**HRVATSKA REGULATORNA AGENCIJA ZA**

**MREŽNE DJELATNOSTI**

Na temelju članka 12. stavka 2. točke 2., članka 16. stavka 1. točke 1. i članka 41. stavka 6. Zakona o elektroničkim komunikacijama (»Narodne novine« br. 76/2022), Vijeće Hrvatske regulatorne agencije za mrežne djelatnosti na sjednici održanoj 23. ožujka 2023. godine donosi

**PRAVILNIK**

**O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI MREŽA I USLUGA**

# I. OPĆE ODREDBE

Sadržaj pravilnika

## Članak 1.

Ovim Pravilnikom propisuju se način i rokovi u kojima operatori javnih elektroničkih komunikacijskih mreža i usluga te mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastruktura (dalje: operatori) moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere kako bi se zaštitila sigurnost njihovih mreža i usluga, način i rokovi izvješćivanja Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: Agencija) o sigurnosnim incidentima od značajnog utjecaja na rad mreža operatora ili obavljanje njihovih usluga, obveza provedbe godišnje revizije mjera sigurnosti mreža i usluga operatora te mjerila i način certificiranja pravnih osoba koje je za provedbu te revizije ovlastila Agencija.

Značenje pojmova

## Članak 2.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. ENISA (eng. European Union Agency for Cybersecurity): Europska agencija za kibernetičku sigurnost
2. IKT proizvod, proces ili usluga: značenje kako je propisano člankom 2. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013
3. Nacionalna taksonomija računalno-sigurnosnih incidenata: ujednačeni kriteriji pri klasifikaciji računalno- sigurnosnih incidenata na nacionalnoj razini u vlastitim informacijskim sustavima i računalnim mrežama
4. Nacionalni CERT: nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj
5. Nacionalno akreditacijsko tijelo: značenje kako je propisano člankom 2. točkom 11. Uredbe (EZ) br. 765/20085 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93
6. PiXi platforma: nacionalna platforma za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima te prijavu značajnih računalno-sigurnosnih incidenata
7. politika informacijske sigurnosti: skup pravila i postupaka koji definiraju na koji način se sredstva i resursi informacijske tehnologije trebaju koristiti i štititi te kako njima upravljati
8. računalno-sigurnosni incident: sigurnosni incident sukladno kriterijima Nacionalne taksonomije računalno-sigurnosnih incidenata
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, prenesenih ili obrađenih podataka, ili povezanih usluga koje se pružaju ili su dostupne tim elektroničkim komunikacijskim mrežama ili uslugama
11. utjecaj na autentičnost: utjecaj na svojstvo da je entitet ono za što tvrdi da jest (npr. kompromitiranje korisničkog identiteta)
12. utjecaj na cjelovitost: utjecaj na svojstvo točnosti i potpunosti (npr. namjerno ili slučajno neovlašteno mijenjanje ili uništavanje 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: dostupnost informacije neovlaštenim osobama, pojedincima, entitetima ili procesima (npr. 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.

# II. MJERE ZA ZAŠTITU SIGURNOSTI MREŽA I USLUGA

Opće obveze

## Članak 3.

1. Operatori su obvezni poduzeti odgovarajuće tehničke i ustrojstvene mjere, uključujući kodiranje (enkripciju) kada je to primjereno, radi zaštite sigurnosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike i na druge elektroničke komunikacijske mreže i usluge, pri čemu poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga, vodeći računa o raspoloživim tehničkim i tehnološkim rješenjima.
2. Tehničke i ustrojstvene mjere iz stavka 1. ovog članka minimalno uključuju:

* sustav upravljanja rizicima
* sigurnosne zahtjeve za osoblje
* sigurnost sustava i prostora
* upravljanje postupcima
* upravljanje sigurnosnim incidentima
* upravljanje kontinuitetom poslovanja
* nadzor i testiranje sigurnosti
* svjesnost o sigurnosnim prijetnjama.

