32011R1179

PROVEDBENA UREDBA KOMISIJE (EU) br. 1179/2011

od 17. studenoga 2011.

o utvrđivanju tehničkih specifikacija za sustave za online prikupljanje u skladu s Uredbom (EU) br. 211/2011 Europskog parlamenta i Vijeća o građanskoj inicijativi

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 211/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o građanskoj inicijativi [1], a posebno njezin članak 6. stavak 5.,

nakon savjetovanja s europskim nadzornikom za zaštitu podataka,

budući da:

(1) Uredbom (EU) br. 211/2011 propisano je da ako se izjave o potpori prikupljaju online, sustav koji se upotrebljava za tu namjenu mora udovoljavati određenim sigurnosnim i tehničkim zahtjevima i mora ga odobriti nadležno tijelo relevantne države članice.

(2) Sustav za online prikupljanje u smislu Uredbe (EU) br. 211/2011 informacijski je sustav koji se sastoji od softvera, hardvera, okruženja u kojemu je smješten, poslovnih procesa i osoblja za online prikupljanje izjava o potpori.

(3) U Uredbi (EU) br. 211/2011 određeni su zahtjevi koje sustavi za online prikupljanje moraju ispunjavati kako bi bili odobreni i njome je predviđeno da Komisija treba donijeti tehničke specifikacije za primjenu navedenih zahtjeva.

(4) U projektu Top 10 iz 2010. u okviru projekta OWASP (Open Web Application Security Project) naveden je pregled najkritičnijih sigurnosnih rizika za web aplikacije kao i alata za rješavanje navedenih rizika; stoga se tehničke specifikacije temelje na nalazima ovog projekta.

(5) Prilikom primjene tehničkih specifikacija organizatori trebaju zajamčiti da su tijela država članica odobrila sustave za online prikupljanje i trebaju doprinijeti osiguravanju provedbe odgovarajućih tehničkih i organizacijskih mjera potrebnih za ispunjavanje obveza određenih u Direktivi 95/46/EZ Europskog parlamenta i Vijeća [2] u vezi sa sigurnošću aktivnosti obrade u trenutku oblikovanja sustava za obradu i u trenutku same obrade kako bi se očuvala sigurnost i time spriječila svaka neovlaštena obrada i zaštitili osobni podaci od slučajnog ili nezakonitog uništavanja ili slučajnog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa.

(6) Organizatori trebaju olakšati proces odobravanja uporabom softvera koji je propisala Komisija u skladu s člankom 6. stavkom 2. Uredbe (EU) br. 211/2011.

(7) Organizatori građanskih inicijativa, kao kontrolori podataka, trebaju prilikom online prikupljanja izjava o potpori primjenjivati tehničke specifikacije određene u ovoj Uredbi kako bi osigurali zaštitu obrađenih osobnih podataka. Ako podatke obrađuje davatelj usluga obrade podataka, organizatori trebaju osigurati da davatelj usluga obrade podataka postupa samo u skladu s napucima organizatora i da primjenjuje tehničke specifikacije određene u ovoj Uredbi.

(8) U ovoj se Uredbi poštuju temeljna prava i načela ugrađena u Povelju Europske unije o temeljnim pravima, posebno njezin članak 8. u kojem je navedeno da svatko ima pravo na zaštitu osobnih podataka koji se na njega odnose.

(9) Mjere predviđene ovom Uredbom u skladu su s mišljenjem Odbora uspostavljenog člankom 20. Uredbe (EU) br. 211/2011,

[1] SL L 65, 11.3.2011., str. 1.

[2] SL L 281, 23.11.1995., str. 31.

DONIJELA JE OVU ODLUKU:

Članak 1.

Tehničke specifikacije iz članka 6. stavka 5. Uredbe (EU) br. 211/2011 određene su u Prilogu.

Članak 2.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 17. studenoga 2011.

