HRVATSKI SABOR

1305

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.

(1) Operatori ključnih usluga dužni su mjere za postizanje visoke razine kibernetičke sigurnosti provoditi u odnosu na mrežni i informacijski sustav, ili njegov dio, za koji je u postupku identifikacije operatora ključne usluge utvrđeno da o njemu ovisi pružanje ključne usluge kod dotičnog subjekta.

(2) Davatelji digitalnih usluga dužni su mjere za postizanje visoke razine kibernetičke sigurnosti provoditi u odnosu na mrežni i informacijski sustav koji kod njih podržava digitalnu uslugu.

Primjena mjera prema procjeni rizika

Članak 18.

Operatori ključnih usluga i davatelji digitalnih usluga primjenjuju mjere za sprečavanje i ublažavanje učinaka incidenata razmjerno riziku kojemu je izložen njihov mrežni ili informacijski sustav.

Odgovornost za primjenu mjera

Članak 19.

Operatori ključnih usluga i davatelji digitalnih usluga dužni su provoditi mjere za postizanje visoke razine kibernetičke sigurnosti bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to koriste vanjskog davatelja usluge.

Utvrđivanje mjera

Članak 20.

(1) Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuju uredbom koju donosi Vlada Republike Hrvatske (u daljnjem tekstu: Vlada).

(2) Mjere za postizanje visoke razine kibernetičke sigurnosti davatelja digitalnih usluga provode se sukladno Provedbenoj uredbi Komisije iz članka 2. stavka 2. ovog Zakona.

DIO ČETVRTI

OBAVJEŠĆIVANJE O INCIDENTIMA

Obveza obavješćivanja

Članak 21.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju.

(2) Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti nadležni CSIRT.

(3) Obveza obavješćivanja iz ovog članka odnosi se na incidente na mrežnim i informacijskim sustavima iz članka 17. ovog Zakona.

Kriteriji za određivanje učinka incidenata

Članak 22.

(1) Kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga propisuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.

(2) Kriteriji za određivanje incidenata koji imaju znatan učinak na davanje digitalnih usluga propisani su Provedbenom uredbom Komisije iz članka 2. stavka 2. ovog Zakona.

Obavijesti o incidentima

Članak 23.

Sadržaj obavijesti o incidentima iz članka 21. ovog Zakona, način dostave obavijesti i druga pitanja bitna za postupanje s takvim obavijestima uređuju se uredbom Vlade iz članka 20. stavka 1. ovog Zakona.

Informiranje javnosti o incidentu

Članak 24.

(1) Nadležni CSIRT može, po prethodno provedenom savjetovanju s operatorom ključne usluge i nadležnim sektorskim tijelom, obavijestiti javnost o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet usluge koju operator pruža, ako je osviještenost javnosti nužna za sprečavanje širenja i jačanja učinka incidenta ili za rješavanje incidenta koji je u tijeku.

(2) Nadležni CSIRT te, prema potrebi, CSIRT-ovi drugih pogođenih država članica, mogu javnost obavijestiti o pojedinačnim incidentima koji imaju znatan učinak na kontinuitet pojedine digitalne usluge ili zatražiti od davatelja digitalnih usluga da to učini, ako je objavljivanje informacije o incidentu u javnome interesu, osobito ako je to potrebno radi sprečavanja širenja i jačanja učinka incidenta ili rješavanja incidenta koji je u tijeku.

DIO PETI

NADLEŽNA TIJELA

Nadležna sektorska tijela

Članak 25.

(1) Nadležna sektorska tijela utvrđena su Popisom iz Priloga III. ovog Zakona.

(2) Nadležna sektorska tijela obavljaju sljedeće poslove:

– provode postupke identifikacije operatora ključnih usluga sukladno ovome Zakonu

– obavljaju nadzor operatora ključnih usluga i davatelja digitalnih usluga u provedbi mjera za postizanje visoke razine kibernetičke sigurnosti i ispunjavanju drugih obveza iz ovog Zakona

– međusobno surađuju i razmjenjuju iskustva u provedbi ovog Zakona

– surađuju i razmjenjuju relevantne informacije s drugim nadležnim tijelima iz ovog Zakona

– surađuju i razmjenjuju relevantne informacije s tijelom za zaštitu osobnih podataka, kada su osobni podaci ugroženi zbog incidenta na mrežnom i informacijskom sustavu operatora ključne usluge odnosno davatelja digitalne usluge, odnosno s pravosudnim tijelima, kada je takav incident rezultat kriminalnih aktivnosti.