1. Pri poduzimanju mjera iz stavka 1. i 2. ovog članka, operatori u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama, prijetnjama te druge relevantne smjernice.
2. Popis referentnih normi za provođenje mjera iz stavka 1. i 2. ovog članka nalazi se u Dodatku 1. ovog Pravilnika.
3. Mjerama iz stavka 2. ovog članka mora se osigurati i primjena sigurnosne politike kod obrade i zaštite osobnih podataka.
4. Operatori su obvezni dokumentirati poduzete i implementirane mjere iz stavka 2. ovog članka te ih učiniti dostupnim Agenciji na njezin zahtjev. Agencija nadzire mjere koje u provedbi ovog članka poduzimaju operatori te može predlagati zaštitne mjere u skladu s odgovarajućom razinom sigurnosti.
5. Operatori koji imaju više od 100 000 korisnika obvezni su elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja, dostaviti Agenciji politike informacijske sigurnosti za prethodnu godinu, a na zahtjev Agencije i više puta tijekom godine. Operatori koji imaju manje od 100 000 korisnika moraju dostaviti Agenciji politiku informacijske sigurnosti na njezin zahtjev.

Sigurnost 5G mreža i usluga

## Članak 4.

1. U odnosu na 5G mreže, politika informacijske sigurnosti 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, operatori za 5G moraju 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.

1. Pri poduzimanju mjera iz stavka 2. ovog članka, operatori u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama 5G mreža.
2. Operatori su obveznidokumentirati mjere iz stavka 2. ovog članka.

Revizija sigurnosti mreža i usluga

## Članak 5.

1. Operatori 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 obavlja vanjsko revizorsko tijelo koje je Agencija za to ovlastila sukladno članku 9. ovoga Pravilnika.
3. Procjenu rizika te nalaz revizije iz stavka 1. ovog članka, zajedno s planom tretiranja rizika te planom uklanjanja uočenih nedostataka, operatori koji imaju više od 100 000 korisnika obvezni su dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu. Operatori 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/ili za osiguranje sigurnosti mreža i usluga, Agencija može operatorima odrediti dodatne mjere.
5. Agencija može donositi obvezujuće upute, što uključuje mogućnost naloga operatorima za poduzimanjem mjera u svrhu sprečavanja sigurnosnih incidenata kada se utvrdi znatna prijetnja te mjera za uklanjanje posljedica sigurnosnih incidenata kao i rokove provedbe tih mjera.

# III. SIGURNOSNI INCIDENTI

Obavještavanje Agencije o sigurnosnim incidentima

## Članak 6.

1. Operatori su obvezni obavijestiti Agenciju o sigurnosnom incidentu koji je značajnije utjecao na rad mreža ili obavljanje usluga sukladno kriterijima za izvješćivanje iz Dodatka 2., pri čemu operatori provjeravaju ispunjavanje Kvantitativnih kriterija te ukoliko isti nisu zadovoljeni provjeravaju ispunjenost Kvalitativnih kriterija iz navedenog Dodatka.
2. U slučaju da dođe do ispada barem jednog od dva redundantna kabela/informacijska sustava, operatori 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:
4. u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2,
5. u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta,
6. u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta.
7. U slučaju nastanka sigurnosnog incidenta koji ispunjava kvantitativne ili kvalitativne kriterije za izvješćivanje iz Dodatka 2. te je ujedno došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata, operatori su obavezni dostaviti Agenciji obavijest o navedenom incidentu putem predloška iz Dodatka 3. ovog Pravilnika i Nacionalnom CERT-u putem PiXi platforme. Dodatne obveze za prijavu značajnih računalno-sigurnosnih incidenata propisane su u članku 7. ovog Pravilnika.
8. Operatori 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 njihovih mreža i usluga.
9. Sve obavijesti o sigurnosnim incidentima moraju se dostavljati Agenciji elektroničkim putem, zaštićeno zaporkom, na adresu elektroničke pošte [incidenti@hakom.hr](mailto:incidenti@hakom.hr) ili na drugi prikladan način sukladno predlošku iz Dodatka 3. ovog Pravilnika. Nakon što operator prvi puta dostavi obavijest o sigurnosnom incidentu, Agencija će operatoru dostaviti daljnje upute, odnosno upute vezane uz dostavu zaporke.
10. Agencija može zatražiti dopunu obavijesti iz stavka 3. u svrhu praćenja određenog sigurnosnog incidenta te boljeg razumijevanja prirode nastalog sigurnosnog incidenta.
11. Operatori mogu obavijestiti Agenciju i o drugim, po njihovom mišljenju, važnim sigurnosnim incidentima koji se odnose na sigurnost mreža ili usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavka 1. ovog članka.

