PRIJEDLOG

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

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

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 ili se nalaze u .hr vršnoj domeni,
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 izvodi na kompromitiranom informacijskom sustavu krivotvorenjem internetskih stranica neke banke, novčarske institucije i dr.,
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 zaraženog skupa („botnet")*: informacijski sustav sa kojeg je moguće upravljati sa skupinom korisničkih računala u sustavu zaraženog skupa („botnet"),

12. *zaraženi skup („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 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 moraju 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 sprečavajući 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 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 koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme za prethodnu godinu.

OBAVJEŠTAVANJE AGENCIJE O SIGURNOSNIM INCIDENTIMA

Članak 4.

(1) Operatori moraju obavijestiti Agenciju:

1. u slučaju neovlaštenog povezivanja s javnom komunikacijskom mrežom ili dijelom mreže, 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,

3. u slučaju sigurnosnih incidenata, koji izazivaju ili mogu izazvati opasnost za sigurnost i/ili integritet drugih operatora javnih komunikacijskih mreža i/ili usluga ili informacijskih sustava,

4. o svim sigurnosnim incidentima prijavljenim drugim nadležnim javnopravnim tijelima,

    a. o svakom sigurnosnom incidentu koji utječe na ostvarivanje, odnosno primanje ili točno usmjeravanje žurnih poziva,

    b. o svakom sigurnosnom incidentu o kojem operator ima saznanja, a koji je povezan s mogućim gubitkom života.

(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 kontakt podatke 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 dostaviti Agenciji 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 moraju :

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 5.

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.

KLASA: 011-02/12-02/09
UBRBOJ: 376-12/ŽKB-12-01 (MW)
Zagreb, 13. lipnja 2012. godine

PREDSJEDNIK VIJEĆA

Miljenko Krvišek, dipl. ing. el.

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 25999-1/2	BS 25999 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 zaraženog skupa („botnet“)	Uspostavljanje upravljačko-kontrolnog centara zaraženog skupa („botnet“) na informacijskom sustavu. Informacijski sustav može biti kompromitiran ili nekompromitiran.
Kompromitirani informacijski sustavi	Informacijski sustav sa funkcijom prikupljanja ukradenih podataka, odnosno zona ukradenih podataka („drop zone“). Informacijski sustav može biti kompromitiran ili nekompromitiran Kompromitirani informacijski sustav sa uslugom distribucije zlonamjernog koda putem internetskih stranica ili na druge načine Kompromitirani informacijski sustav sa krivotvorenim stranicama za krađu osobnih ili drugih podataka, odnosno prijevara krivotvorenjem internetskih stranica („phishing“)
Prijevara krivotvorenjem internetskih stranica („phishing“)	Pokušaji prijevare građana RH koji koriste kompromitirane informacijske sustave izvan hrvatskog internetskog prostora
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 zaraženog skupa („botnet“)	Sudjelovanje zaraženog korisničkog računala u hrvatskom adresnom prostoru operatora koji pruža uslugu pristupa internetu u ulozi člana zaraženog skupa („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 pristupa žurnim 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 pokretnoj mreži	765 000 korisnika	1 sat
Onemogućena SMS usluga u pokretnoj mreži	255 000 korisnika	4 sata
Onemogućena SMS usluga u pokretnoj mreži	765 000 korisnika	1 sat
Onemogućena usluga elektroničke pošte	60 000 korisnika	4 sata
Onemogućena usluga elektroničke pošte	180 000 korisnika	1 sat
Onemogućena usluga pristupa internetu	60 000 korisnika	4 sata
Onemogućena usluga pristupa internetu	180 000 korisnika	1 sat

KRITERIJI ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA VEZANIH UZ INTERNET

