II

(Niet-wetgevingshandelingen)

VERORDENINGEN

UITVOERINGSVERORDENING (EU) Nr. 1179/2011 VAN DE COMMISSIE

van 17 november 2011

tot vaststelling van technische specificaties voor systemen voor het online verzamelen van steunbetuigingen overeenkomstig Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad over het burgerinitiatief

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad van 16 februari 2011 over het burgerinitiatief ([1]), en met name artikel 6, lid 5,

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming,

Overwegende hetgeen volgt:

(1) In Verordening (EU) nr. 211/2011 wordt bepaald dat wanneer steunbetuigingen online worden verzameld, de daarvoor gebruikte systemen moeten voldoen aan bepaalde beveiligingseisen en technische specificaties en dat de bevoegde instantie van de betrokken lidstaat deze systemen moet certificeren.

(2) Een systeem voor het online verzamelen van steunbetuigingen als bedoeld in Verordening (EU) nr. 211/2011 is een informatiesysteem bestaande uit software, hardware, een hostingomgeving, bedrijfsprocessen en personeel, dat bestemd is voor het online verzamelen van steunbetuigingen.

(3) In Verordening (EU) nr. 211/2011 worden de vereisten vastgesteld waaraan systemen voor het online verzamelen van steunbetuigingen dienen te voldoen om te kunnen worden gecertificeerd en wordt bepaald dat de Commissie technische specificaties dient vast te leggen voor de tenuitvoerlegging van die vereisten.

(4) In het top 10-project van het Open Web Application Security Project (OWASP) wordt voor 2010 een overzicht gegeven van de meest kritieke beveiligingsrisico's voor webtoepassingen en van instrumenten om deze risico's aan te pakken; voor de technische specificaties is daarom uitgegaan van de bevindingen van dit top 10-project.

(5) De organisatoren van een burgerinitiatief dienen de technische specificaties zodanig te implementeren dat het systeem door de autoriteiten van de lidstaat kan worden gecertificeerd en dat wordt bijgedragen tot de tenuitvoerlegging van de passende technische en organisatorische maatregelen die op grond van Richtlijn 95/46/EG van het Europees Parlement en de Raad ([2]) vereist zijn voor de beveiliging van de verwerkingsactiviteiten, zowel bij het ontwerp als bij de uitvoering van het verwerkingssysteem, teneinde de veiligheid te waarborgen en zodoende elke ongeoorloofde verwerking te verhinderen en persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, tegen vervalsing en tegen niet-toegelaten verspreiding of toegang.

(6) Het certificeringsproces wordt vergemakkelijkt indien de organisatoren gebruikmaken van de software die de Commissie verstrekt overeenkomstig artikel 6, lid 2, van Verordening (EU) nr. 211/2011.

(7) De organisatoren van burgerinitiatieven dienen bij het verzamelen van steunbetuigingen, zoals elke voor gegevensverwerking verantwoordelijke, de bij deze verordening vastgestelde technische specificaties ten uitvoer te leggen teneinde de bescherming van de verwerkte gegevens te waarborgen. Indien zij de verwerking uitbesteden aan een verwerker, dienen de organisatoren erop toe te zien dat de verwerker slechts te werk gaat volgens de instructies van de organisatoren en dat hij de bij deze verordening vastgestelde technische specificaties ten uitvoer legt.

(8) Deze verordening eerbiedigt de grondrechten en de beginselen die zijn vervat in het Handvest van de grondrechten van de Europese Unie, met name artikel 8, waarin is bepaald dat eenieder recht heeft op bescherming van zijn persoonsgegevens.

(9) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 20 van Verordening (EU) nr. 211/2011 ingestelde comité,

([1]) PB L 65 van 11.3.2011, blz. 1.

([2]) PB L 281 van 23.11.1995, blz. 31.

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

De in artikel 6, lid 5, van Verordening (EU) nr. 211/2011 bedoelde technische specificaties zijn opgenomen in de bijlage.

Artikel 2

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 17 november 2011.

