II

(Nelegislativní akty)

NAŘÍZENÍ

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) č. 1179/2011

ze dne 17. listopadu 2011,

kterým se stanoví technické specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 211/2011 o občanské iniciativě

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 211/2011 ze dne 16. února 2011 o občanské iniciativě [1], a zejména na čl. 6 odst. 5 uvedeného nařízení,

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

(1) Nařízení (EU) č. 211/2011 stanoví, že pokud se prohlášení o podpoře sbírají online, systém použitý k tomuto účelu musí splňovat určité bezpečnostní a technické požadavky a musí mít potvrzení od příslušného orgánu dotčeného členského státu.

(2) Online systém sběru ve smyslu nařízení (EU) č. 211/2011 je informační systém, který se skládá ze softwaru, hardwaru, hostitelského prostředí, pracovních postupů a personálu a jehož cílem je provádět online sběr prohlášení o podpoře.

(3) Nařízení (EU) č. 211/2011 vymezuje požadavky, které musí online systémy sběru splňovat, aby dostaly potvrzení, a stanoví, že Komise by měla přijmout technické specifikace k provedení těchto požadavků.

(4) Projekt Top 10 2010 neziskového sdružení OWASP (Open Web Application Security Project) poskytuje přehled nejvážnějších bezpečnostních rizik webových aplikací a nástrojů k řešení těchto rizik; technické specifikace proto vycházejí ze závěrů tohoto projektu.

(5) Provedení technických specifikací ze strany organizátorů by mělo zaručit, že orgány členských států potvrdí online systémy sběru, a mělo by pomoci zajistit provádění příslušných technických a organizačních opatření potřebných ke splnění povinností stanovených směrnicí Evropského parlamentu a Rady 95/46/ES [2] o bezpečnosti zpracování jak v době, kdy se systém zpracovávání navrhuje, tak v době samotného zpracování, aby se udrželo zabezpečení, předešlo se neoprávněnému zpracovávání a aby byla zajištěna ochrana osobních údajů před náhodným nebo nezákonným zničením či náhodnou ztrátou, změnou, neoprávněným odhalením nebo přístupem.

(6) Využívání softwaru poskytnutého Komisí v souladu s článkem 6 odst. 2 nařízení (EU) č. 211/2011 ze strany organizátorů by mělo usnadnit postup vydávání potvrzení.

(7) Organizátoři občanských iniciativ by coby správci údajů měli při online sběru prohlášení o podpoře provádět technické specifikace stanovené v tomto nařízení s cílem zajistit ochranu zpracovávaných osobních údajů. Pokud zpracovávání provádí zpracovatel, organizátoři by měli zajistit, aby zpracovatel postupoval jen na základě pokynů organizátorů a aby prováděl technické specifikace stanovené v tomto nařízení.

(8) Toto nařízení dodržuje základní práva a ctí zásady uznávané Listinou základních práv Evropské unie, zejména článek 8 uvedené listiny, který stanoví, že každý má právo na ochranu osobních údajů, které se ho týkají.

(9) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 20 nařízení (EU) č. 211/2011,

[1] Úř. věst. L 65, 11.3.2011, s. 1.

[2] Úř. věst. L 281, 23.11.1995, s. 31.

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Technické specifikace uvedené v čl. 6 odst. 5 nařízení (EU) č. 211/2011 jsou stanoveny v příloze.

Článek 2

Toto nařízení vstupuje v platnost dvacátý den po jeho vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 17. listopadu 2011.

Za Komisi

José Manuel BARROSO

předseda

PŘÍLOHA

1. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 6 ODST. 4 PÍSM. a) NAŘÍZENÍ (EU) č. 211/2011

Aby se zabránilo automatizovanému podávání prohlášení o podpoře s využitím systému, absolvuje v souladu se současnou praxí signatář před podáním prohlášení o podpoře řádný proces ověřování. Jedním z možných způsobů ověřování je využití účinného testu „captcha".

2. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 6 ODST. 4 PÍSM. b) NAŘÍZENÍ (EU) č. 211/2011

Normy zajištění informací

2.1 Organizátoři předloží dokumentaci, která prokazuje, že splňují požadavky normy ISO/IEC 27001 i bez jejího přijetí. Za tímto účelem musí:

a) provést úplné hodnocení rizika, v němž určí rozsah systému, objasní hospodářské dopady v případě různých porušení zabezpečení informací, uvedou rizika a slabé stránky informačního systému, vypracují dokument s analýzou rizika, v němž budou uvedeny také protiopatření na zabránění takovým rizikům a prostředky nápravy, které budou přijaty v případě výskytu rizika, a na závěr vypracují seznam zdokonalení v upřednostňovaném pořadí;

b) navrhnout a realizovat opatření na řešení rizik souvisejících s ochranou osobních údajů a ochranou rodinného a soukromého života, a opatření, která budou přijata v případě výskytu rizika;

c) v písemné formě pojmenovat další rizika;

d) zajistit organizační prostředky k získání zpětné vazby, co se týče nových hrozeb a vylepšení bezpečnosti.

2.2 Organizátoři si zvolí bezpečnostní kontroly na základě analýzy rizika uvedené v bodě 2.1 písm. a) z těchto norem:

1. ISO/IEC 27002 nebo

2. „Zásady řádné praxe" Fóra informační bezpečnosti

k řešení těchto věcí:

a) hodnocení rizik (doporučuje se ISO/IEC 27005 nebo jiná specifická a vhodná metoda posuzování rizik);

b) fyzická a environmentální bezpečnost;

c) bezpečnost z hlediska lidských zdrojů;

d) komunikace a řízení provozu;

e) standardní opatření ke kontrole přístupu jako doplněk k opatřením uvedeným v tomto prováděcím nařízení;

f) akvizice, vývoj a údržba informačních systémů;

g) zvládání incidentů v oblasti bezpečnosti informací;

h) opatření k nápravě a zmírnění narušení informačních systémů, které by vedly ke zničení nebo náhodné ztrátě, změně zpracovávaných osobních údajů, jejich neoprávněnému odhalení nebo přístupu k nim;

i) soulad;

j) bezpečnost počítačové sítě (doporučuje se ISO/IEC 27033 nebo Zásady řádné praxe).

Uplatňování těchto norem se může omezovat jen na části organizace, které souvisejí s online systémem sběru. Například zabezpečení lidských zdrojů se může omezovat na personál, který má fyzický nebo síťový přístup k online systému sběru, a fyzická/environmentální bezpečnost se může omezovat na budovy, v nichž se systém nachází.

Funkční požadavky

2.3 Online systém sběru se skládá z webové aplikace vytvořené za účelem sběru prohlášení o podpoře pro jednu občanskou iniciativu.

2.4 Jestliže správa systému vyžaduje různé role, vytvoří se různé úrovně přístupu podle zásady nejnižších práv.

2.5 Veřejně přístupné funkce jsou jasně odděleny od funkcí určených pro správu. Kontrola přístupu nebrání čtení informací dostupných ve veřejné části systému včetně informací o iniciativě a o elektronickém formuláři prohlášení o podpoře. Připojení se k iniciativě je možné pouze přes veřejně přístupnou část.

2.6 Systém rozeznává podání duplicitního prohlášení o podpoře a zabraňuje mu.

Bezpečnost na úrovni aplikace

2.7 Systém je vhodně zabezpečený, pokud jde o známe slabé stránky a zneužití. Za tímto účelem splňuje kromě jiného tyto požadavky:

2.7.1 Systém je zajištěn proti injektování kódů (*injection flaws*), jako jsou dotazy v jazyce SQL (*Structured Query Language*), dotazy LDAP (*Lightweight Directory Access Protocol*), dotazy XPath (*XML Path Language*), příkazy operačního systému (OS) nebo argumenty programu. Za tímto účelem je minimálně potřebné, aby:

a) všechny vstupy uživatelů byly ověřovány;

b) se ověřování provádělo nejméně s pomocí logiky na straně serveru;

c) použití jakýchkoli interpretačních překladačů jasně oddělovalo nedůvěryhodné údaje od příkazu nebo dotazu. V případě volání SQL to znamená použít přiřazené proměnné ve všech připravených prohlášeních a uložených procedurách a vyhnout se dynamickým dotazům.

