II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) № 1179/2011 НА КОМИСИЯТА

от 17 ноември 2011 година

относно определяне на технически спецификации за системите за събиране на изявления за подкрепа онлайн по силата на Регламент (ЕС) № 211/2011 на Европейския парламент и на Съвета относно гражданската инициатива

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 211/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. относно гражданската инициатива [1], и по-специално член 6, параграф 5 от него,

след като се консултира с Европейския надзорен орган по защита на данните,

като има предвид, че:

(1) Регламент (ЕС) № 211/2011 предвижда, че когато изявления за подкрепа се събират по електронен път, системата, използвана за тази цел, трябва да удовлетворява някои изисквания за сигурност и технически изисквания и трябва да бъде удостоверена от компетентния орган на съответната държава-членка.

(2) Система за събиране на изявления за подкрепа онлайн по смисъла на Регламент (ЕС) № 211/2011 е информационна система, състояща се от софтуер, хардуер, хостинг среда, бизнес процеси и служители за изпълнение на събирането на изявления за подкрепа онлайн.

(3) В Регламент (ЕС) № 211/2011 се определят изискванията, на които трябва да отговарят системите за събиране на изявления за подкрепа онлайн с цел да бъдат удостоверени, и се предвижда, че Комисията следва да приеме технически спецификации за прилагането на тези изисквания.

(4) Проект Top 10 2010 на OWASP (Open Web Application Security Project) предоставя преглед на най-критичните рискове за сигурността на уебприложения, както и инструменти за справяне с тези рискове; ето защо техническите спецификации се основават на констатациите от този проект.

(5) Прилагането от страна на организаторите на техническите спецификации следва да гарантира удостоверяването на системите за събиране на изявления за подкрепа онлайн от страна на органите на държавите-членки и да допринася за гарантиране на прилагането на подходящите технически и организационни мерки, необходими за изпълнението на задълженията, наложени от Директива 95/46/ЕО на Европейския парламент и на Съвета [2] за сигурността на дейностите по обработването на данни, както при разработването на системата за обработка на данни, така и по време на самата обработка, с цел да се запази сигурността и по този начин да се предотврати неразрешена обработка и да се защитят личните данни срещу случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп.

(6) Процесът на удостоверяване следва да се улесни, като организаторите използват софтуера, предоставен от Комисията в съответствие с член 6, параграф 2 от Регламент (ЕС) № 211/2011.

(7) Организаторите на граждански инициативи, като администратори на данни, следва, когато събират изявления за подкрепа онлайн, да прилагат техническите спецификации, определени в настоящия регламент, с цел гарантиране на защитата на личните данни, които се обработват. Когато обработката се извършва от подизпълнител, организаторите следва да гарантират, че подизпълнителят действа единствено според указанията на организаторите и че изпълнява техническите спецификации, определени в настоящия регламент.

(8) Настоящият регламент зачита основните права и спазва принципите, залегнали в Хартата на основните права на Европейския съюз, и по-специално член 8 от нея, съгласно който всеки има право на защита на своите лични данни.

(9) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, учреден съгласно член 20 от Регламент (ЕС) № 211/2011,

[1] ОВ L 65, 11.3.2011 г., стр. 1.

[2] ОВ L 281, 23.11.1995 г., стр. 31.

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Техническите спецификации, посочени в член 6, параграф 5 от Регламент (ЕС) № 211/2011, са определени в приложението.

Член 2

Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави-членки.

Съставено в Брюксел на 17 ноември 2011 година.

За Комисията
Председател
José Manuel BARROSO

ПРИЛОЖЕНИЕ

1. ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ, НАСОЧЕНИ КЪМ ПРИЛАГАНЕ НА ЧЛЕН 6, ПАРАГРАФ 4, БУКВА а) ОТ РЕГЛАМЕНТ (ЕС) № 211/2011

С цел да се предотврати автоматизирано внасяне на изявление за подкрепа посредством системата, поддръжникът преминава адекватен процес на проверка в съответствие с настоящата практика преди внасянето на изявление за подкрепа. Възможен процес на проверка може да бъде използването на сложни „captcha“.

2. ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ, НАСОЧЕНИ КЪМ ПРИЛАГАНЕ НА ЧЛЕН 6, ПАРАГРАФ 4, БУКВА б) ОТ РЕГЛАМЕНТ (ЕС) № 211/2011

Стандарти за осигуреност на информацията

2.1. Организаторите предоставят документи, доказващи, че те отговарят на изискванията на стандарт ISO/IEC 27001, без да се налага да бъдат сертифицирани. За целта те:

а) са извършили пълна оценка на риска, с която се определя обхватът на системата, изтъква се отражението върху бизнеса в случай на различни нарушения по отношение на осигуреността на информацията, изброяват се заплахите и уязвимостта на информационната система, изготвя се документ за анализ на риска, в който се съдържа също така списък с мерки за противодействие, за да се избегнат такива заплахи, както и решения, които ще бъдат приложени, ако се появи заплаха, и накрая се изготвя списък с приоритизиране на подобренията;

б) са разработили и въвели мерки за справяне с рисковете по отношение на защитата на личните данни и защитата на семейния и личния живот и мерки, които да се предприемат в случай на риск;

в) са идентифицирали остатъчните рискове в писмен вид;

г) са предвидили от организационна гледна точка начини за получаване на обратна информация за нови заплахи и подобрения на сигурността.

2.2. Въз основа на анализа на риска, посочен в точка 2.1, буква а), организаторите подбират проверки на сигурността измежду следните стандарти:

1) ISO/IEC 27002; или

2) „стандарта за добра практика“ на форума на информационната сигурност,

за да обърнат внимание на следните въпроси:

а) оценки на риска (препоръчват се ISO/IEC 27005 или друга специфична и подходяща методология за оценка на риска);

б) физическа сигурност и сигурност на средата;

в) сигурност на човешките ресурси;

г) управление на комуникациите и операциите;

д) стандартни мерки за контрол на достъпа, в допълнение към тези, посочени в настоящия регламент за изпълнение;

е) придобиване, разработване и поддръжка на информационни системи;

ж) управление на инцидентите, свързани със сигурността на информацията;

з) мерки за разрешаване и намаляване на пропуски в информационните системи, които биха довели до унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни;

и) спазване на стандарти;

й) сигурност на компютърната мрежа (препоръчват се ISO/IEC 27033 или SoGP).

Прилагането на тези стандарти може да бъде ограничено до тези части на организацията, които са от значение за системата за събиране на изявления за подкрепа онлайн. Например сигурността, свързана с човешките ресурси, може да бъде ограничена до персонала, който има физически достъп или мрежови достъп до системата за събиране на изявления за подкрепа онлайн, а физическата сигурност и сигурността на средата могат да бъдат ограничени до сградата/-ите, в която/-ито се помещава системата.

Функционални изисквания

2.3. Системата за събиране на изявления за подкрепа онлайн се състои от уеб-базирана програма, създадена за целите на събирането на изявления за подкрепа за една единствена гражданска инициатива.

2.4. Ако управлението на системата изисква различни роли, тогава се създават различни нива на контрол на достъпа съгласно принципа на най-малко привилегии.

2.5. Обществено достъпните елементи са ясно отделени от елементите, предназначени за административни цели. Нито един от типовете контрол на достъпа не затруднява четенето на наличната информация в публично достъпната част на системата, включително информацията за инициативата и електронния формуляр за изявление за подкрепа. Участието в инициативата е възможно само чрез тази публично достъпна зона на системата.

2.6. Системата открива и предотвратява подаването на дублирани изявления за подкрепа.

Сигурност на етапа на програмата

2.7. Системата е защитена по подходящ начин срещу известни слаби места и атаки от вид *exploits*. За тази цел системата удовлетворява, *inter alia*, следните изисквания:

2.7.1. Системата предпазва срещу вливане на информация като заявки чрез Structured Query Language (SQL) („език за структурирани запитвания“), заявки чрез Lightweight Directory Access Protocol (LDAP) (мрежови протокол, проектиран да работи с TCP/IP, за извличане на информация от йерархична директория), заявки чрез XML Path Language (XPath) (XML език за адресиране на елементите на един XML документ чрез задаване на пътека посредством структурата на документа), команди или програмни аргументи на операционната система. За тази цел е необходимо удовлетворяването на най-малко следните изисквания:

а) валидиране на цялата входна информация на потребителя;

б) валидирането се извършва поне по логиката от страната на сървъра;

в) всяко използване на интерпретатори ясно разделя ненадеждни данни от командата или заявката. За инструкции SQL това означава използване на обвързани променливи (bind variables) във всички изготвени изявления и съхранени процедури, както и избягване на динамични заявки.

