

Na temelju odredbe članka 47. stavka 4., Zakona o kibernetičkoj sigurnosti (Narodne novine broj 14/24; dalje u tekstu: Zakon) ravnatelj Hrvatske akademske i istraživačke mreže – CARNET, donosi

POLITIKU UPRAVLJANJA BAZOM PODATAKA O REGISTRACIJI NAZIVA DOMENA

I. OPĆE ODREDBE

Nadležnost i područje primjene

Članak 1.

(1) Ovim dokumentom uspostavlja se politika upravljanja bazom podataka o registraciji naziva domena (dalje u tekstu: baza podataka) u nadležnosti CARNET-a, kako bi se osigurala usklađenost za zakonodavstvom kojim se uređuje područje kibernetičke sigurnosti, primjenjivim sigurnosnim standardima, najboljim praksama i ostalim primjenjivim zahtjevima.

(2) CARNET, kao subjekt kojem je delegirana vršna internetska domena .hr ima ulogu registra naziva vršne nacionalne internetske domene koji je odgovoran za upravljanje njome, što uključuje registraciju naziva domena u okviru vršne domene, tehničko upravljanje vršnom domenom, uključujući upravljanje njezinim poslužiteljima naziva, održavanje njezinih baza podataka i distribuciju datoteka iz zone vršne domene u poslužitelje naziva, neovisno o tome obavlja li sam CARNET bilo koju od tih operacija ili za njihovo obavljanje koristi vanjskog davatelja usluge, ali su isključene situacije u kojima registar koristi nazive vršnih domena samo za vlastitu upotrebu.

Ciljevi donošenja

Članak 2.

U svrhu osiguranja usklađenosti za Zakonom, sposobnosti djelovanja, sprječavanja gubitka i/ili štete na podacima, ovom politikom za upravljanje bazom podataka definiraju se sljedeći ciljevi:

- vjerodostojnost podataka i utvrđivanje postupka provjere podataka temeljem kojih se vrši registracija domene
- utvrđivanje obveze čuvanje podataka i pristupa podacima o korisniku domene
- osiguranje cjelovitosti, dostupnosti i povjerljivosti baze podataka

II. UPRAVLJANJE PODACIMA

Podaci u bazi podataka

Članak 3.

(1) Baza podataka obavezno sadrži podatke i informacije potrebne za identifikaciju korisnika domene i registrara koji upravljaju nazivima domena te za kontakt s njima, i to:

- naziv domene,
- datum registracije
- ime i prezime korisnika domene
- adresa korisnika
- adresu elektroničke pošte
- telefonski broj korisnika
- OIB/VAT broj korisnika,
- telefonski broj za kontakt registrara koji upravlja nazivom domene

Način provjere podataka i informacija

Članak 4.

Podatke i informacije navedene u članku 3. ovog Pravilnika, a koji se prikupljaju prilikom podnošenja zahtjeva za registraciju domene, CARNET provjerava na način da:

- utvrđuje i provjerava identitet korisnika domene uvidom u OIB registar Ministarstva financija RH, Porezne uprave
- vrši verifikaciju korisnika putem priloženih osobnih dokumenata
- vrši verifikaciju korisnika putem sustava e-Građani

Javna objava podataka

Članak 5.

Nakon provedenog postupka registracije domene CARNET bez odgode javno objavljuje podatke o registraciji naziva domena a koji nisu osobni podaci.

Čuvanje podataka, informacija i dokumentacije

Članak 6.

(1) Podatke, informacije i dokumentaciju prikupljenu u postupku obrade zahtjeva za registracijom domene i njegove provjere, CARNET čuva 25 godina od prestanka prava korisnika na korištenje domene, a što se posebno odnosi na:

- identifikacijske dokumente i drugu dokumentaciju na temelju koje je utvrđen identitet korisnika domene
- zahtjev za registraciju domene i drugu dokumentacija vezanu uz registraciju domene.

(2) Nakon proteka roka navedenog u stavku 1. ovog članka, CARNET osobne podatke o korisniku domene trajno briše, a dokumentaciju iz stavka 1. ovoga članka uništava sukladno propisima o zaštiti osobnih podataka.

Obveza prenošenja i omogućavanja pristupa podacima trećih strana

Članak 7.

CARNET je obvezan tijelima kaznenog progona i nadležnom CSIRT-u, tijelu nadležnom za zaštitu osobnih podataka i drugim pravnim osobama s javnim ovlastima, kao i državnim tijelima u okviru izvršavanja javnih ovlasti, na njihov obrazloženi zahtjev, bez odgode, a najkasnije u roku od 72 sata od primitka zahtjeva, dostaviti ili na drugi odgovarajući način omogućiti pristup podacima o korisnicima domene a koji su sadržani u bazi podataka.