Za Komisiju
Predsjednik
José Manuel BARROSO

PRILOG

1. TEHNIČKE SPECIFIKACIJE ČIJI JE CILJ PROVEDBA ČLANKA 6. STAVKA 4. TOČKE (a) UREDBE (EU) br. 211/2011

Kako bi se spriječilo automatsko podnošenje izjave o potpori kroz uporabu sustava, potpisnik prolazi kroz odgovarajući proces provjere u skladu sa sadašnjom praksom prije podnošenja izjave o potpori. Jedan od mogućih procesa provjere je uporaba snažnog testa „captcha".

2. TEHNIČKE SPECIFIKACIJE ČIJI JE CILJ PROVEDBA ČLANKA 6. STAVKA 4. TOČKE (b) UREDBE (EU) br. 211/2011

Standardi informacijske sigurnosti

2.1. Organizatori osiguravaju dokumentaciju kojom dokazuju da ispunjavaju zahtjeve norme ISO/IEC 27001 bez njezina usvajanja. S tim su ciljem organizatori:

(a) proveli potpunu procjenu rizika u okviru koje se utvrđuje područje primjene sustava, ističe poslovni učinak u slučaju različitih povreda informacijske sigurnosti, navode prijetnje i osjetljivosti informacijskog sustava, izrađuje dokument o analizi rizika u kojem su također navedene protumjere za sprečavanje takvih prijetnji i pravni lijekovi koji će se poduzeti u slučaju pojave prijetnje i naposljetku sastavlja prioritetni popis poboljšanja;

(b) oblikovali i proveli mjere za postupanje s rizicima u vezi sa zaštitom osobnih podataka i zaštitom obiteljskog i privatnog života i mjere koje će se poduzeti u slučaju pojave rizika;

(c) utvrdili rezidualne rizike u pisanom obliku;

(d) osigurali organizacijska sredstva za zaprimanje povratnih informacija o novim prijetnjama i poboljšanjima sigurnosti.

2.2. Organizatori na temelju analize rizika iz točke 2.1. podtočke (a) odabiru sigurnosni nadzor između sljedećih normi:

(1) ISO/IEC 27002; ili

(2) „standarda dobre prakse" Foruma za informacijsku sigurnost

za rješavanje sljedećih pitanja:

(a) procjena rizika (preporučuje se ISO/IEC 27005 ili druga posebna i prikladna metodologija za procjenu rizika);

(b) fizičke i ekološke sigurnosti;

(c) sigurnosti ljudskih potencijala;

(d) komunikacijskog i operativnog upravljanja;

(e) standardnih mjera za kontrolu pristupa uz mjere navedene u ovoj Uredbi;

(f) nabave, razvoja i održavanja informacijskih sustava;

(g) upravljanja incidentima u vezi sa sigurnošću informacija;

(h) mjera za otklanjanje i ublažavanje povreda informacijskih sustava koje za posljedicu mogu imati uništavanje ili slučajni gubitak, izmjenu, neovlašteno otkrivanje obrađenih osobnih podataka ili pristup njima;

(i) usklađenosti;

(j) sigurnosti računalne mreže (preporučuje se ISO/IEC 27033 ili standard dobre prakse).

Primjena navedenih normi može se ograničiti na dijelove organizacije koji su relevantni za sustav za online prikupljanje. Na primjer, sigurnost ljudskih potencijala može se ograničiti na cjelokupno osoblje koje ima fizički ili mrežni pristup sustavu za online prikupljanje, a fizička/ekološka sigurnost može se ograničiti na zgrade u kojima je smješten sustav.

Funkcionalni zahtjevi

2.3. Sustav za online prikupljanje sastoji se od web aplikacije uspostavljene za prikupljanje izjava o potpori za pojedinačnu građansku inicijativu.

2.4. Ako su za upravljanje sustavom potrebne različite uloge, uspostavljaju se različite razine kontrole pristupa u skladu s načelom najmanjih povlastica.