2.7.2 Systém je zajištěn proti XSS (Cross-Site Scripting). Za tímto účelem je minimálně potřebné, aby:

a) všechny zadané vstupy uživatelů poslané zpět do prohlížeče byly ověřovány, pokud jde o jejich bezpečnost (prostřednictvím kontroly vstupních parametrů);

b) všechny vstupy uživatelů byly řádně vráceny do povelové úrovně před jejich začleněním do stránky výstupu;

c) náležité kódování výstupu zajišťuje, aby prohlížeč takové vstupy vždy považoval za text. Nepoužívá se žádný aktivní obsah.

2.7.3 Systém má silné ověřování totožnosti a řízení relací, což minimálně vyžaduje, aby:

a) identifikační údaje byly při ukládání vždy chráněny pomocí hašování nebo šifrování. riziko, že se někdo identifikuje pomocí „pass-the-hash“, bylo minimalizováno;

b) identifikační údaje se nedaly uhodnout nebo přepsat kvůli slabým funkcím správy účtu (např. vytvoření účtu, změna hesla, získání zapomenutého hesla, slabé identifikátory relace (ID));

c) identifikátory relace a údaje o relaci se nezobrazovaly v URL (*Uniform Resource Locator*);

d) identifikátory relace byly odolné vůči útokům pomocí fixace relací (*session fixation*);

e) časový limit identifikátorů relace zajistil odhlášení uživatelů;

f) identifikátory relace po úspěšném přihlášení nemohly rotovat;

g) hesla, identifikátory relace a další identifikační údaje se zasílaly jen prostřednictvím TLS (*Transport Layer Security*);

h) administrativní část systému byla chráněna. Pokud je chráněna jednofaktorovou identifikací, obsahuje heslo minimálně 10 znaků, mezi nimiž je nejméně jedno písmeno, jedna číslice a jeden speciální znak. Případně se může použít dvoufaktorová identifikace. V případě, že se použije pouze jednofaktorová identifikace, zahrnuje tento postup dvoustupňový mechanismus ověřování pro přístup k administrativní části systému přes Internet, v němž se jeden faktor rozšíří o další prostředky identifikace, například o jednorázovou kontrolní větu/kód přes SMS nebo asymetricky zašifrovaný náhodný řetězec (challenge string), který se dešifruje s pomocí osobního klíče organizátora/správce, který systém nezná.

2.7.4 Systém nemá nezajištěné odkazy na přímé objekty. Za tímto účelem je minimálně potřebné, aby:

a) v případě přímých odkazů na omezené zdroje aplikace ověřila, zda má uživatel autorizovaný přístup k přesně požadovanému zdroji;

b) jestliže je odkaz nepřímý, mapování k přímému odkazu bylo omezeno na hodnoty povolené pro aktuálního uživatele.

2.7.5 Systém musí být zajištěn proti zneužití oprávněných dotazů (*cross-site request forgery flaw*).

2.7.6 K dispozici je náležitá konfigurace zajištění, což přinejmenším vyžaduje, aby:

a) všechny komponenty programového vybavení byly aktuální včetně OS, webového serveru/serveru aplikace, databázového systému (DBMS), aplikací a všech knižnic kódů;

b) nepotřebné funkce OS a webového serveru/serveru aplikace byly vypnuty, vymazány nebo nebyly nainstalovány;

c) implicitně nastavená hesla k účtu se změnila nebo zablokovala;

d) zpracování chyb bylo nastaveno tak, aby zabránilo úniku tzv. *stack traces* a jiných příliš informativních chybových hlášení;

e) nastavení bezpečnostních parametrů ve vývojových strukturách a knihovnách bylo nakonfigurováno v souladu s osvědčenými postupy, například s pokyny OWASP.

2.7.7 Systém umožňuje takovéto šifrování údajů:

a) Osobní údaje v elektronickém formátu jsou šifrovány při ukládání nebo odesílání příslušným orgánům členských států v souladu s čl. 8 odst. 1 nařízení (EU) č. 211/2011, přičemž klíče se spravují a zálohují odděleně.

b) Odolné standardní algoritmy a odolné klíče se používají v souladu s mezinárodními normami. K dispozici je správa klíčů.

c) Hesla jsou hašována s pomocí odolného standardního algoritmu a používá se vhodný náhodný řetězec (salt).

d) Všechny klíče a hesla jsou chráněny před neoprávněným přístupem.

