NN 68/2018 (27.7.2018.), Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

VLADA REPUBLIKE HRVATSKE

1399

Na temelju članka 30. stavka 2. Zakona o Vladi Republike Hrvatske (»Narodne novine«, br. 150/11, 119/14 i 93/16) i članka 20. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (»Narodne novine«, broj 64/18), Vlada Republike Hrvatske je na sjednici održanoj 26. srpnja 2018. godine donijela

UREDBU

O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

DIO PRVI
OPĆE ODREDBE

Predmet uredbe

Članak 1.

Ovom se Uredbom utvrđuju mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga, način njihove provedbe, kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti i druga bitna pitanja za obavješćivanje o incidentima.

Usklađenost s propisima Europske unije

Članak 2.

(1) Ovom Uredbom 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) Ovom se Uredbom 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).

Pojmovi

Članak 3.

U smislu ove Uredbe pojedini pojmovi imaju sljedeće značenje:

1) »Zakon« – je Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

2) »operator ključnih usluga« – je operator koji je odlukom iz članka 9. Zakona određen operatorom ključne usluge

3) »davatelj digitalnih usluga« – je bilo koji privatni subjekt koji pruža neku digitalnu uslugu s Popisa iz Priloga II. Zakona u Europskoj uniji i koji na teritoriju Republike Hrvatske ima sjedište ili svog predstavnika, pod uvjetom da takav davatelj ne predstavlja mikro ili mali subjekt malog gospodarstva kako su oni definirani zakonom kojim se uređuju osnove za primjenu poticajnih mjera gospodarske politike usmjerenih razvoju, restrukturiranju i tržišnom prilagođavanju malog gospodarstva

4) »incident« – bilo koji događaj koji ima stvaran, negativan učinak na sigurnost mrežnih i informacijskih sustava iz članka 17. Zakona

5) »kontinuitet pružanja usluga« – je sposobnost pružanja usluge bez prekida ili ponovnog uspostavljanja pružanja usluge nakon incidenta na unaprijed utvrđenoj i prihvatljivoj razini

6) »korisnik usluge« – svaka fizička i pravna osoba kojoj se usluga pruža temeljem zakona ili pravnog posla

7) »korisnik sustava« – svaka fizička osoba koja ima otvoren račun na ključnom sustavu

8) »odgovorna osoba« – čelnik, član uprave, direktor ili izvršni rukovoditelj najviše razine

9) »nadležni CSIRT« – je CSIRT nadležan na sektorskoj razini prema popisu nadležnosti iz Priloga III. Zakona

10) »nadležno sektorsko tijelo« – je nadležno sektorsko tijelo prema popisu nadležnosti iz Priloga III. Zakona

11) »jedinstvena nacionalna kontaktna točka« – Ured Vijeća za nacionalnu sigurnost.

DIO DRUGI
MJERE ZA POSTIZANJE VISOKE RAZINE KIBERNETIČKE SIGURNOSTI OPERATORA KLJUČNIH USLUGA

POGLAVLJE I.
UPRAVLJANJE SIGURNOŠĆU MREŽNIH I INFORMACIJSKIH SUSTAVA

Okvir upravljanja

Članak 4.

Operatori ključnih usluga dužni su uspostaviti sustav upravljanja sigurnošću mrežnih i informacijskih sustava iz članka 17. Zakona (u daljnjem tekstu: ključni sustavi).

Načela sigurnosti

Članak 5.

Funkcionalnost i sigurnost ključnih sustava temelji se na sljedećim načelima:

– povjerljivosti: svojstvu da usluge ili podaci ne budu dostupne ili otkrivene neovlaštenim osobama

– integritetu: svojstvu da usluge ili podaci nisu neovlašteno ili nepredviđeno mijenjani

– raspoloživosti: svojstvu koje omogućuje pristup ili upotrebljivost usluge ili podataka na zahtjev ovlaštenog korisnika

– autentičnosti: svojstvu koje osigurava da je identitet korisnika zaista onaj za koji se tvrdi da jest.

Uspostava i dokumentiranje politike upravljanja

Članak 6.

(1) Operatori ključnih usluga dužni su uspostaviti i dokumentirati politiku upravljanja sigurnošću ključnih sustava.

(2) Politika upravljanja sigurnošću ključnih sustava mora:

– definirati ciljeve i strateške smjernice očuvanja kontinuiteta poslovanja

– biti temeljena na procjeni i upravljanju rizicima

– opisati sustav upravljanja sigurnošću, uključujući interne nadzore provedbe mjera kibernetičke sigurnosti

– utvrditi donošenje potrebnih sigurnosno-operativnih procedura za ključne sustave, s poveznicama na druge interne akte koji reguliraju postojeće sigurnosno-operativne procedure, neovisno o tome odnose li se na ključne sustave ili sigurnost operatora u cjelini

– uključivati organizaciju i provedbu programa edukacije te stalnog podizanja svijesti o sigurnosti.

(3) Politika upravljanja sigurnošću ključnih sustava donosi se u pisanom obliku i mora ju odobriti najviša upravljačka razina.

Organizacijska struktura

Članak 7.

(1) Operatori ključnih usluga dužni su odrediti osobu s najvišim rukovodnim ovlastima odgovornu za uspostavu i upravljanje sigurnošću ključnih sustava.

(2) Operatori ključnih usluga dužni su uspostaviti organizacijsku strukturu, s formalnom raspodjelom zadaća, ovlasti i odgovornosti kojom će se osigurati primjereno upravljanje sigurnošću ključnih sustava.

Provedba internih nadzora

Članak 8.

(1) Operatori ključnih usluga dužni su uspostaviti sustav internog nadzora provedbe mjera kibernetičke sigurnosti određenih politikom upravljanja sigurnošću ključnih sustava, pri čemu bi poslovi internog nadzora moraju biti organizacijski odvojeni od organizacijske strukture odgovorne za ključne sustave.

(2) Interni nadzor iz stavka 1. ovoga članka provodi se najmanje jednom godišnje.

(3) Rezultati internog nadzora iz stavka 1. ovoga članka dostavljaju se, u pisanom obliku, odgovornoj osobi iz članka 7. stavka 1. ove Uredbe.

