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.