Nadzor

Članak 26.

(1) Nadzor nad operatorom ključnih usluga provodi se jednom svake dvije godine.

(2) Nadzor nad operatorom ključnih usluga provest će se i prije isteka roka iz stavka 1. ovog članka ako nadležno sektorsko tijelo utvrdi ili zaprimi informacije koje ukazuju na to da operator ključne usluge ne izvršava svoje obveze iz ovog Zakona.

(3) Nadzor nad davateljem digitalnih usluga provodi se isključivo nakon što nadležno sektorsko tijelo zaprimi informacije koje ukazuju na to da davatelj digitalne usluge ne postupa sukladno Provedbenoj uredbi Komisije iz članka 2. stavka 2. ovog Zakona i/ili odredbama ovog Zakona.

(4) Nadležno sektorsko tijelo za davatelje digitalnih usluga provodi nadzor uz podršku nadležnog tehničkog tijela za ocjenu sukladnosti i nadležnog CSIRT-a.

Obveze operatora ključnih usluga i davatelja digitalnih usluga u okviru nadzora

Članak 27.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, dostaviti:

– podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava, uključujući dokumentirane sigurnosne politike, i

– dokaze o učinkovitoj provedbi sigurnosnih mjera.

(2) Učinkovita provedba sigurnosnih mjera dokazuje se ili rezultatima revizije sigurnosti mrežnih i informacijskih sustava koju je obavio kvalificirani revizor ili ocjenom sukladnosti mrežnih i informacijskih sustava koju daje tehničko tijelo za ocjenu sukladnosti.

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

(4) Operatori ključnih usluga i davatelji digitalnih usluga dužni su u okviru nadzora nadležnom sektorskom tijelu, na njegov zahtjev, omogućiti neposredan pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih usluga.

(5) Nadležno sektorsko tijelo nadzor davatelja digitalne usluge, koji ima sjedište ili svog predstavnika u Republici Hrvatskoj, a čiji se mrežni i informacijski sustavi nalaze u drugoj ili više država članica, može provoditi u suradnji s nadležnim tijelima tih država članica.

Predmet nadzora

Članak 28.

(1) U okviru nadzora nadležna sektorska tijela nadziru pravilnost provedbe propisanih:

– mjera za postizanje visoke razine kibernetičke sigurnosti

– obveza vezanih uz obavješćivanje o incidentima i

– drugih postupanja prema zahtjevima nadležnih tijela koja se podnose sukladno ovom Zakonu ili propisu donesenom na temelju ovog Zakona.

(2) U provedbi nadzora nadležna sektorska tijela:

– izdaju obvezujuću uputu operatoru ključnih usluga kada utvrde da on:

a) ne provodi mjere za postizanje visoke razine kibernetičke sigurnosti i/ili da ne izvršava druge obveze iz ovog Zakona ili

b) da postoje nedostaci u provedbi mjera odnosno izvršavanju obveza iz ovog Zakona

– izdaju naloge davatelju digitalnih usluga za otklanjanje svakog utvrđenog nepoštivanja provedbenog propisa Europske komisije iz članka 2. stavka 2. ovog Zakona i/ili odredbi ovog Zakona

– podnose optužne prijedloge.

(3) Nadležna sektorska tijela dužna su u aktima iz stavka 2. podstavka 1. i 2. ovog članka naznačiti rok za postupanje.

Obavljanje nadzora

Članak 29.

Nadzor obavljaju inspektori, nadzornici i supervizori, u skladu s nadležnostima koje proizlaze iz propisa o ustrojstvu i djelokrugu rada tih tijela te drugih propisa koji određuju njihovu nadležnost.

Jedinstvena nacionalna kontaktna točka

Članak 30.