2.7.2. Системата предпазва срещу Cross-Site Scripting (XSS) (писане на скриптове между различни сайтове). За тази цел е необходимо удовлетворяването на най-малко следните изисквания:

а) сигурността на цялата предоставена потребителска входна информация, изпратена обратно към браузъра, е потвърдена (чрез валидиране на входната информация);

б) цялата входна информация на потребителя е предмет на правилна операция *escape*, преди да бъде включена в страницата с изходна информация;

в) правилното кодиране на изходната информация гарантира, че изходната информация е обработена като текст в браузъра. Не се използва никакво активно съдържание.

2.7.3. Системата има прецизно управление на автентикацията и сесията, за което е необходимо удовлетворяването на най-малко следните изисквания:

а) удостоверението за самоличността е винаги защитено, когато се съхранява чрез използване на хеширане или криптиране. Намаляване на риска от това някой да удостовери самоличността си като използва атака от вида „pass-the-hash“;

б) удостоверението за самоличността не може да бъде оттатнато или написано повторно чрез слаби функции за управление на акаунта (например създаване на акаунт, промяна на парола, възстановяване на парола, слаби идентификатори на сесията (IDs);

в) идентификаторите на сесията и данните за сесията не са посочени в унифицирания локатор на ресурс (Uniform Resource Locator (URL);

г) идентификаторите на сесията не са уязвими спрямо атаки за фиксиране на сесията;

д) наличие на таймаут на идентификаторите на сесията, с което се гарантира, че потребителите напускат програмата;

е) идентификаторите на сесията не могат да бъдат повторно генерирани след успешно включване в програмата;

ж) пароли, идентификатори на сесия и други удостоверения за самоличността се изпращат единствено чрез Transport Layer Security (TLS) (стандартен протокол за осигуряване на сигурни уеб комуникации);

з) административната част на системата е защитена. Ако тя е защитена чрез автентикация с един фактор, тогава паролата се състои от минимум 10 знака, включително най-малко една буква, една цифра и един специален знак. Другата възможност е да бъде използвана автентикация с два фактора. Когато се използва единствено автентикация с един фактор, това включва двустепенен механизъм за проверка за достъп до административната част на системата чрез интернет, в който единственият фактор се подсилва с други средства за автентикация като еднократна тайна фраза/еднократен код, изпратени чрез SMS съобщения, или асиметрично криптирана случайна поредица от данни за получаване на достъп, която се разкодира чрез непознат за системата частен ключ на организаторите/администраторите.

2.7.4. Системата няма незащитени директни препратки към даден обект. За тази цел е необходимо удовлетворяването на най-малко следните изисквания:

а) за директни препратки към защитени ресурси, програмата проверява дали потребителят има разрешен достъп за точно този ресурс;

б) ако препратката е косвена, асоциирането с пряка препратка е ограничено до стойности, разрешени за съответния потребител.

2.7.5. Системата е защитена срещу подправяне на искане между различни сайтове.

2.7.6. Наличие на правилна конфигурация за сигурността, за което е необходимо удовлетворяването на най-малко следните изисквания:

а) всички софтуерни компоненти да бъдат актуални, включително оперативната система, уеб сървъра, приложния сървър, системата за управление на бази данни (Data Base Management System (DBMS), програмите и всички библиотеки с кодове;

б) ненужните услуги на оперативната система, уеб сървъра и приложния сървър са деактивирани, отстранени или не са инсталирани;

в) подразбиращите се пароли за акаунт са променени или деактивирани;

г) въведена е система за обработка на грешки за предотвратяване на изтичането на чувствителна информация поради следи от стек и други прекалено информативни съобщения за грешка;

д) настройките за сигурност в рамките за разработка и библиотеките са конфигурирани в съответствие с най-добрите практики, като например насоките на Open Web Application Security Project (OWASP).

2.7.7. В системата е предвидено криптиране на данни, както следва:

а) личните данни в електронен формат се криптират при съхраняване или прехвърляне до компетентните органи на държавите-членки в съответствие с член 8, параграф 1 от Регламент (ЕС) № 211/2011, като ключовете се управляват и архивират отделно;

б) използват се сложни стандартни алгоритми и сложни ключове в съответствие с международните стандарти. Налице е управление на ключовете;

в) паролите са хеширани със сложен стандартен алгоритъм и се използва подходяща инициализация;

г) всички ключове и пароли са защитени срещу неразрешен достъп.