Voor de Commissie
De voorzitter
José Manuel BARROSO

BIJLAGE

1. TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER a), VAN VERORDENING (EU) Nr. 211/2011

Om geautomatiseerde indiening van steunbetuigingen via het systeem te voorkomen, moet de ondertekenaar, voor hij zijn steunbetuiging kan indienen, een passend verificatieproces volgen dat in overeenstemming is met de gangbare praktijk. Een van de mogelijke verificatieprocessen is het gebruik van een sterke uitvoering van het „Captcha"-systeem.

2. TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER b), VAN VERORDENING (EU) Nr. 211/2011

Normen voor informatiezekerheid

2.1. De organisatoren verstrekken documentatie waaruit blijkt dat zij voldoen aan de vereisten van de norm ISO/IEC 27001, maar zij hoeven zich voor deze norm niet formeel te laten certificeren. Om aan de norm te voldoen, dienen zij:

a) een volledige risicobeoordeling te hebben uitgevoerd, in het kader waarvan het toepassingsgebied van het systeem is vastgesteld, de gevolgen voor de activiteiten van allerlei inbreuken op de informatiezekerheid zijn aangegeven, de bedreigingen voor en kwetsbaarheden van het informatiesysteem zijn vermeld, een risicoanalyse is opgesteld die tegenmaatregelen noemt waarmee deze bedreigingen kunnen worden voorkomen en maatregelen die zullen worden genomen als een bedreiging zich voordoet, en tot slot een geprioriteerde lijst van verbeteringen is opgesteld;

b) maatregelen voor risicobehandeling te hebben opgezet en geïmplementeerd met betrekking tot de bescherming van persoonsgegevens en de bescherming van het familie- en gezinsleven en het privéleven, alsmede maatregelen die zullen worden genomen als een risico zich voordoet;

c) een schriftelijke opgave van de restrisico's te hebben gedaan;

d) te hebben voorzien in de organisatorische middelen om feedback te ontvangen over nieuwe bedreigingen en verbeteringen van de beveiliging.

2.2. Op basis van de risicoanalyse die overeenkomstig punt 2.1, onder a), is verricht, kiezen de organisatoren veiligheidsbeheersingsmaatregelen volgens een van de onderstaande normen:

1. ISO/IEC 27002 of

2. de „Standard of Good Practice" van het Information Security Forum,

om de volgende zaken aan te pakken:

a) risicobeoordelingen (aanbevolen wordt ISO/IEC 27005 of een andere specifieke geschikte beoordelingsmethodologie toe te passen);

b) fysieke en omgevingsbeveiliging;

c) beveiliging in verband met de menselijke factor;

d) communicatie- en activiteitenbeheer;

e) standaardmaatregelen voor toegangscontrole, naast de maatregelen die in deze uitvoeringsverordening worden aangegeven;

f) aanschaf, ontwikkeling en onderhoud van informatiesystemen;

g) beheer van incidenten op het gebied van informatiebeveiliging;

h) maatregelen om inbreuken op informatiesystemen ongedaan te maken en de gevolgen ervan te verminderen, wanneer deze inbreuken kunnen leiden tot vernietiging, accidenteel verlies, vervalsing of ongeoorloofde bekendmaking van of ongeoorloofde toegang tot de verwerkte persoonsgegevens;

i) naleving van de voorschriften;

j) beveiliging van het computernetwerk (ISO/IEC 27033 of de reeds genoemde Standard of Good Practice wordt aanbevolen).

De toepassing van deze normen mag worden beperkt tot slechts die onderdelen van de organisatie die relevant zijn voor het systeem voor het online verzamelen van steunbetuigingen. De beveiliging in verband met de menselijke factor kan bijvoorbeeld worden beperkt tot het personeel dat fysiek of via het netwerk toegang heeft tot het systeem, en de fysieke en omgevingsbeveiliging kan worden beperkt tot het gebouw of de gebouwen waarin het systeem zich bevindt.