2.5. Funkcije kojima se može javno pristupiti jasno su odvojene od funkcija namijenjenih za potrebe upravljanja. Nijednom kontrolom pristupa ne smije se onemogućiti čitanje podataka koji se nalaze u javno dostupnom dijelu sustava, uključujući podatke o inicijativi i elektronički obrazac izjave o potpori. Potpisivanje za inicijativu moguće je samo preko tog javno dostupnog dijela.

2.6. Sustav otkriva i sprečava podnošenje duplikata izjava o potpori.

Sigurnost na razini primjene

2.7. Sustav je prikladno zaštićen od poznatih osjetljivosti i iskorištavanja. S tim ciljem udovoljava, između ostalog, sljedećim zahtjevima:

2.7.1. Sustav štiti od ubacivanja kao što su ubacivanja uzrokovana strukturiranim jezikom za upite (SQL), laganim protokolom za pristup imeniku (LDAP), jezikom za navigaciju u XML dokumentima (XPath), naredbama operativnog sustava (OS) ili argumentima programa. Za tu je namjenu potrebno najmanje sljedeće:

(a) svi se ulazni podaci korisnika potvrđuju;

(b) potvrđivanje se provodi najmanje logikom na strani poslužitelja;

(c) pri svakoj uporabi tumača jasno se odvajaju nepouzdani podaci od naredbe ili upita. Za SQL pozive to znači uporaba vezanih varijabli u svim pripremljenim izjavama i pohranjenim postupcima i izbjegavanje dinamičnih upita.

2.7.2. Sustav štiti od unakrižnog skriptiranja (XSS). Za tu je namjenu potrebno najmanje sljedeće:

(a) provjerava se sigurnost svih ulaznih podataka korisnika poslanih natrag prema pretraživaču (kroz potvrdu unosa);

(b) svi su ulazni podaci korisnika pravilno kodirani prije no što ih se uvrsti na izlaznu stranicu;

(c) pravilnim se kodiranjem izlaznih podataka osigurava da se navedeni ulazni podaci uvijek obrađuju kao tekst u pretraživaču. Ne upotrebljavaju se aktivni sadržaji.

2.7.3. Sustav ima snažno upravljanje autentikacijom i sjednicom za što je potrebno najmanje sljedeće:

(a) prilikom pohranjivanja uvijek se zaštićuju podaci o prijavi uporabom raspršenog adresiranja ili kodiranja. Time se smanjuje rizik da se prilikom autentikacije upotrijebi metoda „pass-the-hash”;

(b) podatke o prijavi nemoguće je pogoditi niti se može preko njih pisati na temelju slabih funkcija za upravljanje računom (npr. stvaranje računa, promjena lozinke, obnova lozinke, slabi identifikator sjednice (ID));

(c) identifikatori sjednice i podaci o sjednici nisu prikazani u jedinstvenom lokatoru resursa (URL);

(d) identifikatori sjednice nisu osjetljivi na fiksaciju sjedničkog ključa;

(e) identifikatori sjednice vremenski su ograničeni čime se osigurava odjava korisnika;

(f) identifikatori sjednice ne ponavljaju se nakon uspješne prijave;

(g) lozinke, identifikatori sjednice i drugi podaci o prijavi šalju se samo preko protokola za sigurnost prijenosnog sloja (TLS);

(h) dio sustava koji se odnosi na upravljanje je zaštićen. Ako je zaštićen autentikacijom na temelju jednog čimbenika, lozinka je sastavljena od najmanje 10 znakova uključujući barem jedno slovo, jedan broj i jedan posebni znak. Kao druga mogućnost može se upotrebljavati autentikacija na temelju dva čimbenika. Ako se upotrebljava autentikacija na temelju samo jednog čimbenika, ona uključuje mehanizam provjere koji se sastoji od dva koraka za pristup upravljačkom dijelu sustava preko interneta u kojem se jedan čimbenik proširuje drugim sredstvima autentikacije kao što je jednokratna lozinka/kod putem SMS-a ili asimetrično kodirani nasumični niz koji se treba dekodirati uporabom sustavu nepoznatog privatnog ključa organizatora/administratora.