Periodična provjera podataka

Članak 8.

CARNET jednom godišnje, za sve korisnike domena provodi provjeru postojanja korisnika domene, kao i usklađenost postupanja korisnika domene s obvezama iz propisa kojim je uređeno ustrojstvo i upravljanje vršnom nacionalnom internetskom domenom.

III. OSIGURANJE CJELOVITOSTI, DOSTUPNOSTI I POVJERLJIVOSTI BAZE PODATAKA

Kontrola pristupa

Članak 9.

(1) Pristup bazi podataka imaju samo osobe koje za to imaju posebna ovlaštenja.

(2) Posebna ovlaštenja za pristup bazi podataka iz stavka 1. ovog članka temelje se na pojedinim ulogama i odgovornostima osoba koje pristupaju bazi podataka te minimalnim potrebama za obavljanje radnih zadataka.

(3) Ovlaštenja za pristup bazi podataka se redovito ažuriraju i revidiraju.

Članak 10.

(1) Svaka prijava i aktivnost koja se odnosi na bazu podataka se bilježi u zapisima pri čemu se koriste alati i procesi za praćenje i bilježenje aktivnosti na mrežnom i informacijskom sustavu.

(2) Zapisi iz stavka 1. ovog članka čuvaju se u skladu s regulatornim okvirom.

Cjelovitosti i dostupnost podataka

Članak 11.

(1) Za predmetnu bazu podataka CARNET osigurava visoku razinu različitih aspekata sigurnosti, s ciljem osiguravanja cjelovitosti, povjerljivosti i dostupnosti podataka.

Fizička sigurnost

(2) CARNET osigurava 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. Također, uspostavljen je tehnički sustav nadzora fizičke sigurnosti i sigurnosti okruženja koji se redovito nadzire. Svi ključni poslužitelji smješteni su u prostorije posebne namjene koje imaju uspostavljenju kontrolu pristupa, adekvatnu klimatizaciju, protupožarnu zaštitu te alternativne načine napajanja u slučaju prestanka opskrbe električne energije iz primarnog izvora.

Sigurnost pristupa

(3) CARNET je definirao osobe koje imaju pravo pristupa pojedinim segmentima sustava. Poslovne aktivnosti koje se obavljaju na ključnim sustavima ili podupiru sustav su dokumentirane, a CARNET se u dodjeli privilegiranih prava pristupa vodi principima *opravdane poslovne potrebe, najmanjih potrebnih prava te dvostruke provjere.*

Sigurnost informacijskog sustava

(4) CARNET ima formalno usvojeni program upravljanja sigurnošću informacijskih sustava koji propisuje načela uspostave programa sigurnosti, uloge u programu sigurnosti, upravljanje sigurnošću poslovnih procesa, procjenu rizika, postupanje s informacijama, fizičku sigurnost, sigurnost mreže, sigurnost računalnih i programskih sustava, politiku prihvatljivog korištenja, kategorizaciju informacija, upravljanje incidentima i rad s vanjskim partnerima.

Postupak i periodičnost izrade sigurnosne preslike

(5) Sigurnosne preslike podataka se pohranjuju na dedicerani sustav na izdvojenoj lokaciji. Pored toga, redovito se radi sigurnosna preslika baze podataka, a uspješnost vraćanja podataka iz sigurnosne preslike se periodički testira.

Provjera ranjivosti i analiza rizika

(6) Minimalno jednom godišnje se provodi penetracijsko testiranje i ispituje ranjivost cjelokupne infrastrukture registra te se ispravke i nadogradnje provode temeljem rezultata testiranja.

(7) Također, CARNET se u poslovnom odlučivanju vodi temeljem analize rizika te u obzir uzima relevantne prijetnje i ranjivosti sustava. Na temelju provedenih analiza, CARNET donosi i implementira mjere podizanja sigurnosti s posebnim težištem na osiguranju raspoloživosti, povjerljivosti i cjelovitosti podataka.

Postupanje u slučaju incidenta

(8) CARNET je definirao krizni plan aktivnosti koji omogućava pravovremeno prepoznavanje kriznih situacija, definiranje strategija rješavanja i kontroliranje krize i prije nastanka štetnih posljedica. Krizni plan obuhvaća i procedure i postupanja u slučaju incidenata.

(9) Incidenti iz područja primjene Zakona o kibernetičkoj sigurnosti prijavljuju se putem Nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima.

Klasa: 700-800/25/218

Ur.broj: 91448-650-97-25-10



Hrvoje Puljiz
Ravnatelj CARNET-a