NN 64/2018 (18.7.2018.), Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

HRVATSKI SABOR

Na temelju članka 89. Ustava Republike Hrvatske, donosim

ODLUKU

O PROGLAŠENJU ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Proglašavam Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, koji je Hrvatski sabor donio na sjednici 6. srpnja 2018.

Klasa: 011-01/18-01/79
Urbroj: 71-06-01/1-18-2
Zagreb, 10. srpnja 2018.

Predsjednica
Republike Hrvatske
Kolinda Grabar-Kitarović, v. r.

ZAKON

O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

DIO PRVI
OSNOVNE ODREDBE

Cilj i predmet

Članak 1.

(1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (u daljnjem tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe.

(2) Cilj je ovog Zakona osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.

(3) Sastavni su dio ovog Zakona:

a) Prilog I. – Popis ključnih usluga s kriterijima i pragovima za donošenje ocjene o važnosti negativnog učinka incidenta

b) Prilog II. – Popis digitalnih usluga

c) Prilog III. – Popis nadležnih tijela.

Usklađenost s propisima Europske unije

Članak 2.

(1) Ovim Zakonom se u hrvatsko zakonodavstvo preuzima Direktiva 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19. 7. 2016.).

(2) Ovim se Zakonom osigurava provedba Provedbene uredbe Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26/48, 31. 1. 2018. – u daljnjem tekstu: Provedbena uredba Komisije).

Primjena

Članak 3.

(1) Ovaj Zakon primjenjuje se na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu.

(2) Davatelji digitalnih usluga podliježu nadležnostima i ovlastima propisanim ovim Zakonom ako na teritoriju Republike Hrvatske imaju sjedište ili svog predstavnika te pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt maloga gospodarstva kako su oni definirani zakonom kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju maloga gospodarstva.

Odnos propisa prema drugim propisima

Članak 4.

(1) Ako u provedbi ovog Zakona nastaju ili se koriste klasificirani podaci ili se obrađuju osobni podaci, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti.

(2) Ako su za pojedini sektor s Popisa iz Priloga I. ovog Zakona posebnim zakonom propisane mjere koje po svom sadržaju i svrsi odgovaraju zahtjevima iz ovog Zakona, ili predstavljaju strože zahtjeve, na pružatelje ključnih usluga koji pripadaju tom sektoru primjenjuju se odgovarajuće odredbe tog posebnog zakona.

Pojmovi

Članak 5.

U smislu ovog Zakona pojedini pojmovi imaju sljedeće značenje:

1) *kibernetička sigurnost* – je sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru

2) *kibernetički prostor* – je virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na internet

3) *mrežni i informacijski sustav* – je (a) elektronička komunikacijska mreža kako je ona definirana zakonom kojim se uređuje područje elektroničkih komunikacija; (b) bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka ili (c) digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja

4) *sigurnost mrežnih i informacijskih sustava* – je sposobnost mrežnih i informacijskih sustava da, na određenoj razini pouzdanosti, odolijevaju bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost, pohranjenih, prenesenih ili obrađenih podataka, ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup

5) *nacionalna strategija kibernetičke sigurnosti* – je okvir kojim se pružaju strateški ciljevi i prioriteti za kibernetičku sigurnost na nacionalnoj razini

6) *nadležna tijela* – su nadležna sektorska tijela, jedinstvena nacionalna kontaktna točka, nadležni CSIRT-ovi i tehnička tijela za ocjenu sukladnosti

7) *operator ključnih usluga* – je bilo koji javni ili privatni subjekt koji ispunjava kriterije iz članka 6. ovog Zakona

8) *davatelj digitalnih usluga* – je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. ovog Zakona u Europskoj uniji

9) *javni subjekti* – su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave te pravne osobe koje imaju javne ovlasti ili obavljaju javnu službu

10) *privatni subjekti* – su fizičke i pravne osobe koje pružaju ili daju usluge

11) *sjedište* je stalno mjesto poslovanja gdje pružatelj odnosno davatelj usluga u neodređenom razdoblju upravlja svojom djelatnošću

12) *predstavnik* je bilo koja fizička ili pravna osoba sa sjedištem u Republici Hrvatskoj koju je davatelj digitalnih usluga koji nema sjedište u Europskoj uniji izričito imenovao da djeluje u njegovo ime i kojoj se nadležno sektorsko tijelo ili nadležni CSIRT mogu obratiti umjesto davatelju digitalnih usluga koji je obveznik primjene ovog Zakona

13) *incident* je bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava

14) *rješavanje incidenta* – su svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega

15) *rizik* je bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava

16) *središte za razmjenu internetskog prometa (IXP)* – je mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP pruža međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način

