pogođenih korisničkih identifikacijskih podataka, postupak je isti kao kod grupe incidenata »Kompromitirani informacijski sustav«
Napadi uskraćivanjem usluge (»denial of service attacks«)	1. Analizirati strukturu malicioznog prometa 2. Ovisno o rezultatu analize strukture malicioznog prometa, poduzeti moguće mjere za filtriranje prometa 3. Po potrebi zatražiti od nadležnog tijela sukladno važećem Zakonu o informacijskoj sigurnosti koordinaciju sa nadležnim tijelima u drugim državama
Korisnička računala u sustavu mreže zaraženih računala (»botnet«)	1. Informirati korisnike o postojanju i tipu zaraze na njihovom računalu