2.7.8 Systém omezuje přístup URL na základě přístupových úrovní uživatelů a jejich oprávnění. Za tímto účelem je minimálně potřebné, aby:

a) pokud se k zajištění kontroly identifikace a autorizace za účelem přístupu na stránku používají externí bezpečnostní mechanismy, byly náležitě nakonfigurovány pro každou stránku.

b) Pokud se používá ochrana na základě úrovně kódu, musí být k dispozici pro každou požadovanou stránku.

2.7.9 Systém využívá dostatečnou ochranu Transport Layer Protection. Za tímto účelem jsou k dispozici všechna tato opatření nebo minimálně stejně silná opatření:

a) Systém vyžaduje nejnovější verzi HTTPS (Hypertext Transfer Protocol Secure) pro přístup ke všem citlivým zdrojům s použitím certifikátů, které jsou platné, neskončila jim platnost, nebyly odvolány a odpovídají všem doménám, které stránka používá.

b) Systém označuje všechny citlivé soubory *cookies* jako bezpečné.

c) Server nakonfiguruje poskytovatele TLS tak, aby podporoval jen šifrovací algoritmy, které odpovídají osvědčeným postupům. Uživatelé jsou informováni, že musí ve svém prohlížeči umožnit podporu TLS.

2.7.10 Systém poskytuje ochranu proti zrušeným přesměrováním a převodům (forwards).

Bezpečnost databáze a integrita údajů

2.8 Pokud online systémy sběru, používané pro různé občanské iniciativy, sdílejí společné zdroje hardwaru a zdroje operačního systému, nesmí sdílet žádné údaje, a to ani přístupové/šifrovací údaje. Promítne se to také v hodnocení rizika a přijatých protiopatření.

2.9 Riziko, že se někdo identifikuje v databázi pomocí „pass-the-hash", je minimalizováno.

2.10 Údaje, které signatáři poskytnou, jsou přístupné jen pro správce databáze/organizátora.

2.11 Identifikační údaje správce, osobní údaje získané od signatářů a jejich záložní kopie jsou zajištěny s pomocí odolných šifrovacích algoritmů v souladu s bodem 2.7.7 písm. b). V systému však mohou zůstat uloženy tyto nezašifrované údaje: členský stát, jehož se týká prohlášení o podpoře, datum podání prohlášení o podpoře a jazyk, v němž signatář vyplnil prohlášení o podpore.

2.12 Signatáři mají k poskytnutým údajům přístup pouze v průběhu relace, v níž vyplňují formulář prohlášení o podpoře. Po podání prohlášení o podpoře uvedená relace skončí a poskytnuté údaje už nejsou přístupné.

2.13 Osobní údaje signatářů jsou v systému, včetně záložních kopií, dostupné pouze v zašifrovaném formátu. Za účelem konzultací o údajích nebo vydání osvědčení ze strany příslušných orgánů v souladu s článkem 8 nařízení (EU) č. 211/2011 mohou organizátoři exportovat šifrované údaje v souladu s bodem 2.7.7 písm. a).

2.14 Stálost údajů vložených do formuláře prohlášení o podpoře musí být atomická. To znamená, že poté, co uživatel do formuláře prohlášení o podpoře vložil všechny požadované údaje a potvrdil své rozhodnutí podpořit iniciativu, systém buď úspěšně vloží všechny údaje z formuláře do databáze, nebo v případě chyby neuloží žádné údaje. Systém informuje uživatele o úspěchu nebo neúspěchu jeho požadavku.

2.15 Používaný databázový systém musí být aktuální a musí se neustále vylepšovat o nové prvky.

2.16 Všechny aktivity systému se protokolují. Systém zajistí, aby se kontrolní záznamy se zapsanými výjimkami a dalšími níže uvedenými bezpečnostními událostmi mohly vytvořit a uchovávat, dokud tyto údaje nebudou zničeny v souladu s čl. 12 odst. 3 nebo 5 nařízení (EU) č. 211/2011. Záznamy jsou náležitě chráněny, například jejich uložením na zašifrovaných nosičích. Organizátoři/správci pravidelně kontrolují záznamy v souvislosti s podezřelou aktivitou. Minimální obsah záznamů:

a) datum a čas přihlášení a odhlášení organizátorů/správců;

b) vytvořené záložní kopie;

c) všechny změny a aktualizace správce databáze.