Sigurnosni incidenti	**Kriterij za prijavu**	**Minimalno trajanje sigurnosnog incidenta**
Upravljačko-kontrolni centar zaraženog skupa („botnet“)	Potrebno je odmah prijaviti svaki upravljačko-kontrolni centar	neovisno o trajanju
Kompromitirani informacijski sustav	Zlonamjerna funkcionalnost je aktivna duže od 12 sati	12 sati
Prijevara krivotvorenjem internetskih stranica („phishing“)	Zlonamjerna aktivnost je prisutna duže od 8 sati	8 sati
Nedozvoljene mrežne aktivnosti	Potrebno je odmah 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 odmah napade na infrastrukturu operatora koji pruža uslugu pristupa internetu.	30 minuta/neovisno o trajanju
Korisnička računala u sustavu zaraženog skupa („botnet“)	Potrebno je jednom mjesečno prijaviti prosječan broj zaraženih računala za prethodni mjesec	Periodički, jednom mjesečno
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 sigurnosnog incidenta	
Uzrok sigurnosnog incidenta	
Kratki opis sigurnosnog incidenta	
Utjecaj: 1. Vrste mreža i elemenata koji su obuhvaćeni 2. Obuhvaćene usluge (uključujući žurne službe) 3. Broj/razmjer obuhvaćenih korisnika 4. Vrijeme oporavka (ako je poznato) 5. Obuhvaćeno geografsko područje (ako je poznato)	
Rješavanje sigurnosnog incidenta	
Opis poduzetih mjera	
Dugoročne mjere	

Obuhvaćeno međupovezivanje	
Kontakt podaci za praćenje procesa	
Ostale važne informacije	

OPIS PODATAKA POTREBNIH ZA IZVJEŠTAJ

Potrebni podaci	Opis podataka
Naziv operatora	Potrebno je navesti puni naziv operatora
Datum podnošenja izvještaja	Potrebno je navesti datum podnošenja izvještaja Agenciji
Datum i vrijeme nastanka/otkrivanje sigurnosnog incidenta	Potrebno je navesti datum i vrijeme nastanka sigurnosnog incidenta ili, ako ti podaci nisu dostupni, datum i vrijeme otkrivanja sigurnosnog incidenta
Vrsta sigurnosnog incidenta	Potrebno je specificirati vrstu sigurnosnog incidenta sukladno Dodatku 2
Uzrok sigurnosnog incidenta	Potrebno je specificirati i opisati uzrok sigurnosnog incidenta. Uzroci mogu biti: 1. Prirodna nepogoda, 2. Ljudska greška, 3. Kvar ili greška na hardveru ili softveru, 4. Greška treće strane ili vanjske procedure (npr. stroj za iskop je presjekao kabel, greške u procesu nabave) ili 5. Zlonamjeran napad (logički ili fizički)
Kratki opis sigurnosnog incidenta	Ukratko opisati sigurnosni incident. Primjer opisa sigurnosnog incidenta vezanog uz internet: informacijski sustavi u sigurnosnom incidentu, funkcija zlonamjernog koda na njima, cilj zlonamjerne aplikacije ili

	opisati karakteristike napada uskraćivanjem usluge („denial of service attacks“), vrstu napada (napad na uslugu, aplikaciju, operativni sustav), količina zauzetog prijenosnog opsega, vrsta paketa kojima je izvršen napad, trajanje napada i dr.
Utjecaj: 1. Vrste mreža i elemenata koji su obuhvaćeni 2. Obuhvaćene usluge (uključujući žurne službe) 3. Broj/razmjer obuhvaćenih korisnika 4. Vrijeme oporavka (ako je poznato) 5. Obuhvaćeno geografsko područje (ako je poznato)	1. npr. nepokretna, pokretna, pristupna mreža, bazna stanica i dr. 2. npr. govorna, SMS usluga, usluga elektroničke pošte, usluga pristupa internetu (potrebno je navesti i da li prekid ima utjecaj na pristup prema određenim žurnim službama) 3. ukoliko je prekid na centrali s poznatim brojem korisnika potrebno je navesti broj, ako nije moguće vidjeti točan broj potrebno je navesti: ili razmjere obuhvaćenosti (npr. tisuća ili milijun obuhvaćenih korisnika) ili udio krajnjih korisnika vjerojatno obuhvaćenih (postotak), ili koristeći mrežno mjerilo (npr. broj baznih stanica bez usluge ili nekih drugih mrežnih elemenata) 4. potrebno je navesti informacije o vremenu trajanja sigurnosnog incidenta, odnosno o vremenu u kojem korisniku nije bila omogućena usluga ili je bio izložen zlonamjernom kodu, aplikaciji ili prijevari krivotvorenjem internetskih stranica („phishing“). 5. osigurati sve raspoložive informacije o geografskom području koje je obuhvaćeno sigurnosnim incidentom