Jedinstvena nacionalna kontaktna točka:

– dostavlja Europskoj komisiji podatke koji omogućavaju procjenu učinkovitosti provedbe mjera iz ovog Zakona i propisa donesenog na temelju ovog Zakona, sukladno zahtjevima utvrđenim propisom iz članka 2. ovog Zakona

– sudjeluje u radu Skupine za suradnju, koja je osnovana u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama te razvijanja povjerenja i sigurnosti na razini Europske unije u području kibernetičke sigurnosti,

– jednom godišnje podnosi Skupini za suradnju sažeto izvješće o zaprimljenim obavijestima o incidentima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 21. i člankom 32. stavkom 1. točkama 8., 10. i 11. ovog Zakona, osim za sektor poslovnih usluga za državna tijela

– na zahtjev nadležnog CSIRT-a, obavijesti o incidentima iz članka 21. ovog Zakona prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica, osim za sektor poslovnih usluga za državna tijela

– izrađuje smjernice o sadržaju obavijesti, načinu i rokovima informiranja jedinstvene nacionalne kontaktne točke o broju identificiranih operatora ključnih usluga i naznakama njihove važnosti te o obavijestima o incidentima

– vodi brigu o potrebi razvoja i usklađivanja nacionalne strategije kibernetičke sigurnosti s ciljevima ovog Zakona i zahtjevima Europske unije u području kibernetičke sigurnosti

– surađuje s drugim nadležnim tijelima iz ovog Zakona

– kada je to potrebno, savjetuje se i surađuje s tijelom za zaštitu osobnih podataka i pravosudnim tijelima.

Članak 31.

Jedinstvena nacionalna kontaktna točka je Ured Vijeća za nacionalnu sigurnost.

Zadaće nadležnog CSIRT-a

Članak 32.

(1) Nadležni CSIRT na sektorskoj razini, prema popisu nadležnosti iz Priloga III. ovog Zakona, obavlja sljedeće poslove:

– prati incidente

– pruža rana upozorenja i najave te informira o rizicima i incidentima

– provodi dinamičku analizu rizika i incidenata te izrađuje pregled situacije u sektoru

– provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključnih usluga odnosno davatelja digitalnih usluga

– prima obavijesti o incidentima

– na zahtjev operatora ključnih usluga odnosno davatelja digitalnih usluga analizira i odgovara na incidente

– ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu dostavlja operatoru ključnih usluga relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito informacije koje bi mogle pridonijeti djelotvornom rješavanju incidenta

– donosi smjernice za ujednačavanje i unapređenje stanja provedbe obveze obavješćivanja o incidentima iz članka 21. ovog Zakona

– informira nadležno sektorsko tijelo o incidentima iz članka 21. ovog Zakona

– u suradnji s nadležnim sektorskim tijelom, određuje prekogranične utjecaje incidenata iz članka 21. ovog Zakona

– informira jedinstvenu nacionalnu kontaktnu točku o incidentima iz članka 21. ovog Zakona, sukladno njezinim smjernicama

– dostavlja jedinstvenoj nacionalnoj kontaktnoj točki podatke o glavnim elementima postupaka rješavanja incidenata koje provodi

– obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu operatora ključnih usluga ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici

– obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu iz članka 21. ovog Zakona na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica

– surađuje s drugim CSIRT-ovima na nacionalnoj i međunarodnoj razini

– sudjeluje u Mreži CSIRT-ova na razini Europske unije koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje

– promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija.

(2) Operatori ključnih usluga i davatelji digitalnih usluga dužni su surađivati s nadležnim CSIRT-om i s njim razmjenjivati potrebne informacije u postupku rješavanja incidenata.

(3) Nadležni CSIRT u obavljanju svojih zadaća iz ovog Zakona ne može snositi odgovornost za štetu uzrokovanu incidentom na mrežnim i informacijskim sustavima operatora ključnih usluga i davatelja digitalnih usluga.

Osiguravanje uvjeta za obavljanje poslova nadležnog CSIRT-a

Članak 33.

Nadležni CSIRT je dužan:

– osigurati visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida, uz raspoloživost sredstava za mogućnost dvosmjernog kontaktiranja te jasno određenim i poznatim komunikacijskim kanalima za njihove klijente i suradnike

– svoje prostore i informacijske sustave za potporu smjestiti na sigurne lokacije i

– osigurati kontinuitet rada na način da:

a) je opremljen odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje

b) ima dovoljno zaposlenika kako bi se na odgovarajući način osigurala dostupnost u svako doba

c) se oslanja na infrastrukturu čiji je kontinuitet osiguran te su im u tu svrhu dostupni redundantni sustavi i rezervni radni prostor.

