II

(Atti mhux leġiżlattivi)

REGOLAMENTI

REGOLAMENT TA' IMPLIMENTAZZJONI TAL-KUMMISSJONI (UE) Nru 1179/2011

tas-17 ta' Novembru 2011

li jistabbilixxi speċifikazzjonijiet tekniċi għas-sistemi ta' ġbir onlajn skont ir-Regolament (UE) Nru 211/2011 tal-Parlament Ewropew u tal-Kunsill dwar l-inizjattiva taċ-ċittadini

IL-KUMMISSJONI EWROPEA,

Wara li kkunsidrat it-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidrat ir-Regolament (UE) Nru 211/2011 tal-Parlament Ewropew u tal-Kunsill tas-16 ta' Frar 2011 dwar l-inizjattiva taċ-ċittadini [1], u b'mod partikolari l-Artikolu 6(5) tiegħu,

Wara li kkonsultat lill-Kontrollur Ewropew għall-Protezzjoni tad-Dejta

Billi:

(1) Ir-Regolament (UE) Nru 211/2011 jipprovdi li fejn id-dikjarazzjonijiet ta' appoġġ jinġabru onlajn, is-sistema użata għal dak il-għan għandha tissodisfa ċerti rekwiżiti tekniċi u ta' sigurtà u għandha tkun iċċertifikata mill-awtorità kompetenti tal-Istat Membru rilevanti.

(2) Sistema ta' ġbir onlajn fit-tifsira tar-Regolament (UE) Nru 211/2011 hija sistema tal-informazzjoni, li tikkonsisti minn softwer, ħardwer, ambjent tal-hosting, proċessi tan-negozju u persunal sabiex isir il-ġbir tad-dikjarazzjonijiet ta' appoġġ onlajn.

(3) Ir-Regolament (UE) Nru 211/2011 jistabbilixxi r-rekwiżiti li s-sistemi ta' ġbir onlajn għandhom jikkonformaw magħhom sabiex jiġu ċċertifikati u jipprovdi li l-Kummissjoni għandha tadotta speċifikazzjonijiet tekniċi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

(4) Il-proġett tal-Ogħla 10 tal-2010 tal-Proġett Open Web għas-Sigurtà tal-Applikazzjonijiet (The Open Web Application Security Project — OWASP) filwaqt li jipprovdi ħarsa ġenerali tal-aktar riskji kritiċi għas-sigurtà tal-applikazzjonijiet tal-web jipprovdi wkoll għodda biex jiġu indirizzati dawn ir-riskji; għalhekk l-ispeċifikazzjonijiet tekniċi huma bbażati fuq is-sejbiet ta' dan il-proġett.

(5) L-implimentazzjoni mill-organizzaturi tal-ispeċifikazzjonijiet tekniċi għandha tiggarantixxi ċertifikazzjoni ta' sistemi ta' ġbir onlajn mill-awtoritajiet tal-Istati Membri, u tikkontribwixxi biex tiżgura l-implimentazzjoni ta' miżuri tekniċi u organizzattivi xierqa li huma meħtieġa biex ikun hemm konformità mal-obbligi imposti mid-Direttiva 95/46/KE tal-Parlament Ewropew u tal-Kunsill [2] dwar is-sigurtà tal-attivitajiet tal-ipproċessar, kemm fiż-żmien tad-disinn tas-sistema tal-ipproċessar u anki fiż-żmien tal-ipproċessar innifsu, sabiex tinżamm is-sigurtà u biex b'hekk issir prevenzjoni għal kwalunkwe pproċessar mhux awtorizzat u tkun protetta d-dejta personali kontra l-qerda aċċidentali jew mhux skont il-liġi jew telf aċċidentali, alterazzjoni, żvelar jew aċċess mhux awtorizzat.

(6) Il-proċess ta' ċertifikazzjoni għandu jiġi ffaċilitat permezz tal-użu mill-organizzaturi tas-softwer ipprovdut mill-Kummissjoni skont l-Artikolu 6(2) tar-Regolament (UE) Nru 211/2011.

(7) L-organizzaturi tal-inizjattivi taċ-ċittadini, bħala kontrolluri tad-dejta, għandhom, meta jiġbru d-dikjarazzjonijiet ta' appoġġ onlajn, jimplimentaw l-ispeċifikazzjonijiet tekniċi stipulati f'dan ir-Regolament sabiex jiżguraw il-protezzjoni tad-dejta personali pproċessata. Fejn l-ipproċessar isir minn proċessur, l-organizzaturi għandhom jiżguraw li l-proċessur jaġixxi biss skont struzzjonijiet mill-ogranizzaturi u li jimplimenta l-ispeċifikazzjonijiet tekniċi stipulati f'dan ir-Regolament.

(8) Dan ir-Regolament jirrispetta d-drittijiet fundamentali u josserva l-prinċipji minquxa fil-Karta tad-Drittijiet Fundamentali tal-Unjoni Ewropea, b'mod partikolari l-Artikolu 8 tagħha, li jiddikjara li kull persuna għandha d-dritt għall-protezzjoni tad-dejta personali li tirrigwardaha.