Rješavanje sigurnosnog incidenta	Opis svih mjera i radnji poduzetih nakon otkrivanja sigurnosnog incidenta u svrhu njegovog uklanjanja ili smanjenja u slučaju korisničkih računala u zaraženom skupu („botnet“)
Opis poduzetih mjera	Opis poduzetih mjera koje su se poduzele nakon uklanjanja ili smanjenja sigurnosnog incidenta kako bi se smanjio rizik vezan uz ponavljanje istog ili sličnog incidenta.
Dugoročne mjere	Opis poduzetih dugoročnih mjera, radnji ili procedura koje su poduzete nakon rješavanja ili smanjenja (u slučaju korisničkih računala u sastavu zaraženog skupa („botnet“)) sigurnosnog incidenta kako bi se poboljšala sigurnost
Obuhvaćena međupovezivanja	Potrebno je navesti i opisati ako je sigurnosnim incidentom obuhvaćeno nacionalno i/ili međunarodno međupovezivanje. Ako usluga koja je obuhvaćena sigurnosnim incidentom može uzrokovati oštećenja/promijene imovine ili usluga drugog operatora, onda taj sigurnosni incident obuhvaća i međupovezivanje.
Kontakt podaci za praćenje procesa	Ime, prezime, adresa elektroničke pošte i izravna linija odgovorne osobe kojoj se Agencija može obratiti vezano uz praćenje upita
Ostale važne informacije	Ukoliko postoje, potrebno je navesti dodatne važne informacije

Obrazloženje odredbi pravilnika

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga je u cijelosti novi podzakonski akt kojeg HAKOM donosi temeljem članka 99. stavak 9. Zakona o elektroničkim komunikacijama („Narodne novine“ br. 73/08 i 90/11, ZEK). Navedeni članak ZEK-a bitno je izmijenjen 2011. kada su u njega ugrađene odredbe koje operatorima i regulatornom tijelu nameću dodatne obveze vezane uz sigurnost i cjelovitost elektroničkih komunikacijskih mreža i usluga.

Izmjene članka 99. učinjene su radi usklađivanja s regulatornim okvirom EU u području elektroničkih komunikacija, posebice s odredbom članka 13.a Okvirne Direktive (Direktiva br. 2002/21/EC, izmijenjena i dopunjena Direktivom br. 2009/140/EC)

Prema izmijenjenom članku 99. ZEK-a operatoru su, između ostalog, dužni obavijestiti HAKOM o sigurnosnim incidentima koji su od značajnog utjecaja na rad mreža ili obavljanje usluga. S druge strane, HAKOM je obvezan prema potrebi, izvijestiti ENISA-u (*European Network and Information Security Agency*) i nadležna nacionalna regulatorna tijela drugih država članica Europske unije o povredi sigurnosti ili gubitku cjelovitosti mreže. Osim toga, jedanput godišnje HAKOM je obvezan dostaviti Komisiji i ENISA-i sažeto izvješće o obavijestima o sigurnosnim incidentima koje su zaprimljene u tijeku protekle kalendarske godine te o mjerama koje su poduzete u vezi sa zaprimljenim obavijestima.

Ovim Pravilnikom uređuju se stoga konkretne sigurnosne mjere koje su operatori dužni poduzeti te način i rokovi u kojima su operatori dužni obavijestiti HAKOM o sigurnosnim incidentima.

Prilikom izrade Pravilnika vodilo se računa o tehničkim uputama ENISA-e za primjenu članka 13.a Okvirne Direktive.

Pravilnik se sastoji od normativnog dijela i dodataka koji čine njegov sastavni dio.

U članku 3. propisane su mjere za osiguranje sigurnosti i integriteta javnih komunikacijskih mreža i/ili usluga koje operatori moraju poduzeti. U Dodatku 1. dane su referentne norme za provođenje mjera iz članka 3. i njihov opis.

U članku 4. propisani su rokovi i način obavještavanja HAKOM-a o sigurnosnim incidentima. U Dodatku 2. pobliže su opisani sigurnosni incidenti i kriteriji za izvješćivanje. U Dodatku 3. propisani su obrasci za izvješćivanje.

U članku 5. propisane su obveze izvještavanja drugih subjekata o sigurnosnim incidentima.