NN 112/2021 (15.10.2021.), Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga

HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

1957

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 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 pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga (dalje: pružatelji) moraju poduzimati sve odgovarajuće mjere kako bi zajamčili sigurnost i 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) o povredi sigurnosti i/ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga.

POJMOVI I ZNAČENJA

Članak 2.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *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,

2. *ENISA (eng. European Union Agency for Network and Information Security):* Agencija Europske unije za mrežnu i informacijsku sigurnost,

3. *IKT proizvod, proces ili usluga:* značenje kako je propisano Uredbom (EU) 2019/881

4. *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,

5. *Nacionalna taksonomija računalno-sigurnosnih incidenata:* ujednačeni kriteriji pri klasifikaciji računalno-sigurnosnih incidenata u vlastitim informacijskim i mrežnim sustavima, na nacionalnoj razini

6. *Nacionalni CERT:* nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj,

7. *PiXi platforma:* nacionalna platforma za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima te prijavu značajnih računalno-sigurnosnih incidenata,

8. *sigurnosna politika:* skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove vrijednosti, uključujući opremu (eng. *hardware),* programsku podršku (eng. *software)* i podatke,

9. *sigurnosni incident:* događaj koji ima stvarni negativni učinak na sigurnost elektroničkih komunikacijskih mreža ili usluga,

10. *sigurnost mreža i usluga:* sposobnost elektroničkih komunikacijskih mreža i usluga da, određenom pouzdanošću, odolijevaju bilo kojoj radnji kojom se ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost tih mreža i usluga, pohranjenih ili prenesenih ili obrađenih podataka, ili srodnih usluga koje se pružaju ili su dostupne tim elektroničkim komunikacijskim mrežama ili uslugama,

11. *utjecaj na autentičnost:* kompromitiranje korisničkog identiteta,

12. *utjecaj na cjelovitost:* namjerno ili slučajno neovlašteno mijenjanje komunikacijskih podataka ili metapodataka,

13. *utjecaj na dostupnost:* djelovanje na kontinuitet pružanja usluge, degradiranje performanse usluge, te djelomični ili potpuni pad mreže ili usluge,

14. *utjecaj na povjerljivost:* kompromitiranje povjerljivosti komunikacije, komunikacijskih podataka ili metapodataka,

15. *značajan računalno-sigurnosni incident:* računalno-sigurnosni incident koji utječe na kritične podatke (neklasificirane i klasificirane) i/ili informacijske sustave i računalne mreže u javnom i privatnom sektoru, posebice na sustave koji su dio nacionalne kritične infrastrukture, na kojima se ti podaci obrađuju i kojima se prenose te koji može ostvariti i/ili ostvaruje negativan utjecaj na svakodnevni život velikog broja građana, nacionalnu ekonomiju i nacionalnu sigurnost u cjelini.

MJERE ZA ZAŠTITU SIGURNOSTI I CJELOVITOSTI MREŽA I USLUGA

Opće obveze

Članak 3.

(1) Pružatelji su obvezni poduzimati odgovarajuće tehničke i ustrojstvene mjere, uključujući šifriranje kada je primjereno, radi zaštite sigurnosti i cjelovitosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže i usluge, pri čemu poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga.

(2) Tehničke i ustrojstvene mjere iz stavka 1. ovog članka osobito uključuju:

– sustav upravljanja rizicima koji obuhvaća i sigurnosnu politiku te je temeljen na procjeni rizika, uz odgovarajuću primjenu mjerodavnih tehničkih smjernica ENISA-e o prijetnjama

– sigurnosne zahtjeve za osoblje

– sigurnost sustava i prostora

– upravljanje postupcima

– upravljanje sigurnosnim incidentima

– upravljanje kontinuitetom poslovanja

– nadzor i testiranje sigurnosti

– svjesnost o sigurnosnim prijetnjama.

(3) Pri poduzimanju mjera iz stavka 1. i 2. ovog članka, pružatelji u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama, prijetnjama te druge relevantne smjernice.

(4) Popis referentnih normi za provođenje mjera iz stavka 1. i 2. ovog članka nalazi se u Dodatku 1. ovog Pravilnika.

(5) Osim referentnih normi iz Dodatka 1. ovog Pravilnika, pružatelji mogu primijeniti i druge odgovarajuće norme te mjerodavne nacionalne i/ili međunarodne sigurnosne standarde u svrhu ostvarivanja mjera iz ovog Pravilnika.

(6) Mjerama iz stavka 2. ovog članka mora se osigurati i primjena sigurnosne politike kod obrade i zaštite osobnih podataka.