Dodatne obveze za značajne računalno-sigurnosne incidente

## Članak 7.

1. U slučaju svakog sigurnosnog incidenta, operatori uvijek moraju provjeriti je li došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata.
2. Obavijesti o značajnim računalno-sigurnosnim incidentima sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata moraju se dostavljati putem PiXi platforme u roku 24 sata nakon njihovog otkrivanja. Uvjeti i način korištenja ove platforme propisani su u Uvjetima korištenja PiXi platforme koja se nalazi na internetskoj stranici Nacionalnog CERT-a.
3. 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.
4. 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 definiranju konkretnih aktivnosti i korektivnih mjera u vezi s nastalim ili potencijalnim računalno-sigurnosnim incidentima.

Obavještavanje drugih subjekata o sigurnosnim incidentima

## Članak 8.

1. Operatori su obvezni bez odgode:
2. na jasan i lako dokaziv način obavijestiti korisnike svojih usluga o sigurnosnom incidentu koji je značajnije utjecao na rad mreža ili obavljanje njihovih 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.
3. u slučaju posebne i znatne prijetnje od sigurnosnog incidenta u javnim elektroničkim komunikacijskim mrežama ili uslugama, obavijestiti korisnike svojih usluga na koje bi takva prijetnja mogla utjecati o svim mogućim mjerama zaštite ili pravnim sredstvima koja mogu uporabiti.
4. Operatori će o vlastitom trošku poduzeti odgovarajuće i hitne mjere u svrhu sprječavanja nastanka štete u slučaju sigurnosnog incidenta.

# IV. OVLAŠTENJE ZA OBAVLJANJE REVIZIJE SIGURNOSTI MREŽA I USLUGA

Ovlašteno revizorsko tijelo

## Članak 9.

1. Poslove revizije sigurnosti mreža i usluga operatora mogu obavljati pravne osobe na temelju rješenja o ovlaštenju koje donosi Agencija.
2. Agencija će izdati ovlaštenje ako je pravna osoba akreditirana od strane Hrvatske akreditacijske agencije ili drugog nacionalnog akreditacijskog tijela u smislu Uredbe (EZ) br. 765/2008, za obavljanje revizije informacijskih sustava sukladno važećim standardima ISO 27 001 i ISO 22 301.
3. Agencija donosi rješenje o ovlaštenju iz stavka 1. ovog članka temeljem zahtjeva pravne osobe. Zahtjev koji pravna osoba podnosi Agenciji mora sadržavati sljedeće:

* podatke o podnositelju zahtjeva
* presliku potvrde o akreditaciji iz stavka 2. ovoga članka.

1. Rješenje o ovlaštenju iz stavka 1. ovog članka može se vremenski ograničiti ili vrijediti do ukidanja.
2. Agencija će ukinuti rješenje o ovlaštenju iz stavka 1. ovog članka ako pravna osoba više ne ispunjava uvjete iz stavka 2. ovog članka.
3. Popis ovlaštenih pravnih osoba za obavljanje revizije sigurnosti mreža i usluga operatora vodi Agencija, koja ga redovito dopunjuje i objavljuje na svojim internetskim stranicama.

# V. PRIJELAZNE I ZAVRŠNE ODREDBE

## Članak 10.

Operatori mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastruktura obvezni su uskladiti svoj rad i poslovanje s odredbama ovog Pravilnika u roku od godine dana od dana stupanja na snagu ovog Pravilnika.

## Članak 11.

Stupanjem na snagu ovog Pravilnika prestaje vrijediti Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21).

## Članak 12.

Ovaj Pravilnik stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

KLASA: 011-02/23-02/05

URBROJ: 376-05-4-23-1

|  |  |
| --- | --- |
|  | PREDSJEDNIK VIJEĆA |
|  | Tonko Obuljen |

# DODATAK 1

## MINIMALNE MJERE SIGURNOSTI

|  |  |
| --- | --- |
| Minimalne mjere sigurnosti | Referentne norme |
| Sustav za upravljanja rizicima | ISO 27001  ISO 27002  ISO 27005  ISO 27036-3 |
| Sigurnosni zahtjevi za osoblje | ISO 27001  ISO 27002 |
| Sigurnost sustava i objekata (prostora) | ISO 27001  ISO 27002 |
| Upravljanje operacijama (postupcima) | ISO 27001  ISO 27002 |
| Upravljanje sigurnosnim incidentima | ISO 27001  ISO 27002 |
| Upravljanje kontinuitetom poslovanja | ISO 27001  ISO 27002  ISO 22301 |
| Nadzor i testiranje sigurnosti | ISO 27001  ISO 27002 |
| Svjesnost o sigurnosnim prijetnjama | ISO 27001  ISO 27002 |