Functionele vereisten

2.3. Het systeem voor het online verzamelen van steunbetuigingen bestaat uit een instantie van een webtoepassing die is opgezet voor het verzamelen van steunbetuigingen aan één enkel burgerinitiatief.

2.4. Indien voor het beheer van het systeem verschillende rollen vereist zijn, wordt voorzien in verschillende toegangscontroleniveaus volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend.

2.5. Publiek toegankelijke voorzieningen zijn duidelijk afgescheiden van de voorzieningen die voor beheersdoeleinden bestemd zijn. Er is geen toegangscontrole die verhindert dat de informatie in het publieke gedeelte van het systeem wordt gelezen; dit geldt onder meer voor informatie over het initiatief en voor het elektronische steunbetuigingsformulier. Steunbetuigingen voor een initiatief kunnen uitsluitend via dit publieke gedeelte worden ingediend.

2.6. Het systeem signaleert en voorkomt dat meer dan éénmaal een steunbetuiging wordt ingediend.

Beveiliging op toepassingsniveau

2.7. Het systeem wordt adequaat beschermd tegen bekende kwetsbaarheden en exploits. Daartoe moet het aan onder andere de volgende vereisten voldoen:

2.7.1. Het systeem wordt beschermd tegen injectie van zoekopdrachten via onder andere SQL (Structured Query Language), LDAP (Lightweight Directory Access Protocol), XPath (XML Path Language), opdrachten van het besturingssysteem of argumenten bij programma's. Daartoe is in ieder geval het volgende vereist:

a) alle gebruikersinput wordt gevalideerd;

b) de validering wordt ten minste aan serverzijde uitgevoerd;

c) bij gebruik van interpreters worden niet-vertrouwde gegevens altijd gescheiden van (zoek)opdrachten. Voor SQL-opdrachten betekent dit dat bij alle prepared statements en stored procedures gebruik moet worden gemaakt van bindingsvariabelen en dat dynamische zoekopdrachten moeten worden vermeden.

2.7.2. Het systeem wordt beschermd tegen cross-site scripting (XSS). Daartoe is in ieder geval het volgende vereist:

a) van alle gebruikersinput die naar de browser wordt teruggestuurd, wordt de veiligheid geverifieerd (door middel van validering van de input);

b) alle gebruikersinput wordt waar nodig voorzien van escape sequences, voordat deze in de outputpagina wordt opgenomen;

c) de output wordt zodanig gecodeerd dat de input door de browser altijd als tekst wordt behandeld. Er wordt geen actieve content gebruikt.

2.7.3. Het systeem is voorzien van sterke authenticatie en sessiebeheer, waarvoor in ieder geval het volgende vereist is:

a) inloggegevens worden bij opslag altijd beschermd door hashing of encryptie. Het risico dat authenticatie plaatsvindt door middel van „pass-the-hash" moet worden verminderd;

b) inloggegevens kunnen niet worden geraden of overschreven als gevolg van zwak accountbeheer (bv. account aanmaken, wachtwoord wijzigen, wachtwoord herstellen, zwakke sessie-identificatoren (sessie-id's));

c) sessie-id's en sessiegegevens worden niet weergegeven in de URL (Uniform Resource Locator);

d) sessie-id's zijn niet vatbaar voor aanvallen door middel van session fixation;

e) sessie-id's verstrijken, waardoor gebruikers worden uitgelogd;

f) sessie-id's worden na een succesvolle login niet opnieuw gebruikt;

g) wachtwoorden, sessie-id's en andere gegevens worden uitsluitend via Transport Layer Security (TLS) verzonden;

h) Het beheersgedeelte van het systeem wordt afgeschermd. Als het wordt beschermd met enkelvoudige authenticatie, moet het wachtwoord uit ten minste tien tekens bestaan, waaronder ten minste één letter, één cijfer en één speciaal teken. Ook dubbele authenticatie kan worden gebruikt. Bij enkelvoudige authenticatie moet voor internettoegang tot het administratieve gedeelte van het systeem een verificatie in twee stappen worden toegepast: de enkelvoudige authenticatie wordt uitgebreid met een andere authenticatiemethode, zoals een via sms verzonden eenmalige wachtzin of wachtcode, of een asymmetrisch geëncrypteerde challenge in de vorm van een toevalsgetal, die wordt gedecrypteerd met de geheime sleutel van de organisatoren/administratoren, die bij het systeem niet bekend is.