(4) Odgovorna osoba iz članka 7. stavka 1. ove Uredbe dužna je osigurati provedbu mjera kibernetičke sigurnosti u skladu s rezultatima internog nadzora iz stavka 1. ovoga članka.

POGLAVLJE II.
UPRAVLJANJE RIZICIMA

Uspostava sustava upravljanja rizicima

Članak 9.

(1) Operatori ključnih usluga dužni su uspostaviti sustav upravljanja rizicima kojima je izložen ključni sustav.

(2) Sustav upravljanja rizicima iz stavka 1. ovoga članka mora uključivati:

– metodologiju utvrđivanja rizika od incidenata

– određivanje odgovornih osoba za provođenje redovite procjene rizika od incidenata

– izradu ili odabir kataloga primjenjivih rizika i njegovo ažuriranje

– prihvaćeni način obrade rizika (izbjegavanje, ublažavanje, prijenos ili prihvaćanje rizika)

– popis preostalih rizika

– postupak donošenja formalne odluke o prihvaćanju preostalih rizika od strane najviše upravljačke razine.

Procjena rizika

Članak 10.

(1) Operatori ključnih usluga primjenjuju mjere za sprečavanje i ublažavanje učinaka incidenata razmjerno procjeni rizika kojemu je izložen njihov ključni sustav.

(2) Operatori ključnih usluga dužni su provoditi aktivnosti vezane za izgradnju, nadogradnju i održavanje ključnih sustava uvažavajući rezultate procjene rizika kojemu je izložen njihov ključni sustav.

Članak 11.

(1) Operatori ključnih usluga dužni su kontinuirano ažurirati katalog rizika, uzimajući u obzir unutarnje i vanjske prijetnje koje se pojavljuju, novootkrivene ranjivosti, gubitak djelotvornosti postojećih mjera za sprečavanje i ublažavanje učinaka incidenata, promjene rizika uslijed promjene arhitekture informacijskih sustava, sve promjene koje utječu na sigurnost ključnih sustava, kao i rezultate prethodnih procjena rizika.

(2) Operatori ključnih usluga dužni su najmanje jednom godišnje provoditi procjenu rizika kojemu je izložen njihov ključni sustav i donositi odluku o prihvaćanju preostalih rizika.

Identifikacija opreme, osoba i aktivnosti u okviru kojih se provodi procjena rizika

Članak 12.

(1) Operatori ključnih usluga dužni su identificirati:

– opremu od koje se sastoje ključni sustavi

– osobe koje imaju pravo pristupa ključnim sustavima i

– poslovne aktivnosti koje se obavljaju na ključnim sustavima ili su u potpori ključnih sustava.

(2) Operatori ključnih usluga dužni su procjenom rizika obuhvatiti sve identificirane elemente iz stavka 1. ovoga članka.

Sprječavanje, otkrivanje i rješavanje incidenata te ublažavanje učinka incidenata

Članak 13.

(1) Procjena rizika provodi se za identificiranu opremu, osobe i aktivnosti iz članka 12. ove Uredbe.

(2) Procjena rizika provodi se na temelju prihvaćenog kataloga rizika s obavezom procjene rizika najmanje za definirana područja zaštite ključnih sustava u poglavlju III. ove Uredbe.

(3) Procijenjeni rizici obrađuju se izbjegavanjem, ublažavanjem, prijenosom ili prihvaćanjem rizika.

(4) Za procijenjene sigurnosne rizike obrada se provodi izborom različitih sigurnosnih mjera i kontrola iz odgovarajuće međunarodne norme informacijske sigurnosti.

(5) Sigurnosne mjere i kontrole iz odgovarajuće međunarodne norme informacijske sigurnosti moraju omogućavati: odvraćanje, izbjegavanje, prevenciju, detekciju, reakciju i oporavak, djelujući na odgovarajući način na prijetnje i ranjivosti ključnih sustava, odnosno na utjecaje incidenata na ključne sustave.

Dokumentacija o procjeni rizika

Članak 14.

Operatori ključnih usluga dužni su dokumentaciju nastalu provedbom procjene rizika kojemu je izložen njihov ključni sustav štititi na način koji osigurava pristup isključivo ovlaštenim osobama.

POGLAVLJE III.
PODRUČJA ZAŠTITE KLJUČNIH SUSTAVA

Fizička sigurnost i sigurnost okruženja

Članak 15.

Operatori ključnih usluga dužni su osigurati provedbu mjera koje se odnose na fizičku sigurnost i sigurnost okruženja ključnih sustava od štete uzrokovane kvarom sustava, ljudskim pogreškama, zlonamjernim djelovanjem ili djelovanjem prirodnih fenomena.

Sigurnost opskrbe

Članak 16.

(1) Operatori ključnih usluga dužni su osigurati dostupnost opreme, materijala, energenata i drugih resursa nužnih za redovno i kontinuirano funkcioniranje i održavanje ključnih sustava.

(2) Opskrbni lanac resursa iz stavka 1. ovoga članka mora uključivati procjenu sigurnosti svih odabranih izvođača i podizvođača, kao i praćenje izvora nabavljenih resursa.

Upravljanje ugovornim odnosima

Članak 17.

(1) Operatori ključnih usluga dužni su redovito procjenjivati i na prihvatljivu razinu svesti rizike koji proizlaze iz ugovornih odnosa s pravnim i fizičkim osobama čije izvršenje može utjecati na ključne sustave.

(2) Operatori ključnih usluga dužni su kontinuirano nadzirati način i kvalitetu pružanja ugovorenih poslova i usluga koje mogu utjecati na ključne sustave.

(3) Operatori ključnih usluga dužni su provesti postupak procjene rizika prije ostvarivanja ugovornog odnosa s pravnim i fizičkim osobama čije aktivnosti mogu utjecati na ključne sustave.

Upravljanje eksternalizacijom

Članak 18.

(1) Operatori ključnih usluga koji za upravljanje i/ili održavanje ključnih sustava koriste vanjskog davatelja usluge, dužni su redovito procjenjivati i na prihvatljivu razinu svesti rizike koji se mogu u okviru eksternalizacije usluge pojaviti.