Tehničko tijelo za ocjenu sukladnosti

Članak 34.

(1) Tehničko tijelo za ocjenu sukladnosti provodi periodične provjere mjera iz članka 14. ovog Zakona poduzetih nad sigurnošću mrežnih i informacijskih sustava operatora ključnih usluga i davatelja digitalnih usluga, ako reviziju sigurnosti mrežnih i informacijskih sustava ne obavlja kvalificirani revizor.

(2) Tehnička tijela za ocjenu sukladnosti određena su Popisom s Priloga III. ovog Zakona.

Zahtjev za ocjenu sukladnosti

Članak 35.

(1) Tehničko tijelo za ocjenu sukladnosti provodi provjere iz članka 34. ovog Zakona na zahtjev nadležnog sektorskog tijela ili samog operatora ključnih usluga, odnosno davatelja digitalnih usluga.

(2) Nadležno sektorsko tijelo podnosi zahtjev iz stavka 1. ovog članka kada utvrdi da revizija sigurnosti mrežnih i informacijskih sustava kod pojedinog operatora ključne usluge odnosno davatelja digitalne usluge nije provedena ili da je nije proveo kvalificirani revizor.

(3) Operator ključne usluge, odnosno davatelj digitalnih usluga može podnijeti zahtjev za ocjenu sukladnosti kada ne postoji obveza revizije subjekta prema posebnom propisu.

Dostava podataka u postupku ocjene sukladnosti

Članak 36.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su tehničkom tijelu za ocjenu sukladnosti, na njegov zahtjev, dostaviti podatke potrebne za procjenu razine sigurnosti njihovih mrežnih i informacijskih sustava te im omogućiti pristup svojim objektima i sustavima koji im služe za potporu u obavljanju ključnih odnosno digitalnih 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.

Izvješće o ocjeni sukladnosti

Članak 37.

(1) Tehničko tijelo za ocjenu sukladnosti nakon provedene provjere iz članka 34. ovog Zakona izrađuje izvješće o provjeri mjera za postizanje visoke razine sigurnost mrežnih i informacijskih sustava koje sadrži:

– ocjenu sukladnosti, ako utvrdi da operator ključne usluge odnosno davatelj digitalne usluge učinkovito provodi mjere za postizanje visoke razine kibernetičke sigurnosti ili

– korektivne mjere za postizanje učinkovite provedbe mjera za postizanje visoke razine kibernetičke sigurnosti, s naznakom roka njihova izvršenja.

(2) Tehničko tijelo za ocjenu sukladnosti dostavlja izvješće iz stavka 1. ovog članka bez odgode nadležnom sektorskom tijelu i operatoru ključnih usluga, odnosno davatelju digitalnih usluga.

Završno izvješće o ocjeni sukladnosti

Članak 38.

(1) Operator ključnih usluga, kao i davatelj digitalnih usluga, dužan je, u zadanom roku, provesti korektivne mjere i o tome, bez odgađanja, obavijestiti tehničko tijelo za ocjenu sukladnosti.

(2) Tehničko tijelo za ocjenu sukladnosti će po primitku obavijesti iz stavka 1. ovog članka, kao i u slučaju neprovođenja ili nepotpunog provođenja korektivnih mjera, izraditi završno izvješće o provedenoj provjeri iz članka 34. ovog Zakona koje će dostaviti nadležnom sektorskom tijelu radi provođenja nadzora.

Obavijest o onemogućavanju ili otežavanju provedbe ocjene sukladnosti

Članak 39.

Ako operator ključnih usluga i davatelj digitalnih usluga odbije omogućiti ili neopravdano odgađa ili otežava provedbu povjere iz članka 34. ovog Zakona, tehničko tijelo za ocjenu sukladnosti će o tome bez odgode izvijestiti nadležno sektorsko tijelo.

DIO ŠESTI

ZAŠTITA PODATAKA

Članak 40.