2.7.4. Het systeem bevat geen onveilige directe objectreferenties. Daartoe is in ieder geval het volgende vereist:

a) voor directe referenties naar voorzieningen met restricties verifieert de toepassing of de gebruiker toegang mag worden verleend tot de gevraagde voorziening;

b) als het om een indirecte referentie gaat, wordt de mapping naar de directe referentie beperkt tot de waarden die voor de betrokken gebruiker zijn toegestaan.

2.7.5. Het systeem wordt beschermd tegen cross-site request forgery.

2.7.6. Het systeem is voorzien van een deugdelijke beveiligingsconfiguratie, waarvoor in ieder geval het volgende is vereist:

a) alle softwareonderdelen zijn up-to-date, inclusief het besturingssysteem, de web-/toepassingsserver, het databasemanagementsysteem (DBMS), de toepassingen en alle codelibrary's;

b) niet-benodigde services van het besturingssysteem en de web-/toepassingsserver zijn gedeactiveerd, verwijderd of niet geïnstalleerd;

c) standaardwachtwoorden voor accounts zijn gewijzigd of de standaardaccounts gedeactiveerd;

d) de foutafhandeling is zodanig opgezet dat stack traces en andere te informatieve foutmeldingen niet worden doorgelaten;

e) de beveiligingsinstellingen van ontwikkelingsframeworks en -library's zijn conform de beste praktijken, zoals de richtsnoeren van OWASP.

2.7.7. Gegevens in het systeem worden als volgt geëncrypteerd:

a) persoonsgegevens in elektronische vorm worden geëncrypteerd voor zij worden opgeslagen of verzonden naar de bevoegde autoriteiten van de lidstaten overeenkomstig artikel 8, lid 1, van Verordening (EU) nr. 211/2011. Beheer en back-up van de sleutels zijn daarvan gescheiden;

b) er wordt gebruikgemaakt van sterke standaardalgoritmen en sterke sleutels, die aan de internationale normen voldoen. Er is gezorgd voor sleutelbeheer;

c) wachtwoorden worden gehasht met een sterk standaardalgoritme en er wordt een passende saltwaarde gebruikt;

d) alle sleutels en wachtwoorden worden tegen ongeoorloofde toegang beschermd.

2.7.8. Het systeem beperkt URL-toegang op basis van de toegangs- en gebruiksrechten van de gebruiker. Daartoe is in ieder geval het volgende vereist:

a) als de authenticatie- en autorisatiecontroles voor de toegang tot een pagina via externe beveiligingsmechanismen worden uitgevoerd, moeten deze voor elke pagina naar behoren zijn geconfigureerd;

b) als bescherming op codeniveau wordt gebruikt, moet die voor elke opgevraagde pagina gelden.

2.7.9. Het systeem maakt gebruik van afdoende bescherming van de transportlaag. Daartoe zijn alle volgende maatregelen vereist, of maatregelen die ten minste even effectief zijn:

a) voor de toegang tot elke gevoelige voorziening vereist het systeem de meest recente versie van HTTPS (Hypertext Transfer Protocol Secure); de certificaten moeten geldig zijn, zij mogen niet zijn verstreken of ingetrokken en zij moeten overeenstemmen met alle domeinen die voor de site worden gebruikt;

b) het systeem stelt voor alle gevoelige cookies de flag „secure" in;

c) op de server is de TLS-provider zodanig geconfigureerd dat deze slechts de beste encryptiealgoritmen ondersteunt. De gebruikers wordt meegedeeld dat zij TLS-ondersteuning in hun browser moeten activeren.