(2) Operatori ključnih usluga odgovorni su da pružatelj usluga iz stavka 1. ovoga članka u potpunosti primjenjuje mjere zaštite ključnih sustava propisane ovom Uredbom.

(3) Operatori ključnih usluga dužni su provesti postupak procjene rizika eksternalizacije usluge prije sklapanja ugovora o pružanju usluge.

(4) Ugovori iz stavka 3. ovoga članka moraju sadržavati klauzulu o obvezi omogućavanja nesmetanog nadzora nadležnog sektorskog tijela.

(5) Ugovori iz stavka 3. ovoga članka moraju sadržavati klauzulu o obvezi pružanja usluge i nakon raskida ugovora u razumnom roku koji omogućuje operatoru ključne usluge sklapanje ugovora s drugim vanjskim davateljem usluge ili organizaciju samostalnog izvršavanja usluge od strane operatora ključne usluge.

Kontrola pristupa prostorima

Članak 19.

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera kojima se osigurava ovlašten i ograničen fizički i logički pristup prostorima u kojima se nalaze ključni sustavi, utemeljen na poslovnim i/ili sigurnosnim zahtjevima.

(2) Operatori ključnih usluga dužni su utvrditi i trajno ažurirati postupke kontrole pristupa prostorima iz stavka 1. ovoga članka, kojima moraju minimalno obuhvatiti:

– definiranje popisa osoba s pravom pristupa

– postupke ulaska osoba bez trajnog prava pristupa

– nadzor kontrole pristupa.

Fizičko i logičko razdvajanje ključnih sustava

Članak 20.

(1) Operatori ključnih usluga dužni su provesti fizičko i/ili logičko odvajanje ključnih sustava od svih ostalih mrežnih i informacijskih infrastruktura.

(2) Ako fizičko i/ili logičko odvajanje ključnih sustava nije moguće, operatori ključnih usluga dužni su skladu s procjenom rizika:

– provesti mjere koje umanjuju preostali rizik nastao zbog nemogućnosti potpunog odvajanja

– dokumentirati i prihvatiti preostale rizike

– dokumentirati sve točke ključnog sustava u kojima odvajanje nije moguće.

Kontrola pristupa ključnom sustavu

Članak 21.

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera kojima se osigurava ovlašten i ograničen fizički i logički pristup ključnim sustavima, utemeljen na poslovnim i/ili sigurnosnim zahtjevima.

(2) Operatori ključnih usluga dužni su utvrditi i trajno ažurirati postupke kontrole pristupa ključnim sustavima, kojima moraju minimalno obuhvatiti:

– postupke i sustave kontrole pristupa koji uključuju korištenje jedinstvenih identifikatora osoba i osiguravaju postupke autentifikacije

– mehanizme kontrole pristupa ključnim sustavima, koji moraju osigurati da istome pristupaju isključivo korisnici koji na to imaju pravo, a u skladu s poslovnim i/ili sigurnosnim zahtjevima

– sustav upravljanja korisničkim pravima pristupa, koji mora uključivati identifikacije, autentifikacije, autorizacije, evidentiranja, kao i stalni nadzor korisničkih prava pristupa

– sustav kontinuiranog praćenja pristupa ključnim sustavima koji minimalno mora omogućiti odobravanje i nadzor prava pristupa, praćenje i izvješćivanje u slučaju pokušaja neovlaštenog pristupa

– administratorski pristup ključnim sustavima koji se provodi u skladu s pravilima koja jamče korištenje sklopovske i programske opreme i mrežnog okruženja namijenjenog isključivo administratorskom pristupu

– redovitu procjenu učinkovitosti postupaka i pravila kontrole pristupa i po potrebi njihovo unaprjeđivanje

– redovitu reviziju dodijeljenih prava pristupa i njihovo oduzimanje u slučaju prestanka potrebe za istim.

Dnevnik aktivnosti ključnih sustava

Članak 22.

(1) Operatori ključnih usluga dužni su koristiti sustav za nadzor i bilježenje korisničkih aktivnosti na ključnom sustavu.

(2) Vrste zapisa koje se bilježe moraju minimalno obuhvaćati prijave i odjave korisnika sustava, otvaranje i zatvaranje korisničkih računa, promjene prava korisnika, promjene sigurnosnih prava na sustavu i podatke o funkcioniranju sustava koji pokrivaju odgovarajuće poslužitelje.

(3) Svaki zabilježeni zapis sustava za nadzor i bilježenje korisničkih aktivnosti mora minimalno sadržavati:

– identitet korisnika sustava

– vrstu zapisa

– vrijeme zapisa

– logičku lokaciju ključnog sustava na koju se zapis odnosi.

(4) Sustav za nadzor i bilježenje korisničkih aktivnosti mora:

– omogućavati prikupljanje podataka o korisničkim aktivnostima sa svih dijelova ključnog sustava

– biti odvojen od sustava s kojih prikuplja podatke i

– uspostavljen na način da se maksimalno umanji mogućnost neovlaštene izmjene zapisa korisničkih aktivnosti.

(5) Operatori ključnih usluga dužni su osigurati kontinuirano praćenje aktivnosti i provođenje postupka analize zapisa u slučaju incidenta.

(6) Zapisi u sustavu za nadzor i bilježenje korisničkih aktivnosti čuvaju se najmanje posljednjih 6 mjeseci.

Zaštita podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu

Članak 23.

(1) Operatori ključnih usluga dužni su osigurati provedbu mjera zaštite podataka koji se obrađuju, pohranjuju i prenose u ključnom sustavu u svrhu zaštite povjerljivosti, raspoloživosti i cjelovitosti podataka.

(2) Operatori ključnih usluga dužni su utvrditi osjetljive podatke nad kojima je potrebno primijeniti kriptografske mehanizme zaštite tijekom njihove obrade, pohrane i prenošenja u ključnom sustavu u svrhu zaštite povjerljivosti i cjelovitosti podataka.

(3) Operatori ključnih usluga dužni su mjere iz stavaka 1. i 2. odgovarajuće primjenjivati i na prijenosne medije koji se koriste za obradu, pohranu ili pomoću kojih se prenose podaci u ključnom sustavu.

Zaštita od zlonamjernog programskog koda

Članak 24.