2.7.4. Sustav nema izravne reference na nesigurne objekte. Za tu je namjenu potrebno najmanje sljedeće:

(a) kod izravnih referenci na ograničene resurse aplikacija provjerava je li korisnik ovlašten pristupiti točno zatraženom resursu;

(b) kod neizravnih referenci mapiranje izravne reference ograničeno je na vrijednosti odobrene za trenutačnog korisnika.

2.7.5. Sustav štiti od krivotvorenja zahtjeva između stranica.

2.7.6. Postavljena je pravilna sigurnosna konfiguracija koja zahtijeva najmanje sljedeće:

(a) sve su softverske komponente ažurirane, uključujući operativni sustav, web/aplikacijski poslužitelj, sustav za upravljanje datotekama (DBMS), aplikacije i sve knjižnice kodova;

(b) onemogućene su, uklonjene ili nisu instalirane nepotrebne usluge operativnog sustava i web/aplikacijskog poslužitelja;

(c) promijenjene su ili onemogućene početne lozinke za račun;

(d) postavljeno je postupanje s pogreškama kako bi se spriječilo propuštanje tragova stoga ili drugih poruka o pogrešci s previše podataka;

(e) sigurnosne postavke u razvojnim okvirima i knjižnicama konfigurirane se u skladu s najboljim praksama kao što su smjernice OWASP-a.

2.7.7. Sustav osigurava kodiranje podataka kako slijedi:

(a) osobni podaci u elektroničkom obliku kodiraju se prilikom pohrane ili prijenosa nadležnim tijelima država članica u skladu s člankom 8. stavkom 1. Uredbe (EU) br. 211/2011 uz odvojeno upravljanje ključevima i njihovu sigurnosnu kopiju;

(b) snažni standardni algoritmi i snažni ključevi upotrebljavaju se u skladu s međunarodnim standardima. Uvedeno je upravljanje ključevima;

(c) lozinke se raspršuju pomoću snažnog standardnog algoritma i upotrebljava se odgovarajući proizvoljni niz znakova, tj. „salt”;

(d) svi ključevi i lozinke zaštićeni su od neovlaštenog pristupa.

2.7.8. Sustav ograničava pristup putem URL-a na temelju pristupnih razina i dozvola korisnika. Za tu je namjenu potrebno najmanje sljedeće:

(a) ako se upotrebljavaju vanjski sigurnosni mehanizmi za provjere autentikacije i odobrenja za pristup stranici, trebaju biti pravilno konfigurirani za svaku stranicu;

(b) ako se upotrebljava zaštita na razini koda, treba biti uvedena za svaku zatraženu stranicu.

2.7.9. Sustav upotrebljava dostatnu zaštitu prijenosnog sloja. Za tu su namjenu uvedene sve sljedeće mjere ili mjere barem jednake snage:

(a) sustav zahtijeva najnoviju verziju protokola za prijenos hipertekstualnih datoteka preko uspostavljene sigurne veze (HTTPS) za pristup svim osjetljivim resursima uz uporabu valjanih certifikata koji nisu istekli, nisu opozvani i koji odgovaraju svim domenama koje upotrebljava ta stranica;

(b) sustav označava sve osjetljive kolačiće kao „sigurne”;

(c) poslužitelj konfigurira davatelja usluga TLS-a tako da podržava samo algoritme za kodiranje u skladu s najboljim praksama. Korisnici su obaviješteni da moraju omogućiti podršku za TLS u svom pretraživaču.

2.7.10. Sustav štiti od neprovjerenih preusmjeravanja i prosljeđivanja.

Sigurnost baza podataka i cjelovitost podataka

2.8. Ako sustavi za online prikupljanje koji se upotrebljavaju za različite građanske inicijative dijele hardverske resurse i resurse operativnog sustava, oni ne razmjenjuju nikakve podatke, uključujući podatke o prijavi potrebne za pristup/kodiranje. Povrh toga, navedeno se odražava u procjeni rizika i provedenim protumjerama.