2.7.8. Системата ограничава достъпа до URL съобразно нивата за достъп и разрешителните на потребителя. За тази цел е необходимо удовлетворяването на най-малко следните изисквания:

а) ако се използват външни механизми за сигурност за проверки на самоличността и на разрешителните за достъп до интернет страници, те трябва да бъдат правилно конфигурирани за всяка страница;

б) ако се използва защита на равнище на кода, такава защита трябва да има за всяка поискана страница.

2.7.9. Системата използва достатъчно Transport Layer Protection. За тази цел са налице всички от следните мерки или други мерки, които имат поне равностойна сила:

а) системата изисква най-новата версия на Hypertext Transfer Protocol Secure (HTTPS) за достъп до всякакви чувствителни ресурси посредством сертификати, които са валидни, не са с изтекъл срок на валидност, не са отменени и съответстват на всички домейни, използвани от сайта;

б) системата определя „сигурен“ флаг („secure“ flag) за всички блокове с чувствителни данни (cookies);

в) сървърът конфигурира протокола TLS, за да го използва само за поддръжка на алгоритми за криптиране в съответствие с най-добрите практики. Потребителите са информирани за това, че трябва да активират помощния TLS в техния браузър.

2.7.10. Системата е защитена срещу невалидирано пренасочване и препращане.

Сигурност на базата данни и цялост на данните

2.8. Когато системите за събиране на изявления за подкрепа онлайн за различни граждански инициативи делят хардуерни ресурси и оперативни системи, те не споделят никакви данни, нито удостоверения за самоличност за достъп/криптиране. В допълнение, това е отразено в оценката на риска и на прилаганите мерки за противодействие.

2.9. Намален е рискът от това някой да удостовери самоличността си в базата данни, като използва атака от вид „pass-the-hash“.

2.10. Данните, предоставени от поддръжниците, са достъпни само за администратора/организатора на базата данни.

2.11. Административното удостоверение за самоличността, личните данни, събрани от поддръжниците, и съхраняването им са защитени със сложни алгоритми за криптиране в съответствие с точка 2.7.7, буква б). Въпреки това държавата-членка, в която изявлението за подкрепа ще бъде отчетено, датата на внасяне на изявление за подкрепа и езикът, на който е попълнен формуляра за изявлението за подкрепа, могат да бъдат съхранени в системата без криптиране.

2.12. Поддръжниците имат единствено достъп до данни, попълнени по време на сесията, в която те са оформили окончателно формуляра за изявление за подкрепа. Веднъж след като формулярът за изявление за подкрепа е внесен, сесията се затваря и внесените данни вече не са достъпни.

2.13. Личните данни на поддръжниците са налични в системата, включително в архива, само в криптирана форма. За целите на консултиране на данните или удостоверяване от националните органи в съответствие с член 8 от Регламент (ЕС) № 211/2011, организаторите могат да експортират криптирани данни в съответствие с точка 2.7.7, буква а).

2.14. Наличието на данните, въведени във формуляра за изявление за подкрепа, е атомарно. Това означава, че след като потребителят е вписал всички изисквани данни във формуляра за изявление за подкрепа и валидира своето решение да подкрепи инициативата, системата или успешно вкарва всички данни от формуляра в базата данни, или, в случай на грешка, не запазва никакви данни. Системата информира потребителя за успеха или неуспеха на неговото/нейното искане.

2.15. Използваният DBMS е актуализиран и постоянно коригиран при откриване на нови атаки от вид *exploits*.

2.16. Всички дневници за дейността на системата са налице. Системата гарантира, че дневниците за одит на изключенията и други важни събития, свързани със сигурността, посочени по-долу, могат да се изготвят и съхраняват до момента, в който данните се унищожат в съответствие с член 12, параграф 3 или 5 от Регламент (ЕС) № 211/2011. Дневниците са адекватно защитени, например, чрез съхранение върху кодирани носители. Организаторите/администраторите редовно проверяват дневниците за подозрителни действия. Съдържанието на дневника включва най-малко следното:

а) дати и часове на влизане и излизане на организатори/администратори;

б) извършено архивиране;

в) всички изменения и актуализации, извършени от администратори на бази данни.