(1) Popisi operatora ključnih usluga, kao i svi drugi podaci koji nastaju u okviru provedbe ovog Zakona koriste se isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona.

(2) Popis i podaci iz stavka 1. ovog članka predstavljaju informacije u odnosu na koje je moguće ograničiti pravo pristupa korisniku informacija, ovisno o rezultatima testa razmjernosti i javnog interesa koji se provodi prema odredbama posebnog zakona o pravu na pristup informacijama.

(3) Nadležna tijela dužna su pri razmjeni podataka iz stavka 1. ovog članka voditi računa o potrebi ograničavanja pristupa podacima kada je to potrebno u svrhu sprječavanja, otkrivanja, provođenja istraživanja i vođenja kaznenog postupka.

Članak 41.

Nadležna tijela iz ovog Zakona dužna su s podacima operatora ključnih usluga i davatelja digitalnih usluga postupati u skladu sa zahtjevima povjerljivosti, ako su oni utvrđeni posebnim propisima o zaštiti takvih podataka.

DIO SEDMI

PREKRŠAJNE ODREDBE

Članak 42.

(1) Novčanom kaznom u iznosu od 150.000,00 do 500.000,00 kuna kaznit će se za prekršaj pravna osoba – operator ključne usluge koji:

– ne postupi po obvezujućoj uputi nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 1. ovog Zakona

– odbije dostaviti ili neopravdano odgađa dostavljati obavijesti o incidentima iz članka 21. ovog Zakona.

(2) Novčanom kaznom u iznosu od 50.000,00 do 150.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 43.

(1) Novčanom kaznom u iznosu od 150.000,00 do 500.000,00 kuna kaznit će se za prekršaj pravna osoba – davatelj digitalne usluge koji:

– ne postupi po danom nalogu nadležnog sektorskog tijela iz članka 28. stavka 2. podstavka 2. ovog Zakona

– odbije dostaviti ili neopravdano odgađa dostavljati obavijesti o incidentima iz članka 21. ovog Zakona.

(2) Novčanom kaznom u iznosu od 50.000,00 do 150.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 44.

(1) Novčanom kaznom u iznosu od 50.000,00 do 100.000,00 kuna kaznit će se za prekršaj pravna osoba – operator ključne usluge i davatelj digitalne usluge koji:

– odbije postupiti ili neopravdano ne postupi po zahtjevu iz članka 27. ovog Zakona

– odbije omogućiti ili neopravdano odgađa ili otežava postupanje tehničkog tijela za ocjenu sukladnosti po zahtjevu iz članka 35. stavka 2. ovog Zakona.

(2) Novčanom kaznom u iznosu od 20.000,00 do 50.000,00 kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 10.000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

Članak 45.

(1) Novčanom kaznom u iznosu od 15.000,00 do 50.000,00 kuna kaznit će se za prekršaj pravna osoba – subjekt koji pruža neku od ključnih usluga koji:

– ne postupi po zahtjevu nadležnog sektorskog tijela za dostavu podataka iz članka 11. stavka 1. ovog Zakona

– ne dostavlja obavijesti o promjenama u roku iz članka 11. stavka 4. ovog Zakona.

(2) Novčanom kaznom u iznosu od 5000,00 do 25.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka fizička osoba obrtnik ili osoba koja obavlja drugu samostalnu djelatnost.

(3) Novčanom kaznom u iznosu od 2000,00 do 20.000,00 kuna kaznit će se za prekršaj iz stavka 1. ovog članka i odgovorna osoba u pravnoj osobi i odgovorna osoba u javnom subjektu.

DIO OSMI

PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 46.

Vlada će Uredbu iz članka 20. stavka 1. ovog Zakona donijeti u roku od 30 dana od dana stupanja na snagu ovog Zakona.

Članak 47.

(1) Nadležna sektorska tijela dužna su postupak identifikacije operatora ključnih usluga provesti u roku od 90 dana od dana stupanja na snagu ovog Zakona.

(2) Nadležna sektorska tijela dužna su jedinstvenoj nacionalnoj kontaktnoj točki dostaviti obavijesti iz članka 12. stavka 2. ovog Zakona u roku od 120 dana od dana stupanja na snagu ovog Zakona.

Članak 48.