2.9. Smanjen je rizik da se prilikom autentikacije za pristup bazi podataka upotrijebi metoda „pass-the-hash".

2.10. Podacima koje su pružili potpisnici može pristupiti samo administrator baze podataka/organizator.

2.11. Administrativni podaci o korisnicima, osobni podaci prikupljeni od potpisnika i njihove sigurnosne kopije zaštićeni su snažnim algoritmima za kodiranje u skladu s točkom 2.7.7. podtočkom (b). Međutim, država članica u kojoj će se brojati izjave o potpori, datum podnošenja izjave o potpori i jezik na kojem je potpisnik popunio obrazac izjave o potpori mogu se pohraniti u nekodiranom obliku u sustavu.

2.12. Potpisnici imaju pristup dostavljenim podacima samo za vrijeme dok popunjavaju obrazac izjave o potpori. Nakon što podnesu obrazac izjave o potpori sjednica se zaključuje i podnesenim se podacima više ne može pristupiti.

2.13. Osobni podaci potpisnika dostupni su u sustavu, uključujući sigurnosnu kopiju, samo u kodiranom obliku. Za pregled podataka ili dobivanja odobrenja za podatke od nacionalnih tijela u skladu s člankom 8. Uredbe (EU) br. 211/2011 organizatori mogu izvesti kodirane podatke u skladu s točkom 2.7.7. podtočkom (a).

2.14. Podaci uneseni u obrazac izjave o potpori ne pohranjuju se zasebno. Drugim riječima, jednom kada je korisnik unio sve potrebne pojedinosti u obrazac izjave o potpori i potvrdio svoju odluku da želi poduprijeti inicijativu, sustav uspješno pohranjuje sve podatke iz obrasca u bazu podataka ili, u slučaju pogreške, ne pohranjuje ni jedan podatak. Sustav obavješćuje korisnika o uspjehu ili neuspjehu njegova zahtjeva.

2.15. Upotrijebljeni je DBMS ažuriran, a u slučaju novootkrivenih prijetnji stalno mu se dodaju zakrpe.

2.16. Uspostavljeni su dnevnici aktivnosti sustava. Sustav osigurava izradu nadzornih dnevnika u kojima se bilježe izuzeci i drugi događaji važni za sigurnost navedeni dolje i njihovo čuvanje dok se podaci ne unište u skladu s člankom 12. stavkom 3. ili 5. Uredbe (EU) br. 211/2011. Dnevnici su zaštićeni na odgovarajući način, na primjer pohranom na kodiranom mediju. Organizatori/administratori redovito provjeravaju dnevnike kako bi otkrili sumnjive aktivnosti. Sadržaj dnevnika uključuje najmanje:

(a) datume i vremena prijava i odjava organizatora/administratora;

(b) podatke o napravljenim sigurnosnim kopijama;

(c) sve promjene i ažurirane podatke u vezi s administratorom baze podataka.

Sigurnost infrastrukture – fizička lokacija, mrežna infrastruktura i okruženje poslužitelja

2.17. *Fizička sigurnost*

Bez obzira na vrstu smještaja, stroj u kojem je smještena aplikacija pravilno je zaštićen čime se osigurava:

(a) kontrola pristupa području u kojem je smještena aplikacija i nadzorni dnevnik;

(b) fizička zaštita podataka iz sigurnosne kopije od krađe ili slučajnog gubitka;

(c) postavljanje poslužitelja na kojem je smještena aplikacija u zaštićenom okviru.

2.18. *Sigurnost mreže*

2.18.1. Sustav je smješten na poslužitelju s internetskim sučeljem koji je postavljen u demilitariziranoj zoni (DMZ) i zaštićen vatrozidom.