(1) Operator je dužan zaštiti ključni sustav od zlonamjernog programskog koda primjenom odgovarajućih sigurnosnih mjera i kontrola.

(2) Sigurnosne mjere i kontrole iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje zlonamjernog programskog koda unutar ključnog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnog sustava i održavanje kontinuiteta pružanja ključne usluge.

Zaštita od narušavanja raspoloživosti ključnog sustava

Članak 25.

(1) Operator je dužan zaštititi ključni sustav od računalnih napada koji mogu narušiti njegovu raspoloživost primjenom odgovarajućih sigurnosnih mjera i kontrola.

(2) Sigurnosne mjere i kontrole iz stavka 1. ovoga članka moraju osigurati prepoznavanje i onemogućavanje računalnih napada koji mogu narušiti raspoloživost ključnog sustava te zapisivanje i pohranu informacija nužnih za prepoznavanje narušavanja funkcionalnosti ključnog sustava i održavanje kontinuiteta pružanja ključne usluge.

Razvoj i održavanje ključnih sustava

Članak 26.

(1) Operatori ključnih usluga dužni su definirati načine, kriterije i postupke razvoja ključnih sustava, s posebnim naglaskom na važnost razmatranja sigurnosnih aspekata od početne faze projekta, a u skladu s donesenom metodologijom upravljanja projektima.

(2) Operatori ključnih usluga dužni su, u sklopu procesa razvoja ključnih sustava, uspostaviti i dokumentirati proces razvoja i isporuke sustava koji obuhvaća postupke analize i projektiranja, razvoja programske podrške, testiranja i uvođenja u produkcijski plan.

(3) Operatori ključnih usluga dužni su na odgovarajući način razdvojiti razvojnu, testnu i produkcijsku okolinu.

(4) Operatori ključnih usluga dužni su osigurati da sve razvijene programske komponente ključnog sustava, kao i nove sklopovske komponente ključnog sustava, prije uvođenja u produkcijski rad budu na odgovarajući način testirane i da ih odobre odgovorne osobe.

(5) Operatori ključnih usluga dužni su osigurati da se za sve programske komponente ključnog sustava, prije uvođenja u produkcijski rad, provede postupak provjere ranjivosti i penetracijskog testiranja.

Upravljanje projektima

Članak 27.

(1) Operatori ključnih usluga dužni su utvrditi kriterije, načine i postupke upravljanja projektima razvoja i održavanja ključnih sustava iz članka 26. ove Uredbe.

(2) Operatori ključnih usluga dužni su za svaki projekt iz stavka 1. ovoga članka odrediti odgovornu osobu i projektni tim.

Upravljanje sklopovskom imovinom

Članak 28.

(1) Operatori ključnih usluga dužni su upravljati sklopovskom imovinom ključnog sustava tijekom cijelog njegovog životnog ciklusa.

(2) Postupak upravljanja sklopovskom imovinom mora obuhvatiti identifikaciju, evidentiranje, korištenje, održavanje, rashodovanje i kontrolirano uništavanje imovine.

Upravljanje promjenama programske imovine

Članak 29.

(1) Operatori ključnih usluga dužni su upravljati promjenama programske imovine ključnih sustava.

(2) Postupak upravljanja programskom imovinom mora obuhvatiti minimalno:

– utvrđivanje postojećih inačica programske imovine ključnih sustava

– identifikaciju i praćenje svih promjena inačica programske imovine ključnih sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost ključnog sustava

– evidentiranje svih promjena inačica programske imovine ključnih sustava onim slijedom kako su nastale zajedno s vremenom nastanka promjene.

(3) Operatori ključnih usluga dužni su u slučaju svake značajnije promjene programske imovine ključnog sustava, u skladu s procjenom rizika, provesti postupak provjere ranjivosti i penetracijskog testiranja.

Konfiguracija ključnih sustava

Članak 30.

(1) Operatori ključnih usluga dužni su osigurati:

– da ključni sustavi sadrže isključivo sklopovsku i programsku opremu koja je nužna za nesmetano funkcioniranje i sigurnost sustava i

– da se na ključnom sustavu dopusti samo onaj podatkovni promet koji je nužan.

(2) Ako uvjet iz stavka 1. ovoga članka nije moguće zadovoljiti, operatori ključnih usluga dužni su u skladu s procjenom rizika:

– provesti mjere koje umanjuju preostali rizik nastao zbog nemogućnosti ograničenog korištenja sklopovske i programske opreme i nužnog podatkovnog prometa

– dokumentirati i prihvatiti preostale rizike.

(3) Pravila kojima se definiraju ograničenja podatkovnog prometa, kao što su mrežne adrese, protokoli i portovi, potrebno je redovito obnavljati sukladno funkcionalnim i sigurnosnim potrebama ključnog sustava.

(4) Ograničenja podatkovnog prometa moraju se primjenjivati unutar ključnog sustava, između funkcionalnih podsustava, kao i kod vanjskih povezivanja ključnog sustava.

(5) Konfiguraciju ključnih sustava i popis svih elemenata koji čine ključni sustav potrebno je detaljno dokumentirati.

Preventivne provjere ranjivosti ključnih sustava

Članak 31.

(1) Operatori ključnih usluga dužni su, u skladu s procjenom rizika, osigurati provođenje redovitih i kontinuiranih provjera ranjivosti ključnih sustava, osobito onih dijelova sustava koji koriste resurse na javno dostupnim mrežnim i informacijskim sustavima.

(2) Operatori ključnih usluga dužni su osigurati da se nedostatci i ranjivosti utvrđeni tijekom postupaka provjere ranjivosti i penetracijskog testiranja obrade kroz postupak upravljanja rizicima.

Upravljanje kontinuitetom poslovanja

Članak 32.

(1) Operatori ključnih usluga dužni su identificirati poslovne procese bitne za osiguranje kontinuiteta poslovanja ključne usluge u slučajevima incidenata iz članka 35. ove Uredbe.

(2) Operatori ključnih usluga dužni su donositi operativne planove postupanja u svrhu osiguranja kontinuiteta poslovanja ključnih usluga, koji moraju minimalno uključivati:

– konkretne tehničke procedure postupanja u svrhu oporavka ključne usluge

– jasne korake i odgovornosti za aktivaciju planova oporavka ključne usluge

– definirana vremena u kojima ključna usluga mora biti uspostavljena.