# DODATAK 2

## KVANTITATIVNI KRITERIJI ZA IZVJEŠĆIVANJE

|  |  |  |
| --- | --- | --- |
| **Dostupnost:** | **Minimum krajnjih**  **korisnika obuhvaćenih sigurnosnim incidentom** | **Minimalno trajanje**  **sigurnosnog incidenta** |
| **Govorne usluge u nepokretnoj mreži** | 12 000 | 8 sati |
| **Govorne usluge u nepokretnoj mreži** | 24 000 | 6 sati |
| **Govorne usluge u nepokretnoj mreži** | 60 000 | 4 sata |
| **Govorne usluge u nepokretnoj mreži** | 120 000 | 2 sata |
| **Govorne usluge u nepokretnoj mreži** | 180 000 | 1 sat |
| **Govorne usluge u pokretnoj mreži** | 45 000 | 8 sati |
| **Govorne usluge u pokretnoj mreži** | 90 000 | 6 sati |
| **Govorne usluge u pokretnoj mreži** | 225 000 | 4 sata |
| **Govorne usluge u pokretnoj mreži** | 450 000 | 2 sata |
| **Govorne usluge u pokretnoj mreži** | 675 000 | 1 sat |
| **Usluge pristupa internetu u nepokretnoj mreži** | 11 000 | 8 sati |
| **Usluge pristupa internetu u nepokretnoj mreži** | 22 000 | 6 sati |
| **Usluge pristupa internetu u nepokretnoj mreži** | 55 000 | 4 sata |
| **Usluge pristupa internetu u nepokretnoj mreži** | 110 000 | 2 sata |
| **Usluge pristupa internetu u nepokretnoj mreži** | 165 000 | 1 sat |
| **Usluge pristupa internetu u pokretnoj mreži** | 50 000 | 8 sati |
| **Usluge pristupa internetu u pokretnoj mreži** | 100 000 | 6 sati |
| **Usluge pristupa internetu u pokretnoj mreži** | 250 000 | 4 sata |
| **Usluge pristupa internetu u pokretnoj mreži** | 500 000 | 2 sata |
| **Usluge pristupa internetu u pokretnoj mreži** | 750 000 | 1 sat |
| **Brojevno neovisne interpersonalne komunikacijske usluge** | 50 000 | 8 sati |
| **Brojevno neovisne interpersonalne komunikacijske usluge** | 100 000 | 6 sati |
| **Brojevno neovisne interpersonalne komunikacijske usluge** | 250 000 | 4 sata |
| **Brojevno neovisne interpersonalne komunikacijske usluge** | 500 000 | 2 sata |
| **Brojevno neovisne interpersonalne komunikacijske usluge** | 750 000 | 1 sat |
| **Povjerljivost/ autentičnost/ cjelovitost** | **Minimum krajnjih**  **korisnika obuhvaćenih sigurnosnim incidentom** | **Minimalno trajanje sigurnosnog incidenta** |
| **Govorna usluga u nepokretnoj mreži** | 12 000 | Neovisno o trajanju |
| **Govorna usluga u pokretnoj mreži** | 45 000 | Neovisno o trajanju |
| **Usluga pristupa internetu u nepokretnoj mreži** | 11 000 | Neovisno o trajanju |
| **Usluga pristupa internetu u pokretnoj mreži** | 50 000 | Neovisno o trajanju |
| **Brojevno neovisna interpersonalna komunikacijska usluga** | 50 000 | Neovisno o trajanju |

## KVALITATIVNI KRITERIJI ZA IZVJEŠĆIVANJE

|  |  |
| --- | --- |
| **Sigurnosni incident se odnosi 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** | **Dostupnost/ povjerljivost/ autentičnost/ cjelovitost usluge** |
| 1. Značajan zbog geografskog obuhvata incidenta (prekogranično, nacionalno, 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/otkrivanja sigurnosnog incidenta |  | | Datum i vrijeme  otklanjanja  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  Pokretna telefonija  Nepokretni internet  Pokretni internet  OTT usluge  M2M  Emitiranje  Drugo | |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika |  |  |  | | --- | --- | |  | Broj korisnika | | | | |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | Trajanje |  |  |  | | --- | --- | |  | 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 |  | | | | |