2.7.10. Het systeem wordt beschermd tegen ongeldig gemaakte redirects en forwards.

Databasebeveiliging en gegevensintegriteit

2.8. Als voor verschillende burgerinitiatieven systemen voor het online verzamelen van steunbetuigingen worden gebruikt die gebruikmaken van dezelfde hardware en besturingssysteemvoorzieningen, mogen nooit gegevens (met inbegrip van toegangs- of encryptiegegevens) worden gedeeld. Bovendien moeten de risicobeoordeling en de gebruikte tegenmaatregelen aan deze situatie zijn aangepast.

2.9. Het risico dat authenticatie voor de database plaatsvindt door middel van „pass-the-hash" moet worden verminderd.

2.10. De gegevens die de ondertekenaars verstrekken, mogen uitsluitend toegankelijk zijn voor de databaseadministrator of -beheerder.

2.11. Beheersgegevens, persoonsgegevens die door ondertekenaars zijn opgegeven en back-ups daarvan worden beveiligd met sterke encryptiealgoritmen als bedoeld in punt 2.7.7, onder b). De lidstaat waar de steunbetuiging zal worden geteld, de datum waarop de steunbetuiging is ingediend en de taal waarin de ondertekenaar het formulier heeft ingevuld, mogen echter zonder encryptie in het systeem worden vermeld.

2.12. De ondertekenaars mogen slechts toegang krijgen tot de gegevens die zij hebben opgegeven tijdens de sessie waarin zijn het steunbetuigingsformulier hebben ingevuld. Zodra de steunbetuiging is ingediend, wordt deze sessie afgesloten en zijn de ingediende gegevens niet langer toegankelijk.

2.13. Persoonsgegevens van de ondertekenaar komen slechts in geëncrypteerde vorm in het systeem en in de back-up voor. Voor de raadpleging van gegevens of de certificering door de nationale autoriteiten overeenkomstig artikel 8 van Verordening (EU) nr. 211/2011 mogen de organisatoren de geëncrypteerde gegevens volgens punt 2.7.7, onder a), exporteren.

2.14. De in het steunbetuigingsformulier ingevulde gegevens zijn slechts in hun totaliteit persistent in het systeem. Dat wil zeggen: wanneer de gebruiker alle vereiste gegevens in het steunbetuigingsformulier heeft ingevoerd en zijn besluit om het burgerinitiatief te steunen heeft gevalideerd, legt het systeem ofwel alle gegevens van het formulier volledig vast, ofwel geen van die gegevens, indien er een fout optreedt. Het systeem deelt de gebruiker mee of het verzoek al dan niet met succes is ingevoerd.

2.15. Het databasemanagementsysteem is up-to-date en wordt voortdurend bijgewerkt wanneer nieuwe exploits worden ontdekt.

2.16. Alle activiteitenlogs van het systeem zijn aanwezig. Het systeem zorgt ervoor dat excepties en andere voor de beveiliging relevante gebeurtenissen, zoals hieronder genoemd, worden vermeld in auditlogs die kunnen worden getoond en worden behouden totdat de gegevens worden vernietigd overeenkomstig artikel 12, lid 3) of lid 5), van Verordening (EU) nr. 211/2011. Deze logs worden op passende wijze beschermd, bijvoorbeeld door opslag op geëncrypteerde media. De organisatoren/administratoren gaan regelmatig na of de logs op verdachte activiteiten wijzen. In de logs worden ten minste de volgende gegevens opgenomen:

a) datum en tijdstip waarop de organisatoren/administratoren inloggen en uitloggen;

b) verrichte back-ups;

c) alle door de administrator van de database aangebrachte wijzigingen en bijwerkingen.

Beveiliging van infrastructuur: fysieke locatie, netwerkinfrastructuur en serveromgeving

2.17. *Fysieke beveiliging*

Ongeacht het type hosting dient de machine waarop de toepassing wordt gehost, naar behoren te zijn beschermd, en wel op de volgende wijze:

a) toegangscontrole en auditlog betreffende de toegang tot de hostingruimte;

b) fysieke bescherming van de back-upgegevens tegen diefstal en zoekraken;

c) opstelling van de server waarop de toepassing draait in een beveiligd rek.