(1) Operatori ključnih usluga dužni su provesti mjere za osiguravanje visoke razine kibernetičke sigurnosti u roku od godine dana od dana dostave obavijesti iz članka 10. ovog Zakona.

(2) Operatori ključnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona u roku od 30 dana od dana dostave obavijesti iz članka 10. ovog Zakona.

Članak 49.

(1) Davatelji digitalnih usluga dužni su se uskladiti sa zahtjevima Provedbene uredbe Komisije iz članka 2. stavka 2. ovog Zakona u roku propisanom tom Uredbom.

(2) Davatelji digitalnih usluga dužni su započeti s dostavom obavijesti iz članka 21. ovog Zakona u roku od 120 dana od dana stupanja na snagu ovog Zakona.

Članak 50.

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

Klasa: 022-03/18-01/48

Zagreb, 6. srpnja 2018.

HRVATSKI SABOR

Predsjednik
Hrvatskoga sabora

Gordan Jandroković, v. r.

PRILOG I.

POPIS KLJUČNIH USLUGA S KRITERIJIMA I PRAGOVIMA ZA UTVRĐIVANJE VAŽNOSTI NEGATIVNOG UČINKA INCIDENTA

Sektor	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Energetika	Električna energija	Proizvodnja električne energije	Instalirana snaga proizvodnog postrojenja	300 MW
		Prijenos električne energije	Bez iznimke	–
		Distribucija električne energije	Prekid napajanja	Više od 100.000 obračunskih mjernih mjesta
			Ovisnosti drugih djelatnosti ili područja o pružanju usluge	Distribucija za: ☐ bolnice ☐ zračne luke i kontrole leta ☐ objekte banaka s podatkovnim centrima ☐ policijske uprave ☐ vojne lokacije ☐ aktivna vodocrpilišta i centre upravljanja ☐ objekte operatora telekomunikacijskog sustava ☐ objekte tijela sigurnosno-

				-obavještajnog sustava, ☐ objekte profesionalnih vatrogasnih postrojbi, ☐ objekte Državne uprave za zaštitu i spašavanje (Služba 112) ili ☐ objekte određene nacionalnom kritičnom infrastrukturom
	Nafta	Transport nafte naftovodima	Bez iznimke	–
		Proizvodnja nafte	Proizvedeno nafte pojedinog naftnog polja u tonama godišnje	50.000 t/god
		Proizvodnja naftnih derivata	Proizvedeno naftnih derivata pojedine rafinerije u tonama godišnje	Motorni benzini: 200.000 t/god Dizelsko gorivo: 200.000 t/god Plinska ulja: 100.000 t/god
		Skladištenje nafte i naftnih derivata	Ukupni skladišni kapacitet nafte pojedinog terminala u m3	1.000.000 m3
			Ukupni skladišni kapacitet naftnih derivata pojedinog skladišta (na istoj lokaciji) u m3	60.000 m3

	Plin	Distribucija plina	Broj krajnjih kupaca priključen na distribucijski sustav	Više od 100.000 obračunskih mjernih mjesta.
		Transport plina	Bez iznimke	
		Skladištenje plina	Potrošnja plina u RH, u kWh	25 % potrošnje plina u RH u prethodnoj godini
		Prihvat i otprema UPP – a	Kapacitet uplinjavanja UPP u m3/h	Više od 500.000 m3/h
		Proizvodnja prirodnog plina	Godišnja proizvodnja plina predana u transportni sustav na pojedinom ulazu, u kWh	1.000.000 kWh
Prijevoz	Zračni promet	Zračni prijevoz putnika i tereta	Udio putnika pojedinog zračnog prijevoznika na bilo kojem nacionalnom aerodromu koji ima promet putnika veći od 2.000.000 godišnje (ključni aerodrom)	Zračni prijevoznik koji ima udio veći od 30 % na ključnom aerodromu
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Ukupni godišnji promet putnika pojedine zračne luke	Više od 2.000.000 putnika
		Kontrola zračnog prometa	Otvorenost područja letnih informacija Zagreb (FIR Zagreb) – bez iznimke	–
			Broj operacija na godišnjem nivou	Ukupno 500.000 operacija za FIR Zagreb