Сигурност на инфраструктурата — физическо място, мрежова инфраструктура и среда на сървъра

2.17. *Физическа сигурност*

Независимо от вида на използвания хостинг машината, на която се помещава програмата, е надлежно защитена, за което е необходимо следното:

а) контрол на достъпа до зоната на хостинг и дневник за одит;

б) физическа защита на архивираните данни срещу кражба или случайно преместване;

в) сървърът, на който се помещава програмата, е инсталиран в сигурна кутия.

2.18. *Сигурност на мрежата*

2.18.1. Системата се помещава на интернет сървър, инсталиран в „демилитазирана зона“ (demilitarized zone (DMZ) и защитен със защитна стена.

2.18.2. Когато съответните актуализации и корекции (patches) на продукта за защитна стена станат обществено достъпни, тогава такива актуализации или корекции се инсталират целесъобразно.

2.18.3. Целият входящ и изходящ трафик на сървъра (предназначен за системата за събиране на изявления за подкрепа онлайн), бива инспектиран с правилата на защитна стена и вписван в дневник. С правилата за защитна стена се отказва трафик, който не е необходим за безопасното използване и управление на системата.

2.18.4. Системата за събиране на изявления за подкрепа онлайн трябва да се помещава на подходящо защитен производствен сегмент на мрежата, който е отделен от сегменти, в които се помещават непроизводствени системи като среди за разработване или изпробване.

2.18.5. Налице са мерки за сигурност на Local Area Network (LAN), като:

а) списък за достъп слой 2 (Layer 2 (L2)/сигурност на превключвател на порт;

б) неизползвани превключватели на порт се деактивират;

в) DMZ се намира на предназначена за това Virtual Local Area Network (VLAN)/LAN;

г) не се активира обобщаването на връзки L2 за ненужни портове.

2.19. *Сигурност на оперативната система, на уеб сървъра и на приложния сървър*

2.19.1. Налице е правилна конфигурация на сигурността, включително на елементите, описани в точка 2.7.6.

2.19.2. Приложенията работят с най-нисък набор от привилегии, които са им необходими, за да функционират.

2.19.3. Административният достъп до интерфейса за управление на системата за събиране на изявления за подкрепа онлайн има кратък таймаут на сесията (максимум 15 минути).

2.19.4. Когато съответните актуализации и корекции на оперативната система, среда/време за изпълнение, програми, работещи на сървъри или програми за отстраняване на малуеър станат обществено достъпни, тогава такива актуализации или корекции се инсталират целесъобразно.

2.19.5. Намален е рискът от това някой да удостовери самоличността си в базата данни, като използва атака от вид „pass-the-hash“.

2.20. *Сигурност на клиенти организатори*

За постигане на цялостна сигурност организаторите вземат необходимите мерки, за да гарантират сигурността на своята/своето програма/устройство за клиенти, която/което използват за управление и достъп до системата за събиране на изявления за подкрепа онлайн, както следва:

2.20.1. Потребителите извършват задачи, които не са свързани с поддръжката (като офис автоматизация) с най-нисък набор от привилегии, които са им необходими, за да работят.

2.20.2. Когато съответните актуализации и корекции на оперативната система, инсталирани програми, или програми за отстраняване на малуеър вече станат обществено достъпни, тогава такива актуализации или корекции се инсталират целесъобразно.

3. ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ, НАСОЧЕНИ КЪМ ПРИЛАГАНЕ НА ЧЛЕН 6, ПАРАГРАФ 4, БУКВА в) ОТ РЕГЛАМЕНТ (ЕС) № 211/2011

3.1. Системата дава възможност за всяка отделна държава-членка да се извлече доклад, в който се посочват инициативата и личните данни на поддръжниците, които са предмет на проверка от компетентния орган на тази държава-членка.

3.2. Експортирането на изявления за подкрепа на поддръжниците е възможно във формата от приложение III към Регламент (ЕО) № 211/2011. В системата може освен това да се предвиди възможността за експортиране на изявления за подкрепа в оперативно съвместим формат, като Extensible Markup Language (XML).

3.3. Експортираните изявления за подкрепа се отбелязват за *ограничено разпространение* до съответната държава-членка и са означени като *лични данни*.

3.4. Електронното предаване на експортирани данни до държавите-членки е защитено срещу прихващане, като се използва подходящо цялостно криптиране.