(7) Pružatelji su obvezni dokumentirati poduzete i implementirane mjere iz stavka 2. i 6. ovog članka te ih učiniti

dostupnim Agenciji na njezin zahtjev.

(8) Pružatelji koji imaju više od 100 000 korisnika obvezni su elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja, dostaviti Agenciji sigurnosnu politiku za prethodnu godinu koja obuhvaća mjere iz Dodatka 1. i članka 4. ovog Pravilnika, a na zahtjev Agencije i više puta tijekom godine. Pružatelji koji imaju manje od 100 000 korisnika obvezni su dostaviti Agenciji sigurnosnu politiku na njezin zahtjev.

Sigurnost 5G mreža i usluga

Članak 4.

(1) U odnosu na 5G mreže, sigurnosna politika mora sadržavati i popis kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže, uzimajući u obzir popis kritičnih i osjetljivih dijelova 5G mreže definiran dokumentom EU koordinirana procjena rizika kibernetičke sigurnosti u 5G mrežama.

(2) Uz mjere iz članka 3. stavka 2. ovoga Pravilnika, pružatelji za 5G obvezni su implementirati sljedeće dodatne tehničke i organizacijske mjere:

– oprema za kritične i osjetljive dijelove 5G mreže mora zadovoljavati mjerodavne 5G standarde, osobito 3GPP standarde sukladno mjerodavnim smjernicama ENISA-e, kao i primjenjive EU i nacionalne programe (certifikacijske sheme) kibernetičke sigurnosti

– sustav sigurnosti opskrbe 5G opreme, što između ostalog uključuje procjenu sigurnosti svih odabranih izvođača, proizvođača i njihovih dobavljača, te sustav nadzora nad načinom i kvalitetom pružanja ugovorenih poslova i usluga uz odgovarajuću primjenu mjerodavnih smjernica ENISA-e vezano uz nabavu sigurnih IKT procesa, proizvoda i usluga

– korištenje dobavljača koji dokažu odgovarajuću razinu dugoročne održivosti/otpornosti opreme i/ili IKT procesa, proizvoda i usluga

– provođenje sigurnosne kontrole u skladu s mjerodavnim standardima za sigurnost 5G mreža i usluga

– sustav ograničenja i nadzora udaljenog pristupa kritičnom dijelu mreže i informacijskom sustavu od trećih strana te implementacija, gdje je moguće, principa najmanje privilegiranog i podjela dužnosti

– operativni centar (NOC) i sigurnosno-operativni centar (SOC) mora se nalaziti na području neke od zemalja članicama Europske unije

– NOC i SOC, svako u svom djelokrugu rada, moraju provoditi nadzor kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreža u svrhu pravovremenog otkrivanja nepravilnosti te prepoznavanja i sprečavanja prijetnji

– mjere zaštite upravljanja prometom komunikacijskih mreža ili usluga kako bi se spriječile neovlaštene promjene na mrežnim ili uslužnim komponentama

– mjere fizičke zaštite MEC-a (Multi-access Edge Computing) i baznih stanica temeljeno na procjeni rizika primjerice s obzirom na to gdje se komponente raspoređuju i koriste, te posebne mjere pristupa ograničenom broju sigurnosno provjerenom, kvalificiranom osoblju uz ograničen i nadziran pristup trećih strana

– alati i procesi za osiguravanje integriteta softvera prilikom njegovog ažuriranja i primjene sigurnosnih zakrpa, pouzdane identifikacije i praćenja promjena i statusa zakrpa, osobito u virtualiziranim mrežnim funkcijama

– procedure u svrhu oporavka u slučaju incidenata koji ima utjecaj i na međuovisne kritične sektore i usluge.

(3) Pri poduzimanju mjera iz stavka 2. ovog članka, pružatelji u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama 5G mreža.

(4) Pružatelji su obvezni dokumentirati mjere iz stavka 2. ovog članka.

Revizija sigurnosti mreža i usluga

Članak 5.

(1) Pružatelji su obvezni najmanje jednom godišnje provoditi procjenu rizika te reviziju sigurnosti mreža i usluga kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti iz Dodatka 1 i članka 4. ovog Pravilnika, uzimajući pri tom u obzir rezultate prethodnih revizija.

(2) Reviziju mogu obavljati zaposlenici pružatelja koji nisu vezani za područje revizije i koji imaju odgovarajuće znanje i iskustvo ili vanjsko revizorsko tijelo.

(3) Nalaz revizije iz stavka 1. ovog članka, zajedno s planom uklanjanja uočenih nedostataka, pružatelji koji imaju više od 100 000 korisnika su obvezni dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu. Pružatelji koji imaju manje od 100 000 korisnika obvezni su dostaviti Agenciji nalaz revizije na njezin zahtjev.