	Željeznički promet	Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom	Upravitelj željezničke infrastrukture za javni prijevoz – bez iznimke	
		Usluge prijevoza robe i/ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima	Broj voznih jedinica (vlakova)	20 dnevno
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom	Broj voznih jedinica (vlakova)	20 dnevno
	Vodni prijevoz	Nadzor kretanja brodova (VTS usluga)	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000
			Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000
		Obavljanje poslova pomorske radijske službe	Godišnji broj dolazaka brodova iz međunarodne plovidbe	najmanje 4.000

			Godišnji broj putovanja brodova u domaćem prometu, uključujući obalni linijski promet	najmanje 200.000
		Održavanje objekata sigurnosti plovidbe	Bez iznimke	–
		Prijevoz putnika u međunarodnom i/ili domaćem prometu	Broj putnika godišnje	1.000.000
	Vodni prijevoz	Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu	Količina tereta godišnje u tonama	2.500.000
		Prijevoz putnika, tereta i vozila u unutarnjim morskim vodama i teritorijalnom moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljenim uvjetima reda plovidbe i cjenikom usluga	Broj korisnika	15 % ukupno prevezenih putnika i/ili vozila godišnje
			Tržišni udio	Minimalno 15 % tržišnog udjela
		Praćenje i lociranje plovila u unutarnjoj plovidbi	Broj plovila na unutarnjim plovnim putovima u Republici Hrvatskoj tijekom godine	100

		Obavijesti brodarstvu u unutarnjoj plovidbi	Broj izdanih obavijesti brodarstvu tijekom godine	100
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi	Pokrivenost unutarnjih vodnih putova u Republici Hrvatskoj	Pokrivenost 500 riječnih km
		Baza podataka o trupu plovila u unutarnjoj plovidbi	Broj plovila unesenih u bazu podataka tijekom godine	50
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi	Broj ERI poruka upućenih prema RIS centrima dnevno	50
	Cestovni prijevoz	Javni prijevoz putnika	Broj voznih jedinica	100
			Broj putnika godišnje	5.000.000
		Korištenje cestovne infrastrukture	Upravitelj ceste na TEN – T mreži – bez iznimke	–
			Broj vozila na glavnoj cesti koja vodi do središta naseljenog mjesta većeg od 35.000 stanovnika	20.000 PGDP (prosječni godišnji dnevni promet)
			Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika
		Upravljanje prometnim	Uspostavljen centar za kontrolu i upravljanje	

		tokovima ili informiranje vozača (ITS)	prometom 24/7 – bez iznimke	
			Uspostavljen centar za informiranje vozača o stanju u prometu 24/7 – bez iznimke	
			Broj prometnih svjetala (semafora) u sustavu	100
			Zemljopisna raširenost korištenja usluga	Teritorij cijele države ili grada većeg od 35.000 stanovnika
Bankarstvo		Platne usluge	Globalno sistemski važne kreditne institucije i ostale sistemski važne kreditne institucije	–
Infrastrukture financijskog tržišta		Usluge mjesta trgovanja	Bez iznimke	–
		Usluge središnjih drugih ugovornih strana (CCP)	Bez iznimke	–
Zdravstveni sektor		Primarna zdravstvena zaštita	Centralni zdravstveni informacijski sustav Hrvatske – bez iznimke	–
			Pokrivenost pružatelja primarne zdravstvene zaštite odobrenim programskim rješenjem	40 %
			Broj intervencija u izvanbolničkoj djelatnosti hitne medicine po županijama godišnje	70.000

			Broj zdravstvenih djelatnika zaposlenih u domu zdravlja	500
		Sekundarna zdravstvena zaštita	Zdravstvena VPN mreža HealthNet – bez iznimke	–
			Pokrivenost pružatelja sekundarne zdravstvene zaštite odobrenim programskim rješenjem	40 %
			Broj obavljenih zdravstvenih postupaka, pregleda ili pretraga godišnje	1.000.000
			Broj zdravstvenih djelatnika zaposlenih u općoj bolnici	800
		Tercijarna zdravstvena zaštita	Broj postelja u stacionarnim djelatnostima kliničkog bolničkog centra	900
			Broj postelja u stacionarnim djelatnostima kliničke bolnice	300
			Broj postelja u stacionarnim djelatnostima klinike	80
		Transfuzijska medicina i transplantacija organa	Broj prikupljenih doza pune krvi godišnje	100.000
			Broj donora organa na milijun stanovnika godišnje	30

