NN 66/2019 (10.7.2019.), Pravilnik o izmjenama i dopunama Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga

HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

1312

Na temelju članka 12. stavka 1. točke 1., članka 19. stavka 1. i članka 99. stavka 9. Zakona o elektroničkim komunikacijama (»Narodne novine« br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), Vijeće Hrvatske regulatorne agencije za mrežne djelatnosti donosi

PRAVILNIK

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

Članak 1.

U Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (»Narodne novine« br. 109/12, 33/13, 126/13, 67/16; dalje: Pravilnik), u članku 2. iza točke 3. dodaje se nova točka 4. koja glasi:

»4. računalno-sigurnosni incident: jedan ili više računalnih sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava ili računalne mreže, te ugrožavaju povjerljivost, cjelovitost i dostupnost informacija koji se korištenjem informacijskog sustava ili računalne mreže kreiraju, obrađuju, pohranjuju ili prenose.«

Članak 2.

U Pravilniku iza članka 4. dodaje se novi članak 5. koji glasi:

»Članak 5.

(1) Operatori su obvezni obavijestiti Agenciju o svakom značajnom računalno-sigurnosnom incidentu koji je značajnije utjecao na dostupnost, cjelovitost ili povjerljivost informacijskog sustava ili računalne mreže, sukladno kriterijima za izvješćivanje iz Dodatka 2. ovog Pravilnika. Prilikom podnošenja prijava sukladno ovom članku, u cijelosti se primjenjuje Nacionalna taksonomija računalno-sigurnosnih incidenata.

(2) O računalno-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 24 sata nakon otkrivanja računalno-sigurnosnog incidenta

2. u roku od najviše 20 dana od dana otklanjanja računalno-sigurnosnog incidenta.

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

(4) Nakon pribavljanja potpunih informacija sukladno ovom članku, Agencija će informacije o prijavljenim računalno-sigurnosnim incidentima dostaviti CERT-u kao nacionalnom tijelu za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

(5) Nakon razmatranja prijavljenih incidenata, Agencija će u suradnji s Nacionalnim CERT-om, naložiti eventualnu dopunu izvješća te poduzimanje drugih mjera propisanih Zakonom, uključujući i davanje određenih preporuka, smjernica i upozorenja o sigurnosnim ugrozama.

(6) U slučaju potrebe pokretanja odgovarajućeg postupka iz nadležnosti Agencije u odnosu na prijavljene incidente, Agencija će aktivno surađivati sa CERT-om, te u slučaju potrebe zatražiti stručnu pomoć i koordinaciju pri definiranju konkretnih aktivnosti i korektivnih mjera u vezi s nastalim ili potencijalnim računalno-sigurnosnim incidentima.

(7) Nacionalni CERT će temeljem prikupljenih prijava dobivenih putem adrese elektroničke pošte navedene u stavku 3. ovog članka, dostaviti Agenciji najmanje jednom mjesečno izvješće o značajnim incidentima iz prethodnog razdoblja.

(8) U slučaju osiguravanja alternativnog načina podnošenja prijava pri CERT-u putem odgovarajuće platforme, Agencija će obavijestiti operatore o promijeni načina prijavljivanja značajnih računalno-sigurnosnih incidenata.«

Članak 3.

(1) Dosadašnji članak 5. Pravilnika postaje članak 6. Pravilnika.

(2) Dosadašnji članak 6. Pravilnika postaje članak 7. Pravilnika.

Članak 4.

Dodatak 2. Pravilnika mijenja se novim Dodatkom 2. koji glasi:

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	12 670 korisnika	8 sati
Onemogućena govorna usluga u nepokretnoj mreži	25 340 korisnika	6 sati
Onemogućena govorna usluga u nepokretnoj mreži	63 350 korisnika	4 sata
Onemogućena govorna usluga u nepokretnoj mreži	126 700 korisnika	2 sata
Onemogućena govorna usluga u nepokretnoj mreži	190 000 korisnika	1 sat
Onemogućena govorna usluga u pokretnoj mreži	45 465 korisnika	8 sati
Onemogućena govorna usluga u pokretnoj mreži	90 930 korisnika	6 sati
Onemogućena govorna usluga u pokretnoj mreži	227 326 korisnika	4 sata
Onemogućena govorna usluga u pokretnoj mreži	454 652 korisnika	2 sata
Onemogućena govorna usluga u pokretnoj mreži	681 979 korisnika	1 sat
Onemogućena usluga pristupa internetu u nepokretnoj mreži	11 133 korisnika	8 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	22 266 korisnika	6 sati
Onemogućena usluga pristupa internetu u nepokretnoj mreži	55 666 korisnika	4 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	111 333 korisnika	2 sata
Onemogućena usluga pristupa internetu u nepokretnoj mreži	167 000 korisnika	1 sat
Onemogućena usluga pristupa internetu u pokretnoj mreži	35 814 korisnika	8 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	71 628 korisnika	6 sati
Onemogućena usluga pristupa internetu u pokretnoj mreži	179 070 korisnika	4 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	358 140 korisnika	2 sata
Onemogućena usluga pristupa internetu u pokretnoj mreži	537 211 korisnika	1 sat