(3) Operatori ključnih usluga dužni su periodično, u skladu s procjenom rizika, provesti i dokumentirati testiranje planova iz stavka 2. ovoga članka.

Pričuvna pohrana

Članak 33.

(1) Operatori ključnih usluga dužni su uspostaviti postupak upravljanja pričuvnom pohranom podataka koji su potrebni za ponovnu uspostava ključnih usluga u zahtijevanom vremenu.

(2) Postupak upravljanja pričuvnom pohranom mora obuhvaćati postupke izrade, pohrane i testiranja pričuvnih kopija podataka te oporavka podataka s pričuvnih kopija.

(3) Pričuvne kopije podataka moraju biti ažurne i pohranjene na jednoj ili više lokacija, od kojih najmanje jedna mora biti, u skladu s procjenom rizika, dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci.

DIO TREĆI
OBAVJEŠĆIVANJE O INCIDENTIMA

POGLAVLJE I.
OBVEZNO OBAVJEŠĆIVANJE O INCIDENTIMA

Obveza obavješćivanja

Članak 34.

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

Incidenti sa znatnim učinkom na kontinuitet pružanja ključne usluge

Članak 35.

(1) Učinak incidenta na kontinuitet pružanja ključne usluge utvrđuje se prema sljedećim kriterijima:

– broju korisnika pogođenih prekidom pružanja ključne usluge

– trajanju incidenta

– zemljopisnoj raširenosti incidenta ili

– drugim sektorskim kriterijima poput ekonomskog učinka i ovisnosti drugih područja ili djelatnosti o pružanju usluge.

(2) Incidenti sa znatnim učinkom na kontinuitet pružanja ključne usluge su incidenti koji ispunjavanju kriterije iz stavka 1. ovoga članka prema njihovom razvrstavanju po ključnim uslugama i incidentima kako je to predviđeno Popisom koji se nalazi u Prilogu I. ove Uredbe i čini njezin sastavni dio.

Incidenti sa znatnim učinkom na kontinuitet pružanja digitalne usluge

Članak 36.

Incidenti sa znatnim učinkom na kontinuitet pružanja digitalne usluge su incidenti koji ispunjavaju kriterije iz članka 4. Provedbene uredbe Komisije.

Procjena učinka incidenta na kontinuitet pružanja ključne usluge

Članak 37.

(1) Operatori ključnih usluga dužni su osigurati provođenje procjene učinka svih incidenta u svrhu identificiranja incidenata sa znatnim učinkom na kontinuitet pružanja ključne usluge.

(2) Operatori ključnih usluga dužni su osigurati provođenje procjene iz stavka 1. ovoga članka na način da se:

– broj korisnika pogođenih prekidom pružanja ključne usluge može odrediti prema broju fizičkih i pravnih osoba kojima je operator ključne usluge dužan pružati uslugu temeljem zakona ili pravnog posla ili ako zbog specifičnih okolnosti incidenta to nije primjenjivo, broju fizičkih i pravnih osoba koji su se koristili uslugom procijenjenog temeljem podataka o korištenju ključnom uslugom iz ranijeg razdoblja

– trajanje incidenta može odrediti prema razdoblju trajanju prekida pružanja usluge ili poremećaja u pružanju usluge koji utječe na njezinu dostupnost, autentičnost, cjelovitost ili povjerljivost

– zemljopisna raširenost incidenta može odrediti prema veličini područja na kojem su korisnici ključne usluge bili pogođeni prekidom njezinog pružanja, uključujući područja drugih država članica.

(3) Ako se ne može utvrditi kada je počelo razdoblje prekida ili poremećaja u pružanju usluge, razdoblje trajanja incidenta određuje se prema razdoblju prekida ili poremećaja rada usluge od trenutka u kojem je prekid ili poremećaj u pružanju usluge otkriven.

(4) Operatori ključnih usluga dužni su provoditi procjenu iz stavka 1. ovoga članka kontinuirano tijekom cjelokupnog trajanja incidenta, sve dok se incident ne riješi.

Procjena učinka incidenta na kontinuitet pružanja digitalne usluge

Članak 38.

Davatelji digitalnih usluga dužni su osigurati provođenje procjene svih incidenata u svrhu identificiranja incidenata sa znatnim učinkom na kontinuitet pružanja digitalne usluge sukladno parametrima propisanim u tu svrhu Provedbenom uredbom Komisije.

POGLAVLJE II.

ODJELJAK A.
OBAVIJESTI O INCIDENTIMA SA ZNATNIM UČINKOM NA KONTINUITET PRUŽANJA USLUGE

Vrste obavijesti

Članak 39.

Operatori ključnih usluga i davatelji digitalnih usluga dužni su dostavljati sljedeće obavijesti o incidentima sa znatnim učinkom na kontinuitet pružanja usluge (u daljnjem tekstu: incidenti sa znatnim učinkom):

– inicijalnu obavijest o incidentu sa znatnim učinkom

– prijelazno izvješće o incidentu sa znatnim učinkom i

– završno izvješće o incidentu sa znatnim učinkom.

Inicijalna obavijest o incidentu sa znatnim učinkom

Članak 40.

(1) Inicijalna obavijest o incidentu sa znatnim učinkom dostavlja se odmah, a najkasnije u roku od četiri sata od trenutka otkrivanja incidenta sa znatnim učinkom.

(2) Inicijalna obavijest o incidentu sa znatnim učinkom mora sadržavati opis osnovnih značajki incidenta i njegove očekivane posljedice, temeljene na podacima koji su operatoru ključne usluge odnosno davatelju digitalne usluge bili dostupni tijekom procjene učinka incidenta i po otkrivanju incidenta sa znatnim učinkom.

(3) Inicijalna obavijest o incidentu sa znatnim učinkom mora sadržavati i procjenu dana dostave prijelaznog izvješća o incidentu sa znatnim učinkom koji ne može biti kasnije od tri radna dana od podnošenja inicijalne obavijesti o incidentu.

Prijelazno izvješće o incidentu sa znatnim učinkom

Članak 41.