(4) U slučaju da plan uklanjanja uočenih nedostataka iz stavka 3. ovog članka ne ocijeni primjerenim za sprječavanje i umanjenje utjecaja sigurnosnih i računalno-sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže ili za osiguranje cjelovitosti mreža i usluga, Agencija može pružateljima odrediti dodatne mjere.

(5) Agencija može donositi obvezujuće upute, što uključuje mogućnost naloga pružateljima za poduzimanjem mjera u svrhu sprečavanja sigurnosnog incidenta kada se utvrdi znatna prijetnja i /ili rješavanja sigurnosnog incidenta i vremenske rokove provedbe.

(6) Neovisno o rezultatima revizije, Agencija može pružateljima određivati mjere radi osiguranja sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga, osobito 5G mreža, ukoliko ocijeni da je to potrebno iz razloga nacionalne sigurnosti, temeljem prethodnog mišljenja nadležnog tijela za zaštitu nacionalne sigurnosti ili radi osiguranja ključnih usluga definiranih mjerodavnim zakonom, na prijedlog nadležnih tijela.

OBAVJEŠTAVANJE AGENCIJE O SIGURNOSNIM INCIDENTIMA

Članak 6.

(1) Pružatelji su obvezni obavijestiti Agenciju o sigurnosnom incidentu koji je značajnije utjecao na rad mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2., pri čemu pružatelji provjeravaju ispunjavanje Kvantitativnih kriterija te ukoliko isti nisu zadovoljeni provjeravaju ispunjenost Kvalitativnih kriterija iz navedenog Dodatka. U slučaju svakog sigurnosnog incidenta, pružatelji uvijek moraju provjeriti je li došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata iz navedenog Dodatka.

(2) U slučaju da dođe do ispada barem jednog od dva redundantna kabela/informacijska sustava, pružatelji su obvezni prijaviti navedeni sigurnosni incident kao incident koji ima utjecaj na redundanciju, odgovarajućom primjenom predloška iz Dodatka 3. ovog Pravilnika.

(3) Obavijest o sigurnosnim incidentima iz stavka 1. ovog članka mora se dostaviti Agenciji bez odgode, čim su podaci dostupni, i to putem predloška 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.

(4) U slučaju nastanka sigurnosnog incidenta koji ispunjava kvantitativne ili kvalitativne kriterije za izvješćivanje te je ujedno došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata iz Dodatka 2., pružatelji su obavezni dostaviti Agenciji obavijest o navedenom incidentu putem predloška iz Dodatka 3. ovog Pravilnika i putem PiXi platforme. Dodatne obveze za prijavu značajnih računalno-sigurnosnih incidenata propisane su u članku 7. ovog Pravilnika.

(5) Pružatelji su obvezni osigurati Agenciji podatke za kontakt sukladno Dodatku 3 ovog Pravilnika u svrhu brze razmjene informacija o sigurnosnim incidentima, te pružiti potrebne tehničke informacije Agenciji radi praćenja sigurnosti i integriteta javnih komunikacijskih mreža.

(6) 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 predlošku iz Dodatka 3. ovog Pravilnika.

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

(8) Pružatelji mogu obavijestiti Agenciju i o drugim, po njihovom mišljenju, 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. ovog članka.

DODATNE OBVEZE ZA ZNAČAJNE

RAČUNALNO-SIGURNOSNE INCIDENTE

Članak 7.

(1) Obavijesti o značajnim računalno-sigurnosnim incidentima sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata moraju se dostavljati putem PiXi platforme. Uvjeti i način korištenja ove platforme propisani su u Uvjetima korištenja PiXi platforme koja se nalazi na internetskoj stranici Nacionalnog CERT-a.

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

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

OBAVJEŠTAVANJE DRUGIH SUBJEKATA O SIGURNOSNIM INCIDENTIMA

Članak 8.

Pružatelji su obvezni bez odgode:

1. na jasan i lako dokaziv način obavijestiti korisnike svojih usluga o sigurnosnom incidentu koji je značajnije utjecao na rad javnih komunikacijskih mreža i/ili usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2. te objaviti informacije o nastalom značajnom incidentu na svojoj službenoj internetskoj stranici. Informacije o značajnom incidentu moraju sadržavati opis područja obuhvaćenog incidentom, koji može biti prikazan i u kartografskom obliku.

2. u slučaju osobite opasnosti od sigurnosnog incidenta u javnim elektroničkim komunikacijskim mrežama ili javno dostupnim elektroničkim komunikacijskim uslugama, obavijestiti korisnike svojih usluga na koje bi takva opasnost mogla utjecati, o raspoloživim mjerama za uklanjanje opasnosti i/ili njezinih posljedica, a ako je primjereno i o sigurnosnoj prijetnji.