17) *sustav naziva domena (DNS)* – je hijerarhijsko raspoređeni sustav imenovanja na mreži koji odgovara na upite o nazivima domena

18) *pružatelj DNS usluge* – je javni ili privatni subjekt koji pruža DNS usluge na internetu

19) *registri naziva vršnih domena* – su javni ili privatni subjekti koji upravljaju i rukuju registracijom naziva internetskih domena za određenu vršnu domenu (TLD)

20) *internetsko tržište* – je digitalna usluga koja potrošačima i/ili trgovcima, kako su oni definirani zakonom kojim se uređuje alternativno rješavanje potrošačkih sporova, omogućuje da na internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište

21) *internetska tražilica* – je digitalna usluga koja korisniku omogućuje da pretražuje u načelu sve internetske stranice ili internetske stranice na određenom jeziku na temelju upita o bilo kojoj temi u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem

22) *usluga računalstva u oblaku* – je digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, usluga i aplikacija

23) *država članica* – je država članica Europske unije

24) *kvalificirani revizor* – je fizička ili pravna osoba koja je za obavljanje poslova revizije sigurnosti mrežnih i informacijskih sustava akreditirana pri odgovarajućoj organizaciji za normizaciju, koja je izdala ili daje na korištenje norme koje su u okviru provedbe zahtjeva iz ovog Zakona primijenjene kod određenog operatora ključnih usluga ili davatelja digitalnih usluga

25) *revizija sigurnosti mrežnih i informacijskih sustava* – su postupci koje obavlja kvalificirani revizor radi ocjene usklađenosti uspostavljenih procesa upravljanja mrežnim i informacijskim sustavom i dokumentiranih sigurnosnih politika sa zahtjevima iz ovog Zakona

26) *CSIRT* je kratica za *Computer Security Incident Response Team,* odnosno tijelo nadležno za prevenciju i zaštitu od incidenata, za koju se u Republici Hrvatskoj koristi i kratica CERT (Computer *Emergency Response Team).*

DIO DRUGI
OPERATORI KLJUČNIH USLUGA I DIGITALNE USLUGE

Određivanje operatora ključnih usluga

Članak 6.

Pojedini javni ili privatni subjekt (u daljnjem tekstu: subjekt) odredit će se operatorom ključnih usluga ako:

a) subjekt pruža neku od ključnih usluga s Popisa iz Priloga I. ovog Zakona (u daljnjem tekstu: ključna usluga)

b) pružanje ključne usluge kod tog subjekta ovisi o mrežnim i informacijskim sustavima i

c) incident bi imao znatan negativan učinak na pružanje ključne usluge.

Identifikacijski postupak

Članak 7.

(1) Nadležna sektorska tijela provode postupak identifikacije operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona, u kojem:

a) izrađuju popise svih subjekata koji pružaju ključnu uslugu

b) provode izdvajanje subjekta ovisno o važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge kod tog subjekta i

c) za sve izdvojene subjekte provode procjenu ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.

(2) Nadležno sektorsko tijelo dužno je postupak identifikacije operatora ključnih usluga provoditi redovito, sukladno tržišnim promjenama u sektoru, a najmanje jednom u dvije godine.

Određivanje važnosti negativnog učinka incidenta

Članak 8.

(1) Za određivanje važnosti negativnog učinka koji bi incident imao na pružanje ključne usluge uzimaju se u obzir sljedeći kriteriji:

– broj i vrsta korisnika kojima subjekt pruža uslugu

– postojanje ovisnosti drugih djelatnosti ili područja o pružanju usluge

– tržišni udio subjekta koji pruža uslugu

– zemljopisna raširenost subjekta u pružanju usluge

– mogući utjecaj incidenta, s obzirom na njegovu težinu i trajanje, na gospodarske i društvene aktivnosti te na javnu sigurnost

– važnosti poslovanja subjekta za održavanje dostatne razine ključne usluge, uzimajući u obzir i raspoloživost alternativnih sredstava za pružanje te usluge ili

– drugi sektorski kriteriji poput količine pružene usluge, udjela u pružanju usluge ili imovine subjekta.

(2) Kriteriji iz stavka 1. ovog članka i kriterijski pragovi, ako su definirani, primjenjuju se u postupku identifikacije operatora ključnih usluga, prema njihovom razvrstavanju po ključnim uslugama kako je to predviđeno Popisom iz Priloga I. ovog Zakona.

(3) Ako subjekt koji pruža ključnu uslugu ispunjava kriterije prema Popisu iz Priloga I. ovog Zakona te dostiže kriterijski prag, kada je on Popisom definiran, daje se ocjena važnosti negativnog učinka incidenta na pružanje ključne usluge za tog subjekta te se subjekt izdvaja za provođenje procjene ovisnosti pružanja ključne usluge o mrežnim i informacijskim sustavima.