2.18.2. Kada postanu dostupne javnosti, relevantne ažurirane verzije i zakrpe vatrozida instaliraju se što je prije moguće.

2.18.3. Sav dolazni i odlazni promet na poslužitelju (povezanom sa sustavom za online prikupljanje) pregledava se pravilima vatrozida i bilježi. Pravilima vatrozida sprečava se sav promet koji nije potreban za sigurnu uporabu sustava i njegovo upravljanje.

2.18.4. Sustav za online prikupljanje mora se smjestiti u proizvodnom mrežnom segmentu koji je zaštićen na odgovarajući način i odvojen od segmenata koji se upotrebljavaju za smještaj neproizvodnih sustava kao što su okruženja za razvoj i ispitivanje.

2.18.5. Uspostavljene su sigurnosne mjere za lokalnu mrežu (LAN) kao što su:

(a) popis pristupa sloju 2 (Layer 2 – L2)/sigurnost sklopke porta;

(b) onemogućavanje neupotrijebljenih sklopki porta;

(c) DMZ je u namijenjenoj virtualnoj lokalnoj mreži (VLAN)/LAN-u;

(d) na nepotrebnim portovima nije omogućeno usnopljavanje (trunking) L2.

2.19. *Sigurnost operativnog sustava i web/aplikacijskog poslužitelja*

2.19.1. Uspostavljena je pravilna sigurnosna konfiguracija uključujući elemente navedene u točki 2.7.6.

2.19.2. Aplikacije rade s najmanjim skupom povlastica potrebnim za rad.

2.19.3. Pristup administratora upravljačkom sučelju sustava za online prikupljanje ima kratko vremensko ograničenje sjednice (najviše 15 minuta).

2.19.4. Kada postanu javno dostupne, relevantne ažurirane verzije i zakrpe operativnog sustava, trajanja rada aplikacija na poslužiteljima, aplikacija koje rade na poslužiteljima ili softvera za zaštitu od štetnih programa postavljaju se što je prije moguće.

2.19.5. Smanjen je rizik da se prilikom autentikacije za pristup sustavu upotrijebi metoda „pass-the-hash".

2.20. *Sigurnost klijenata organizatora*

Radi osiguravanja sigurnosti s kraja na kraj mreže, organizatori poduzimaju potrebne mjere kako bi zaštitili svoje klijentske aplikacije/uređaje koje upotrebljavaju za upravljanje sustavom za online prikupljanje i pristup tom sustavu kao što su:

2.20.1. korisnici provode zadatke koji nisu vezani uz održavanje (kao što je uredska automatizacija) s najmanjim skupom povlastica potrebnim za njihovu provedbu;

2.20.2. kada postanu javno dostupne, relevantne ažurirane verzije i zakrpe operativnog sustava, svih instaliranih aplikacija ili softvera za zaštitu od štetnih programa postavljaju se što je prije moguće.

3. TEHNIČKE SPECIFIKACIJE ČIJI JE CILJ PROVEDBA ČLANKA 6. STAVKA 4. TOČKE (c) UREDBE (EU) br. 211/2011

3.1. Sustav pruža mogućnost izrade izvješća za svaku pojedinačnu državu članicu u kojem se navode inicijativa i osobni podaci potpisnika, pod uvjetom da ih provjeri nadležno tijelo države članice.

3.2. Izjave o potpori potpisnika mogu se izvesti u obliku Priloga III. Uredbi (EU) br. 211/2011. Sustav može pružiti dodatnu mogućnost izvoza izjava o potpori u interoperativnom obliku kao što je jezik za označivanje podataka (XML).

3.3. Izvezene izjave o potpori označene su za *ograničenu distribuciju* dotičnim državama članicama i kao *osobni podaci*.

3.4. Elektronički prijenos izvezenih podataka državama članicama zaštićen je od prisluškivanja prikladnim kodiranjem s kraja na kraj mreže.