ZAVRŠNE ODREDBE

Članak 9.

1. Stupanjem na snagu ovog Pravilnika prestaje vrijediti Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 109/12, 33/13-ispravak, 126/13, 67/16 i 66/19).

2. Ovaj Pravilnik stupa na snagu 30 dana od dana objave u »Narodnim novinama«, osim članka 4. koji stupa na snagu 1. lipnja 2022.

Klasa: 011-02/21-02/10

Urbroj: 376-05-4-21-3

Zagreb, 14. listopada 2021.

Predsjednik Vijeća

Tonko Obuljen, v. r.

DODATAK 1

MINIMALNE MJERE SIGURNOSTI

Minimalne mjere sigurnosti	Referentne norme
Sustav za upravljanja rizicima	ISO 27001:2013 ISO 27002:2013 ISO 27005:2018 ISO 27036-3:2013
Sigurnosni zahtjevi za osoblje	ISO 27001:2013 ISO 27002:2013
Sigurnost sustava i objekata (prostora)	ISO 27001:2013 ISO 27002:2013
Upravljanje operacijama (postupcima)	ISO 27001:2013 ISO 27002:2013

Upravljanje sigurnosnim incidentima	ISO 27001:2013 ISO 27002:2013
Upravljanje kontinuitetom poslovanja	ISO 27001:2013 ISO 27002:2013 ISO 22301:2019
Nadzor i testiranje sigurnosti	ISO 27001:2013 ISO 27002:2013
Svjesnost o sigurnosnim prijetnjama	ISO 27001:2013 ISO 27002:2013

DODATAK 2

KVANTITATIVNI KRITERIJI ZA IZVJEŠĆIVANJE

Sigurnosni incident utječe na: **govornu uslugu u nepokretnoj mreži/govornu uslugu u pokretnoj mreži/uslugu pristupa internetu u nepokretnoj mreži/uslugu pristupa internetu u pokretnoj mreži/brojevno neovisnu interpersonalnu komunikacijsku uslugu/uslugu komunikacije između strojeva (M2M)/uslugu odašiljanja radijskih i televizijskih programa**	**Minimum krajnjih korisnika obuhvaćenih sigurnosnim incidentom** [1]	**Minimalno trajanje sigurnosnog incidenta**
Dostupnost	1% – 2%	8 sati
Dostupnost	2% – 5%	6 sati
Dostupnost	5% – 10%	4 sata
Dostupnost	10% – 15%	2 sata
Dostupnost	> 15%	1 sat
Dostupnost	> 1 000 000 korisnik/sati	
Povjerljivost/ autentičnost/ cjelovitost	> 1%	Neovisno o trajanju

[1](Podatak se dobiva na način da se broj korisnika obuhvaćenih incidentom podijeli s ukupnim brojem korisnika pojedine usluge u Hrvatskoj (godišnji podaci dostupni su internetskoj stranici Agencije) te podijeli sa 100.)

KVALITATIVNI KRITERIJI ZA IZVJEŠĆIVANJE

Sigurnosni incident	**Dostupnost/povjerljivost/ autentičnost/cjelovitost usluge**
1. Značajan zbog geografskog obuhvata incidenta (prekogranično, velika udaljena/ruralna područja, otoci, grad Zagreb i sl.) 2. Značajan zbog utjecaja na gospodarstvo i društvo ili na korisnike (nemogućnost pristupa 112, nacionalnim brojevima za hitne službe, utjecaj na javne sustave upozorenja, velika materijalna šteta, visoki rizici za javnu sigurnost ili gubitak života, medijska pokrivenost, utjecaj na kontinuitet osnovnih usluga ili kritičnih sektora/operatora, utjecaj na posebne dane kao dana izbora ili referenduma.)	neovisno o trajanju i broju korisnika

DODATAK 3

PREDLOŽAK ZA IZVJEŠĆIVANJE O SIGURNOSNOM INCIDENTU

Potrebni podaci	**Popunjava operator**
Naziv operatora	
Datum podnošenja izvještaja	
Datum i vrijeme nastanka/ otkrivanje sigurnosnog incidenta	
Opis incidenta	

