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