Bezpečnost infrastruktury – fyzické umístění, síťová infrastruktura a prostředí serveru

2.17 *Fyzická bezpečnost*

Bez ohledu na typ použitého hostitelství je technické zařízení, které je hostitelem aplikace, náležitě chráněno, což znamená:

a) kontrola přístupu k oblasti hostování a kontrolní záznam;

b) fyzická ochrana zálohovaných údajů před krádeží nebo náhodným nesprávným umístěním;

c) server, který je hostitelem aplikace, je nainstalován v zajištěném rámu.

2.18 *Bezpečnost sítí*

2.18.1 Systém je umístěn na internetovém serveru nainstalovaném v demilitarizované zóně a je chráněn s pomocí systému Firewall.

2.18.2 Po zveřejnění příslušných aktualizací a oprav produktu Firewall jsou tyto neprodleně nainstalovány.

2.18.3 Všechny přenosy na server a ze serveru (určené pro online systém sběru) jsou kontrolovány podle pravidel systému Firewall a protokolují se. Pravidla systému Firewall odmítají všechny přenosy, které nejsou potřebné k bezpečnému používání a správu systému.

2.18.4 Online systém sběru musí být umístěn v řádně zabezpečeném produkčním segmentu sítě, který je oddělen od ostatních segmentů používaných k umístění neprodukčních systémů, například k vývoji nebo testování.

2.18.5 Musí být zavedena bezpečnostní opatření pro lokální počítačovou síť (LAN), například:

a) seznam přístupů na úrovni 2 (L2)/bezpečnost přepínače rozhraní (port switch);

b) nevyužité přepínače rozhraní (switch ports) jsou zablokovány;

c) DMZ je umístěna na vyhrazené virtuální lokální počítačové síti (Virtual Local Area Network (VLAN)/LAN);

d) seskupení kanálů (trunking) na úrovni L2 se neumožňuje na nepotřebných portech.

2.19 *Bezpečnost OS a webového serveru/serveru aplikace*

2.19.1 Je zajištěna přiměřená konfigurace bezpečnosti včetně prvků uvedených v bodě 2.7.6.

2.19.2 Aplikace fungují s nejnižší sadou privilegií, která potřebují ke své funkčnosti.

2.19.3 Přístup správce k rozhraní správy online systému sběru má krátký časový limit (maximálně 15 minut).

2.19.4 Příslušné aktualizace a opravy OS, runtime aplikací, aplikací běžících na serveru nebo aplikací proti škodlivému softwaru, musí být bezodkladně nainstalovány po jejich zveřejnění.

2.19.5 Riziko, že se někdo identifikuje v systému pomocí „pass-the-hash“, je minimalizováno.

2.20 *Bezpečnost klienta organizátora*

K zajištění bezpečnosti po celé délce spojení přijmou organizátoři nezbytná opatření k tomu, aby zajistili svou klientskou aplikaci/své klientské technické zařízení, které používají k řízení online systému sběru a k přístupu do tohoto systému, například:

2.20.1 Uživatelé mohou používat neúdržbové funkce (jako například automatizace administrativy) s nejnižší sadou privilegií potřebných k jejich funkčnosti.

2.20.2 Bezodkladně po zveřejnění příslušných aktualizací a oprav OS, instalovaných aplikací nebo programů proti malwaru jsou tyto nainstalovány.

3. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 6 ODST. 4 PÍSM. c) NAŘÍZENÍ (EU) č. 211/2011

3.1 Systém poskytuje možnost extrahovat pro jednotlivé členské státy zprávu, v níž bude uvedena iniciativa a osobní údaje signatářů, které podléhají ověření ze strany příslušného orgánu daného členského státu.

3.2 Prohlášení signatářů o podpoře se mohou exportovat ve formátu přílohy III nařízení č. 211/2011. Systém může kromě toho poskytnout možnost exportovat prohlášení o podpoře v interoperabilním formátu, například v Extensible Markup Language (XML).

3.3 Exportovaná prohlášení o podpoře jsou označena jako *omezená distribuce* pro příslušný členský stát a jako *osobní údaje*.

3.4 Elektronický přenos exportovaných údajů pro členské státy se zabezpečí před „odposlechem“ s pomocí vhodného zašifrování po celé délce spojení.