Tip incidenta	☐ A – Ispad usluge (npr. kontinuitet, dostupnost) ☐ B – Drugi utjecaj na usluge (npr. povjerljivost, cjelovitost, autentičnost) ☐ C – Utjecaj na druge sustave (npr. ucjenjivački zlonamjerni softver u uredskoj mreži, bez utjecaja na uslugu)	☐ D – Prijetnja ili ranjivost (npr. otkrivanje slabosti u kriptiranju) ☐ E – Utjecaj na redundanciju (npr. prelazak na redundanciju ili sigurnosni sustav) ☐ F – Zamalo incident (npr. aktivacija sigurnosnih mjera)	
Obuhvaćene usluge	☐ Nepokretna telefonija	Broj korisnika	Trajanje
	☐ Pokretna telefonija	Broj korisnika	Trajanje
	☐ Nepokretni internet	Broj korisnika	Trajanje
	☐ Pokretni internet	Broj korisnika	Trajanje
	☐ OTT usluge	Broj korisnika	Trajanje
	☐ M2M	Broj korisnika	Trajanje
	☐ Emitiranje	Broj korisnika	Trajanje
	☐ Drugo	Broj korisnika	Trajanje

Izvorni uzrok	☐ Sistemske greške ☐ Ljudske greške ☐ Zlonamjerne radnje ☐ Prirodni fenomen ☐ Greška treće strane		
Tehnologija usluga ili podusluga	☐ Kabelska ☐ DSL ☐ Email ☐ Optika ☐ GRPS/EDGE ☐ GSM	☐ Instant messaging protokol ☐ LTE ☐ MTC ☐ PSTN ☐ Signalizacijski protokol ☐ UMTS	☐ URLLC ☐ VoIP ☐ Web/App ☐ eMBB ☐ Drugo
Tehnički uzroci	☐ Palež ☐ Presjek kabela ☐ Krađa kabela ☐ Prekid hlađenja ☐ DDoS napad ☐ Zemljotres ☐ Prisluškivanje ☐ Elektromagnetska interferencija ☐ Vanjski okolišni uzroci ☐ Neispravna promjena/ažuriranje hardvera	☐ Neispravna promjena/ažuriranje softvera ☐ Vatra ☐ Poplava ☐ Iscrpljene zalihe goriva ☐ Kvar na hardveru ☐ Krađa hardvera ☐ Obilan snijeg/led ☐ Oluja ☐ Krađa identiteta ☐ Zlonamjerni softveri i virusi ☐ Preotimanje mrežnog prometa	☐ Preopterećenje ☐ Phishing ☐ Proceduralna mana ☐ Prekid napajanja ☐ Strujni udari ☐ Sigurnosno isključivanje ☐ Softverska greška ☐ Iskorištavanje ranjivosti ☐ Požar ☐ Drugo
Tehnička imovina obuhvaćena incidentom	☐ Adresni poslužitelji ☐ App ☐ Rezervno napajanje ☐ Sustav naplate i posredovanja ☐ Zgrade i fizički sigurnosni sustavi ☐ Pohrana u oblaku ☐ Sustav hlađenja ☐ Inteligentni mrežni uređaji ☐ Međukonekcijske točke	☐ Logički sigurnosni sustavi ☐ Bazne stanice i upravljački sklopovi ☐ Centar za razmjenu poruka ☐ Mobilni prospojnici ☐ Registar mobilnih korisnika i lokacija ☐ Operativni sustav potpore ☐ Nadzemni kablovi ☐ PSTN prospojnici	☐ Sustav napajanja ☐ SIM/eSIM ☐ Ulični kabineti ☐ Podmorski kabeli ☐ Pretplatnička oprema ☐ Prospojnici i usmjerivači ☐ Prijenosni čvorovi ☐ Podzemni kablovi ☐ Mrežna stanica ☐ Drugo
Čimbenici značajnosti	☐ Broj obuhvaćenih korisnika ☐ Trajanje incidenta ☐ Geografska proširenost	☐ Opseg poremećaja u funkcioniranju ☐ Utjecaj na ekonomiju i društvo	
Skala utjecaja	☐ Bez utjecaja ☐ Manji utjecaj	☐ Veliki utjecaj ☐ Vrlo veliki utjecaj	
Čimbenici ozbiljnosti prijetnje (za *tip D)*	☐ Troškovi ublažavanja ☐ Potencijalna šteta ☐ Stopa širenja prijetnje	☐ Vjerojatnost izlaganja ☐ Kritičnost potencijalno pogođenih sustava ☐ Nedostatak dobrih rješenja za ublažavanje prijetnje	
Ozbiljnost prijetnje (za *tip D)*	☐ Mala	☐ Srednja	☐ Velika

Rješavanje sigurnosnog incidenta i opis poduzetih mjera	
Mjere poduzete nakon otklanjanja sigurnosnog incidenta	
Dugoročne mjere	
Kontakt podaci za praćenje procesa	
Ostale važne informacije	