(1) Prvo prijelazno izvješće o incidentu sa znatnim učinkom dostavlja se najkasnije u roku od tri radna dana od podnošenja inicijalne obavijesti o incidentu.

(2) Prvo prijelazno izvješće o incidentu sa znatnim učinkom mora sadržavati detaljniji opis incidenta i njegovih posljedica.

(3) Ako ne raspolažu stvarnim podacima, operatori ključnih usluga i davatelji digitalnih usluga dužni su prvo prijelazno izvješće podnijeti uz napomenu da se opisi temelje na procjeni podataka.

(4) Operatori ključnih usluga i davatelji digitalnih usluga dužni su, bez odgode, dostavljati i dodatna prijelazna izvješća o incidentu sa znatnim učinkom ako saznaju za nove podatke ili značajnije promjene do kojih je došlo od prvog prijelaznog izvješća, a osobito ako je incident eskalirao ili se smanjio ili su otkriveni novi uzroci ili je poduzeo nove radnje za rješavanje incidenta.

Završno izvješće o incidentu sa znatnim učinkom

Članak 42.

(1) Operatori ključnih usluga i davatelji digitalnih usluga dužni su podnijeti završno izvješće o incidentu sa znatnim učinkom najkasnije u roku od 15 dana od dana procijene da je redovito pružanje usluge ponovno uspostavljeno.

(2) Završno izvješće o incidentu sa znatnim učinkom mora sadržavati stvarne podatke o učinku incidenta, analizu uzroka incidenta, sažetak mjera koje su primijenjene za ublažavanje incidenta ili se planiraju primjenjivati radi otklanjanja uočene ranjivosti i sprečavanja pojave incidenta u budućnosti.

(3) Operatori ključnih usluga i davatelji digitalnih usluga dužni su završno izvješće o incidentu sa znatnim učinkom podnijeti i prije proteka roka iz stavka 1. ovoga članka ako utvrde da već prijavljeni incident više ne ispunjava kriterije za određivanje incidenta sa znatnim učinkom te da se ne očekuje da će ih ispunjavati do rješavanja incidenta, o čemu su dužni obavijestiti nadležni CSIRT bez odgode.

(4) Obavijest iz stavka 3. ovoga članka mora sadržavati naznaku dana dostave završnog izvješća.

(5) Operatori ključnih usluga i davatelji digitalnih usluga obavijestit će nadležni CSIRT o produženju roka iz stavaka 1. i 4. ovoga članka ako im nisu raspoloživi stvarni podaci o učinku incidenta.

(6) U obavijesti iz stavka 5. ovoga članka obvezno se navodi obrazloženje za odgodu i novi procijenjeni rok dostave konačnog izvješća koji ne može biti duži od 30 dana od dana procijene da je redovito pružanje usluge ponovno uspostavljeno.

Dostava obavijesti o incidentima sa znatnim učinkom

Članak 43.

(1) Nadležni CSIRT donosi smjernice za dostavu obavijesti o incidentima sa znatnim učinkom, kojima se određuje način dostave obavijesti i obrasci za obvezno obavješćivanje o incidentima sa znatnim učinkom.

(2) Nadležni CSIRT utvrđuje obrasce iz stavka 1. ovoga članka uz suglasnost nadležnog sektorskog tijela.

(3) Operatori ključnih usluga i davatelji digitalnih usluga dužni su dostavljati obavijesti o incidentima sa znatnim učinkom sukladno smjernicama iz stavka 1. ovoga članka.

Razmjena obavijesti

Članak 44.

(1) Nadležni CSIRT dužan je bez odgode zaprimljene obavijesti o incidentu sa znatnim učinkom dostaviti nadležnom sektorskom tijelu.

(2) Iznimno od stavka 1. ovoga članka, nadležni CSIRT nije u obvezi dostavljati zaprimljene obavijesti o incidentima sa znatnim učinkom ako nadležno sektorsko tijelo temeljem posebnog propisa zaprima izravno od operatora ključne usluge obavijesti o incidentima koje po svom sadržaju i svrsi odgovaraju zahtjevima iz Zakona i ove Uredbe.

(3) Nadležno sektorsko tijelo dužno je obavijestiti nadležni CSIRT o postojanju iznimke iz stavka 2. ovoga članka.

ODJELJAK B.
POSTUPANJE PO OBAVIJESTIMA O INCIDENTIMA SA ZNATNIM UČINKOM

Rješavanje incidenata sa znatnim učinkom

Članak 45.

(1) Nadležni CSIRT po zaprimanju zahtjeva operatora ključnih usluga, davatelja digitalne usluge ili nadležnog sektorskog tijela za rješavanje incidenta provodi analizu i klasifikaciju incidenta na temelju zaprimljenih obavijesti o incidentu sa znatnim učinkom te se uključuje u postupak rješavanja incidenta.

(2) Nadležni CSIRT u rješavanju incidenata sa znatnim učinkom mogu koristiti stručnu pomoć nacionalno nadležnog CSIRT-a za drugi sektor, CSIRT-ova drugih država članica nadležnih za sektor u kojem je incident nastao te, prema potrebi, CSIRT mrežu Europske komisije.

(3) Nadležni CSIRT je dužan, u suradnji s nadležnim sektorskim tijelom, za svaki incident sa znatnim učinkom utvrditi njegov prekogranični utjecaj.

(4) Nadležno sektorsko tijelo dužno je procjenjivati učinak svakog pojedinačnog incidenta, o kojem je obaviješten sukladno članku 44. ove Uredbe, na osiguranje kontinuiteta pružanja ključne odnosno digitalne usluge na sektorskoj razini.

(5) Nadležno sektorsko tijelo dužno je temeljem procjena iz stavka 4. ovoga članka uključivati se u postupak uspostave kontinuiteta pružanja usluge kada je na sektorskoj razini ugrožen kontinuitet pružanja ključne odnosno digitalne usluge.

Evidencije o incidentima sa znatnim učinkom

Članak 46.

(1) Nadležni CSIRT-ovi dužni su voditi evidencije o svim incidentima sa znatnim učinkom prema sektorima i podsektorima iz priloga I. Zakona.