Procjena ovisnosti o mrežnom i informacijskom sustavu

Članak 9.

(1) Ako se utvrdi da subjekt iz članka 8. stavka 3. ovog Zakona koristi mrežni i informacijski sustav za potporu pružanju ključne usluge te da prekid rada ili neispravno funkcioniranje tog sustava može dovesti do prekida u pružanju usluge ili na drugi način negativno utjecati na kvalitetu i/ili obujam usluge, nadležno sektorsko tijelo donosi odluku o određivanju tog subjekta operatorom ključnih usluga.

(2) Iznimno od stavka 1. ovog članka, nadležno sektorsko tijelo može donijeti odluku o određivanju subjekta operatorom ključne usluge neovisno o kriterijima s Popisa iz Priloga I. ovog Zakona, ako u postupku identifikacije utvrdi da subjekt pruža ključnu uslugu u dvije ili više država članica te da ovisnost o mrežnom i informacijskom sustavu subjekta u pružanju usluge može zbog toga imati negativan prekogranični učinak na kontinuitet u pružanju usluge.

(3) Nadležno sektorsko tijelo, radi utvrđivanja kritičnosti prekograničnog učinka iz stavka 2. ovog članka, u suradnji s jedinstvenom nacionalnom kontaktnom točkom provodi savjetovanja s nadležnim tijelom uključene države članice.

Obavijest o identifikaciji

Članak 10.

Nadležno sektorsko tijelo dostavlja identificiranom operatoru ključne usluge obavijest o odluci iz članka 9. ovog Zakona u roku od osam dana od dana njezina donošenja.

Dostava podataka za potrebe postupka identifikacije operatora ključne usluge

Članak 11.

(1) Svaki subjekt koji pruža neku od ključnih usluga dužan je nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti podatke koji su mu potrebni za provođenje postupka identifikacije operatora ključnih usluga.

(2) U zahtjevu iz stavka 1. ovog članka obvezno se navodi svrha zahtjeva, naznaka podataka koji su tijelu potrebni i rok za dostavu podataka.

(3) Subjekti kod kojih nastupe promjene u odnosu na podatke dostavljene sukladno stavku 2. ovog članka, dužni su nadležnom sektorskom tijelu dostaviti obavijest o tim promjenama ako bi one mogle utjecati na određivanje statusa subjekta u postupku identifikacije operatora ključne usluge.

(4) Obavijesti iz stavka 3. ovog članka dostavljaju se u roku od sedam dana od dana nastanka ili uvođenja promjene.

Popis operatora ključnih usluga

Članak 12.

(1) Na temelju odluka iz članka 9. ovog Zakona nadležna sektorska tijela izrađuju, preispituju i ažuriraju Popise operatora ključnih usluga po sektorima s Popisa iz Priloga I. ovog Zakona.

(2) Nadležna sektorska tijela obavješćuju jedinstvenu nacionalnu kontaktnu točku o broju identificiranih operatora ključnih usluga u pojedinom sektoru, s naznakom njihove važnosti za sektor.

Digitalne usluge

Članak 13.

Digitalne usluge na čije se davatelje odnosi ovaj Zakon utvrđene su Popisom iz Priloga II. ovog Zakona.

DIO TREĆI
MJERE ZA POSTIZANJE VISOKE RAZINE KIBERNETIČKE SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Obveza provedbe mjera

Članak 14.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su, radi osiguranja kontinuiteta u obavljanju tih usluga, poduzimati mjere za postizanje visoke razine kibernetičke sigurnosti svojih usluga.

(2) Mjere iz stavka 1. ovog članka sastoje se minimalno od:

– tehničkih i organizacijskih mjera za upravljanje rizicima, uzimajući pri tome u obzir najnovija tehnička dostignuća koja se koriste u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti i

– mjera za sprečavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.

Mjere za upravljanje rizikom operatora ključnih usluga

Članak 15.

Operatori ključnih usluga dužni su poduzimati tehničke i organizacijske mjere za upravljanje rizicima koje moraju obuhvatiti mjere za:

– utvrđivanje rizika od incidenata

– sprječavanje, otkrivanje i rješavanje incidenata i

– ublažavanje učinka incidenata na najmanju moguću mjeru.

Mjere za upravljanje rizikom davatelja digitalnih usluga

Članak 16.

Davatelji digitalnih usluga dužni su prilikom poduzimanja tehničkih i organizacijskih mjera za upravljanje rizicima voditi računa osobito o:

– sigurnosti sustava i objekata

– rješavanju incidenata

– upravljanju kontinuitetom poslovanja

– praćenju, reviziji i testiranju

– sukladnosti s međunarodnim standardima.

Opseg primjene mjera

Članak 17.