			Broj transplantacijskih zahvata na milijun stanovnika godišnje	80
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita	Broj osiguranih osoba u obveznom zdravstvenom osiguranju (OZO)	4.000.000
			Broj osiguranih osoba u dopunskom zdravstvenom osiguranju (DZO)	2.000.000
			Broj upita za provjerom statusa obveznog i dopunskog zdravstvenog osiguranja dnevno	100.000
			Broj izdanih Europskih kartica zdravstvenog osiguranja (EKZO) godišnje	100.000
		Sigurnost hrane	Središnji informacijski sustav sanitarne inspekcije – bez iznimke	
		Zaštita od opasnih kemikalija	Broj sigurnosno – tehničkih listova pregledanih i uvrštenih u registar sigurnosno – tehničkih listova (STL) godišnje	9.000
			Broj opasnih kemikalija prikupljenih i uvrštenih u registar opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH godišnje	3.500

		Distribucija i sigurnost lijekova i medicinskih proizvoda	Broj lijekova (uključujući cjepiva) stavljenih u promet u RH	3.000
			Broj medicinskih proizvoda (različitih klasa rizika) stavljenih u promet u RH	250.000
			Broj stanovnika / osiguranih osoba na broj distribucijskih centara	330.000
		Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara	Nacionalni javnozdravstveni informacijski sustav – bez iznimke	–
Opskrba vodom za piće i njezina distribucija		Opskrba krajnjih korisnika	Količina isporučene vode	10.000.000 m^3/godišnje
Digitalna infrastruktura		DNS usluga za .hr TLD	Bez iznimke	–
		Registar naziva domena za .hr TLD	Bez iznimke	–
		Sustav za registriranje i administriranje sekundarne domene	Subjekt koji pruža ključnu uslugu, ima registriranu domenu preko registara i prepoznao je ovisnost svoje usluge o DNS sustavu.	–

			Broj registriranih domena	20 % od ukupnog broja registriranih domena (unutar .hr i com.hr)
		Usluga IXP	Broj spojenih članica	Veći od 15
Poslovne usluge za državna tijela		Usluge u sustavu e – Građani	Broj korisnika pojedine usluge	100.000
			Dostupnost usluge isključivo putem elektroničke usluge	Utvrđeno da ne postoji alternativni način korištenja usluge
		Poslovne usluge za korisnike državnog proračuna	Broj institucija koje nisu sektorski povezane	10

PRILOG II.

POPIS DIGITALNIH USLUGA

1. Internetsko tržište
2. Internetska tražilica
3. Usluge računalstva u oblaku

PRILOG III.

POPIS NADLEŽNIH TIJELA

Jedinstvena nacionalna kontaktna točka – Ured Vijeća za nacionalnu sigurnost

Sektor ključnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti
Energetika	tijelo državne uprave nadležno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	tijelo državne uprave nadležno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	–
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	–
Zdravstveni sektor	tijelo državne uprave nadležno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	tijelo državne uprave nadležno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNET
Poslovne usluge za državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

Davatelji digitalnih usluga	Nadležno sektorsko tijelo	CSIRT	Tehničko tijelo za ocjenu sukladnosti

	tijelo državne uprave nadležno za gospodarstvo	Nacionalni CERT	Zavod za sigurnost informacijskih sustava

*Napomena: Nadležni CSIRT za sektor Poslovne usluge za državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu tijela državne uprave nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (Srce) ili CARNETA, za koje je nadležni CSIRT Nacionalni CERT.

**Napomena: Tehničko tijelo za ocjenu sukladnosti za sektor Poslovne usluge za državna tijela za sve usluge je Zavod za sigurnost informacijskih sustava, osim za područje koje je u djelokrugu središnjeg državnog tijela nadležnog za znanost i obrazovanje, Sveučilišnog računskog centra (Srce) ili Hrvatske akademske i istraživačke mreže – CARNETA, za koje je tehničko tijelo za ocjenu sukladnosti Hrvatska akademska i istraživačka mreža – CARNET.