(2) Evidencije iz stavka 1. ovoga članka i rokovi za dostavu podataka iz evidencija jedinstvenoj nacionalnoj kontaktnoj točki utvrđuju se smjernicama koje donosi jedinstvena nacionalna kontaktna točka.

POGLAVLJE III.
OBAVJEŠĆIVANJE O INCIDENTIMA NA DOBROVOLJNOJ OSNOVI

Članak 47.

(1) Subjekti koji pružaju ključne usluge s popisa iz Priloga I. Zakona ili digitalne usluge s Popisa iz Priloga II. Zakona, a ne predstavljaju operatora ključnih usluga odnosno davatelja digitalnih usluga u smislu ove Uredbe, mogu nadležni CSIRT obavješćivati o incidentima koji su uzrokovali prekid ili značajniji poremećaj u pružanju ključne ili digitalne usluge.

(2) Subjekti iz stavka 1. ovoga članka dostavljaju obavijesti o incidentima na dobrovoljnoj osnovi sukladno smjernicama iz članka 43. ove Uredbe.

(3) Nadležni CSIRT postupit će po zahtjevu za rješavanje incidenata iz stavka 1. ovoga članka prema prioritetima i raspoloživim resursima, vodeći računa o obvezama iz članka 45. ove Uredbe.

DIO ČETVRTI
PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 48.

Nadležni CSIRT-ovi dužni su donijeti smjernice iz članka 43. stavka 1. ove Uredbe u roku od 90 dana od dana stupanja na snagu ove Uredbe.

Članak 49.

Ova Uredba stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 022-03/18-03/34
Urbroj: 50301-29/09-18-8
Zagreb, 26. srpnja 2018.

Predsjednik
mr. sc. Andrej Plenković, v. r.

PRILOG I.

KRITERIJI ZA UTVRĐIVANJE INCIDENATA KOJI IMAJU ZNATAN UČINAK NA PRUŽANJE KLJUČNE USLUGE

Sektor	Podsektor	Ključna usluga	Kriteriji	Pragovi
Energetika	Električna energija	Proizvodnja električne energije	Smanjenje proizvodnje	60 MW
		Prijenos električne energije	Prekid prijenosa	Bez iznimke
		Distribucija električne energije	Prekid napajanja	Više od 20.000 obračunskih mjernih mjesta
	Nafta	Transport nafte naftovodima	Prekid transporta	Bez iznimke
		Proizvodnja nafte	Smanjenje proizvodnje naftnog polja	10.000 t/god
		Proizvodnja naftnih derivata	Smanjenje proizvodnje naftnih derivata	Motorni benzini: 40.000 t/god Dizelsko gorivo: 40.000 t/god Plinska ulja: 20.000 t/god
		Skladištenje nafte i naftnih derivata	Smanjenje skladišnog kapaciteta nafte na terminalu	200.000 m^3
			Smanjenje skladišnog kapacitet naftnih derivata pojedinog skladišta	12.000 m^3
	Plin	Distribucija plina	Prekid distribucije krajnjim kupcima	Više od 20.000 obračunskih mjernih mjesta.
		Transport plina	Prekid transporta	Bez iznimke
		Skladištenje plina	Smanjenje skladišnih kapaciteta	5% potrošnje plina u RH u prethodnoj godini
		Prihvat i otprema UPP-a	Smanjenje kapaciteta uplinjavanja UPP u m^3/h	Više od 100.000 m^3/h

		Proizvodnja prirodnog plina	Smanjenje proizvodnje plina predanog u transportni sustav na pojedinom ulazu	20%
Prijevoz	Zračni promet	Zračni prijevoz putnika i tereta	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
		Kontrola zračnog prometa	Narušavanje integriteta podataka na ključnim operativnim sustavima	Ugrožen 1 zrakoplov u bilo kojem volumenu kontroliranog zračnog prostora i na manevarskim površinama aerodroma
			Gubitak podataka na ključnim operativnim sustavima	Ugrožen 1 zrakoplov u bilo kojem volumenu kontroliranog zračnog prostora i na manevarskim površinama aerodroma
	Željeznički promet	Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom	Ugrožavanje integriteta prometno-upravljačkog, signalno-sigurnosnog ili elektro-energetskog podsustava	Bez iznimke
		Usluge prijevoza robe i/ili putnika željeznicom	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
	Vodni prijevoz	Nadzor kretanja brodova (VTS usluga)	Ugrožavanje integriteta sustava za nadzor i upravljanje pomorskim prometom VTMIS i pružanja VTS usluga	Onemogućeno korištenje punih funkcionalnosti sustava za nadzor i upravljanje pomorskim prometom VTMIS i pružanja VTS usluga iz najmanje jednog kontrolnog centra u trajanju dužem od 3 sata
		Obavljanje poslova pomorske radijske službe	Ugrožavanje integriteta sustava pomorske radijske službe i pružanja usluga pomorske radijske službe	Onemogućeno korištenje punih funkcionalnosti sustava pomorske radijske službe i pružanja usluga pomorske radijske službe iz najmanje jedne obalne radijske postaje u trajanju dužem od 3 sata
		Održavanje objekata pomorske signalizacije	Ugrožavanje integriteta objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe	Nedostupnost najmanje 20% objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe u pojedinom plovnom području u trajanju dužem od 3 sata
				Nedostupnost najmanje 20% objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe u lukama otvorenim za javni promet od osobitog (međunarodnog) gospodarskog značaja za RH s prilaznim plovnim putovima u trajanju dužem od 3 sata