2.18. *Netwerkbeveiliging*

2.18.1. Het systeem wordt gehost op een met het internet verbonden server die geïnstalleerd is in een demilitarized zone (DMZ) en beveiligd wordt met een firewall.

2.18.2. Wanneer relevante updates en patches voor het firewallproduct worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.

2.18.3. Al het inkomende en uitgaande verkeer van de server (dat bestemd is voor het systeem) wordt aan de hand van de firewallregels gescreend en gelogd. De firewallregels houden alle verkeer tegen dat niet nodig is voor het veilige gebruik en beheer van het systeem.

2.18.4. Het systeem voor het online verzamelen van steunbetuigingen wordt gehost op een afdoende beschermd productiesegment van het netwerk, dat afgescheiden is van segmenten waarop niet-productiesystemen worden gehost, zoals ontwikkelings- of testomgevingen.

2.18.5. Het lokale netwerk (LAN) wordt beveiligd met maatregelen zoals:

a) toegangslijst voor de tweede laag (L2)/poortbeveiliging;

b) deactivering van ongebruikte poorten;

c) de DMZ bevindt zich op een afzonderlijk virtueel netwerk (VLAN) of LAN;

d) er vindt geen L2-trunking plaats op niet-benodigde poorten.

2.19. *Beveiliging van het besturingssysteem en de web-/toepassingsserver*

2.19.1. De beveiliging is correct geconfigureerd met inachtneming van punt 2.7.6.

2.19.2. De toepassingen worden uitgevoerd met slechts die rechten die voor hun functioneren noodzakelijk zijn.

2.19.3. Bij toegang van een administrator tot de beheersinterface van het systeem geldt een korte sessietime-out (maximaal 15 minuten).

2.19.4. Wanneer relevante updates en patches voor het besturingssysteem, de toepassingsruntimes, de op de servers draaiende toepassingen of malwarepreventiesoftware worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.

2.19.5. Het risico dat authenticatie voor de database plaatsvindt door middel van „pass-the-hash" moet worden verminderd.

2.20. *Beveiliging van de door de organisatoren gebruikte clients*

Om ervoor te zorgen dat het hele systeem van begin tot einde is beveiligd, nemen de organisatoren maatregelen ter beveiliging van de clienttoepassing of de machine die zij gebruiken voor het beheer van en de toegang tot het systeem voor het online verzamelen van steunbetuigingen, zoals de hierna volgende.

2.20.1. Niet-beheerstaken (zoals inzake kantoorautomatisering) worden uitgevoerd met slechts die rechten die voor hun functioneren noodzakelijk zijn.

2.20.2. Wanneer relevante updates en patches voor het besturingssysteem, geïnstalleerde toepassingen of malwarepreventie worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.

3. TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER c), VAN VERORDENING (EU) Nr. 211/2011

3.1. Het systeem voorziet in de mogelijkheid om voor elke afzonderlijke lidstaat een rapport op te stellen waarin voor het burgerinitiatief de persoonsgegevens van de ondertekenaars zijn opgenomen, zodat de bevoegde autoriteiten van de betrokken lidstaat deze kunnen verifiëren.

3.2. De door de ondertekenaars ingediende steunbetuigingen kunnen worden geëxporteerd in het formaat van bijlage III bij Verordening (EU) nr. 211/2011. Het systeem mag daarnaast in de mogelijkheid voorzien om de steunbetuigingen te exporteren in een interoperabel formaat zoals xml (Extensible Markup Language).

3.3. De geëxporteerde steunbetuigingen worden met als rubricering *beperkte verspreiding* aan de betrokken lidstaat ter beschikking gesteld en aangemerkt als *persoonsgegevens.*

3.4. De elektronische verzending van de geëxporteerde gegevens naar de lidstaten wordt tegen afluisteren beschermd door middel van geschikte end-to-endencryptie.