Računalno-sigurnosni incident		**Uvjeti prijave računalno-sigurnosnog incidenta**
Kategorija	**Potkategorija**	
Uspješno ostvarena kompromitacija	Malware URL	Zlonamjerna funkcionalnost aktivna je duže od 12 sati.
	Phishing URL	
	Spam URL	
	Web Defacement	
	Sustav zaražen zlonamjernim kodom	
	C&C	
	Korisnički račun	
Pokušaj neovlaštenog pristupa	Pogađanje zaporki	Potrebno je prijaviti svaki slučaj detektiranog pokušaja neovlaštenog pristupa.
	Pokušaj iskorištavanja ranjivosti	
Dostupnost	DoS -Volumetrički napad	Potrebno je prijaviti napade na infrastrukturu operatora koji pruža uslugu pristupa internetu.
	DoS – Napad na aplikacijskom sloju	

Prijevare	Phishing	Potrebno je prijaviti svaki detektirani slučaj ciljanog *phishing* napada (kampanje) prema davatelju usluge pristupa internetu koji za cilj ima stjecanje financijske koristi, krađu osjetljivih podataka ili pokretanje zlonamjernog programa.
Ciljani napad – APT (eng. *Advanced persistent threat)*		Potrebno je prijaviti svaki slučaj ovakvog oblika napada.
Ostalo		Prijava po procjeni operatora davatelja usluga

Članak 5.

Dodatak 3. Pravilnika mijenja se novim Dodatkom 3. koji glasi:

DODATAK 3

PREDLOŽAK ZA IZVJEŠĆIVANJE SIGURNOSNIH INCIDENATA

Potrebni podaci	Popunjava operator
Opis sigurnosnog incidenta	
Naziv operatora	
Datum i vrijeme nastanka/otkrivanja sigurnosnog incidenta	
Izvorni uzrok	☐ Sistemska greška ☐ Ljudska greška ☐ Zlonamjerne radnje ☐ Prirodni fenomen ☐ Greška treće strane
Početni uzrok	☐ Požar ☐ Prekid kabela ☐ Krađa kabela ☐ Prekid hlađenja ☐ Duži napad ☐ Zemljotres ☐ Elektromagnetska interferencija ☐ Pogrešna zamjena/nadogradnja hardvera ☐ Pogrešna zamjena/nadogradnja softvera ☐ Vatra ☐ Poplava ☐ Izrijekom zabrinjavajuće ☐ Kvar na hardveru ☐ Krađa hardvera ☐ Obilan snijeg/led ☐ Oluja ☐ Zlonamjerni softveri i virusi ☐ Prestrukturiranje uvršnog prometa ☐ Nema informacije ☐ Nitko ☐ Preopterećenje ☐ Proceduralna greška ☐ Prekid napajanja ☐ Strujni udari ☐ Sigurnosno isključivanje ☐ Softverska greška ☐ Teroristički napad ☐ Požar ☐ Drugo
Naknadni uzrok	☐ Požar ☐ Prekid kabela ☐ Krađa kabela ☐ Prekid hlađenja ☐ Duži napad ☐ Zemljotres ☐ Elektromagnetska interferencija ☐ Pogrešna zamjena/nadogradnja hardvera ☐ Pogrešna zamjena/nadogradnja softvera ☐ Vatra ☐ Poplava ☐ Izrijekom zabrinjavajuće ☐ Kvar na hardveru ☐ Krađa hardvera ☐ Obilan snijeg/led ☐ Oluja ☐ Zlonamjerni softveri i virusi ☐ Prestrukturiranje uvršnog prometa ☐ Nema informacije ☐ Nitko ☐ Preopterećenje ☐ Proceduralna greška ☐ Prekid napajanja ☐ Strujni udari ☐ Sigurnosno isključivanje ☐ Softverska greška ☐ Teroristički napad ☐ Požar ☐ Drugo
Imovina obuhvaćena incidentom	☐ Aktivni poslužitelji ☐ Rezervno napajanje ☐ Sustavi razlistat i povezivanja ☐ Zgrade i fizički sigurnosni sustavi ☐ Sustav hlađenja ☐ Inteligentni uvršni uređaji ☐ Medukomunikacijske točke ☐ Logički sigurnosni sustavi ☐ Bazne stanice i upravljački sklopovi ☐ Centar za razmjenu poruka ☐ Nema informacije ☐ Operativni sustav poljoprivredni ☐ Nadzorni kabeli ☐ PSTN prospojnici ☐ Sustav napajanja ☐ Ulični kabineti ☐ Pozivnički kabeli ☐ Pretplatnička oprema ☐ Prospojnici i usmjerivači ☐ Prijenosni čvorovi