		Prijevoz putnika u međunarodnom i/ili domaćem prometu	Ovisnost drugih sektora o usluzi	Svi sektori čiji korisnici ili zaposlenici koriste pomorski prijevoz
			Utjecaj incidenata na gospodarske i društvene aktivnosti te na javnu sigurnost	Trajanje incidenta u periodu duljem od jednog dana
		Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu	Nedostupnost i ograničenost operativnog sustava	Nemogućnost obavljanja lučkih operacija u periodu duljem od 3 dana
			Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od 3 dana može uzrokovati zastoje u ovisnim sektorima
			Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od 3 dana može uzrokovati zastoje u ovisnim sektorima
		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	Onemogućeno obavljanje usluge prijevoza	Prekid obavljanja usluge prijevoza na više od 30% linija u trajanju duljem od 3 sata
		Praćenje i lociranje plovila u unutarnjoj plovidbi	Onemogućavanje rada »RIS« sustava koji se odnosi na »Praćenje i lociranje plovila u unutarnjoj plovidbi« (VTT)	Ugroza praćenja i lociranja minimalno jednog plovila u unutarnjoj plovidbi
		Obavijesti brodarstvu u unutarnjoj plovidbi	Onemogućavanje točne i pravovremene objave »Obavijesti brodarstvu u unutarnjoj plovidbi«	Ugroza objave minimalno jedne »Obavijesti brodarstvu u unutarnjoj plovidbi«
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi	Onemogućenje rada korisničkih radnih stanica na obali u pristupu ćelijama »Elektroničkih navigacijskih karata u unutarnjoj plovidbi« (ENC)	Onemogućeno korištenje minimalno jedne ćelije ENC-a
		Baza podataka o trupu plovila u unutarnjoj plovidbi	Ugroza točnosti sadržaja u bazi podataka	Ugroza sadržaja u bazi podataka za minimalno jedno plovilo
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi	Nemogućnost primanja i slanja ERI poruka	Nemogućnost primanja/slanja minimalno jedne ERI poruke
	Cestovni prijevoz	Javni prijevoz putnika	Broj voznih jedinica pogođenih incidentom	20
			Broj putnika pogođenih incidentom	10 000
		Korištenje cestovne infrastrukture	Ugrožavanje integriteta prometno-upravljačkog, elektro-energetskog ili sustava za zaštitu od požara na cestovnoj infrastrukturi (uključujući objekte: mostovi, tuneli, vijadukti)	Bez iznimke
		Upravljanje prometnim tokovima ili informiranje vozača (ITS)	Prekid usluge centra za kontrolu i upravljanje prometom	30 minuta
			Prekid usluge centra za informiranje vozača o stanju u prometu	60 minuta
			Broj prometnih svjetala (semafora) pogođenih incidentom	10
Bankarstvo		Platne usluge	Kriteriji koje operatori ključnih usluga u sektoru bankarstva trebaju upotrijebiti za klasifikaciju značajnih operativnih ili sigurnosnih incidenata prema smjernicama Europskog nadzornog tijela za bankarstvo (EBA) iz članka 96. stavka 3. Direktive (EU) 2015/2366 o platnim uslugama na unutarnjem tržištu (PSD2 Direktiva)	Pragovi koje operatori ključnih usluga u sektoru bankarstva trebaju upotrijebiti za klasifikaciju značajnih operativnih ili sigurnosnih incidenata prema smjernicama Europskog nadzornog tijela za bankarstvo (EBA) iz članka 96. stavka 3. PSD2 Direktive

Infrastrukture financijskog tržišta		Usluge mjesta trgovanja	Trajanje incidenta	30 minuta
		Usluge središnjih drugih ugovornih strana (CCP)	Trajanje incidenta	30 minuta
Zdravstveni sektor		Primarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati
			Nedostupnost informacijskog sustava hitne medicinske pomoći	8 sati
		Sekundarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati
			Nedostupnost bolničkog informacijskog sustava u općoj bolnici	1 sat
		Tercijarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost bolničkog informacijskog sustava u kliničkom bolničkom centru	1 sat
			Nedostupnost bolničkog informacijskog sustava u kliničkoj bolnici	1 sat
			Nedostupnost bolničkog informacijskog sustava u klinici	1 sat
		Transfuzijska medicina i transplantacija organa	Nedostupnost informacijskog sustava za djelatnost transfuzijske medicine	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost koordinatora Nacionalnog transplantacijskog programa	1 sat
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita	Nedostupnost informacijskog sustava ZOROH – Zdravstveno osiguranje – registar osiguranika Hrvatske	24 sata
			Nedostupnost servisa za provjeru statusa obveznog i dopunskog zdravstvenog osiguranja	8 sati
			Nedostupnost sustava za izdavanje Europskih kartica zdravstvenog osiguranja	72 sata
		Sigurnost hrane	Nedostupnost Središnjeg informacijskog sustava sanitarne inspekcije	24 sata
		Zaštita od opasnih kemikalija	Nedostupnost Registra sigurnosno-tehničkih listova	72 sata
			Nedostupnost Registra opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH	72 sata
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Nemogućnost obustave stavljanja u promet lijekova i povlačenja lijekova iz prometa	72 sata
			Nemogućnost praćenja ozbiljnih nesukladnosti i provjere kakvoće lijekova na tržištu RH	60 sati
			Nemogućnost praćenja sigurnosti medicinskih proizvoda	84 sata

		Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu kroz vođenje javnozdravstvenih registara	Nedostupnost Nacionalnog javnozdravstvenog informacijskog sustava	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
Opskrba vodom za piće i njezina distribucija		Opskrba krajnjih korisnika	Prekid opskrbe zdravstveno ispravne vode iz sustava javne vodoopskrbe	više od 24 sata
			Potpuni prekid opskrbe vodom iz sustava javne vodoopskrbe	više od 24 sata
Digitalna infrastruktura		DNS usluga za .hr TLD	Nedostupnost usluge	60 min
			Neovlaštena promjena podataka na domenama	20% od ukupnog broja registriranih .hr domena
		Registar naziva domena za .hr TLD	Nedostupnost usluge	180 min
			Neovlaštena promjena podataka na domenama	20% od ukupnog broja registriranih .hr domena
		Sustav za registriranje i administriranje sekundarne domene	Nedostupnost usluge	180 min
			Nedostupnost ovlaštenih registara	40% od ukupnog broja registara
		Usluga IXP	Nedostupnost usluge za 50% spojenih članica	8 sati
			Nedostupnost usluge za 75% spojenih članica	4 sata
			Nedostupnost usluge za sve spojene članice	2 sata
Poslovne usluge za državna tijela		Usluge u sustavu e-Građani	Broj korisnika pogođenih prekidom	20%
			Trajanje incidenta	2 sata
		Poslovne usluge za korisnike državnog proračuna	Trajanje incidenta	1 sat
			Broj sektorskih korisnika pogođenih incidentom	1