(9) Il-miżuri stabbiliti f'dan ir-Regolament jikkonformaw mal-opinjoni tal-Kumitat stabbilit bl-Artikolu 20 tar-Regolament (UE) Nru 211/2011,

[1] ĠU L 65, 11.3.2011, p. 1.

[2] ĠU L 281, 23.11.1995, p. 31.

ADOTTAT DAN IR-REGOLAMENT:

Artikolu 1

L-ispeċifikazzjonijiet tekniċi msemmija fl-Artikolu 6(5) tar-Regolament (UE) Nru 211/2011 huma stipulati fl-Anness.

Artikolu 2

Dan ir-Regolament għandu jidħol fis-seħħ fl-għoxrin jum wara l-pubblikazzjoni tiegħu f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Dan ir-Regolament għandu jorbot fl-intier tiegħu u japplika direttament fl-Istati Membri kollha.

Magħmul fi Brussell, is-17 ta' Novembru 2011.

Għall-Kummissjoni
Il-President
José Manuel BARROSO

ANNESS

1. SPEĊIFIKAZZJONIJIET TEKNIĊI BIL-GĦAN LI JIMPLIMENTAW L-ARTIKOLU 6(4)(a) TAR-REGOLAMENT (UE) Nru 211/2011

Sabiex issir prevenzjoni ta' sottomissjoni awtomatizzata ta' dikjarazzjoni ta' appoġġ bl-użu tas-sistema, il-firmatarji jgħaddu minn proċess ta' verifika xieraq skont il-prattika attwali qabel is-sottomissjoni ta' dikjarazzjoni ta' appoġġ. Proċess ta' verifika possibbli huwa l-użu ta' "captcha" qawwija.

2. SPEĊIFIKAZZJONIJIET TEKNIĊI BIL-GĦAN LI JIMPLIMENTAW L-ARTIKOLU 6(4)(b) TAR-REGOLAMENT (UE) Nru 211/2011

Standards ta' Assigurazzjoni tal-Informazzjoni

2.1. L-organizzaturi jkunu jipprovdu dokumentazzjoni li turi li jissodisfaw ir-rekwiżiti tal-istandard ISO/IEC 27001, mingħajr ma jkunu meħtieġa li jadottawh. Għal dak il-għan, huma għandhom:

(a) iwettqu valutazzjoni sħiħa tar-riskju, li tidentifika l-ambitu tas-sistema, tenfasizza l-impatt tan-negozju f'każ ta' diversi ksur fl-assigurazzjoni tal-informazzjoni, telenka t-theddid u l-vulnerabbiltajiet tas-sistema tal-informazzjoni, tipproduċi dokument tal-analiżi tar-riskju li jelenka wkoll kontromiżuri biex jiġi evitat tali theddid u rimedji li jittieħdu f'każ ta' theddida, u finalment tfassal lista prijoritizzata ta' titjib;

(b) jiddisinjaw u jimplimentaw miżuri għat-trattament tar-riskji fir-rigward tal-protezzjoni tad-dejta personali u l-ħarsien tal-familja u l-ħajja privata, u miżuri li jittieħdu f'każ li jitfaċċa riskju;

(ċ) jidentifikaw ir-riskji li jifdal bil-miktub;

(d) jipprovdu l-mezzi organizzattivi sabiex jirċievu segwitu dwar theddid ġdid u titjib tas-sigurtà.

2.2. L-organizzaturi jagħżlu kontrolli ta' sigurtà bbażati fuq l-analiżi tar-riskju f'2.1. a) minn dawn l-istandards li ġejjin:

(1) ISO/IEC 27002; jew

(2) "L-Istandard dwar l-Aħjar Prattika" tal-Forum dwar is-Sigurtà tal-Informazzjoni

biex jindirizzaw il-kwistjonijiet li ġejjin:

(a) Il-valutazzjonijiet tar-riskju (ISO/IEC 27005 jew metodoloġija oħra speċifika u xierqa għall-evalwazzjoni tar-riskju, huma rakkomandati);

(b) Sigurtà fiżika u ambjentali;

(ċ) Sigurtà tar-riżorsi umani;

(d) Il-ġestjoni tal-komunikazzjoni u l-operazzjonijiet;

(e) Miżuri standard ta' kontroll għall-aċċess, b'żieda ma' dawk stabbiliti f'dan ir-Regolament ta' Implimentazzjoni;

(f) L-akkwist, l-iżvilupp u l-manutenzjoni tas-sistemi tal-informazzjoni;

(g) Il-ġestjoni tal-inċidenti ta' sigurtà tal-informazzjoni;

(h) Miżuri biex jirrimedjaw u jrażżnu ħsarat fis-sistemi ta' informazzjoni li jistgħu jirriżultaw fil-qerda jew it-telf aċċidentali, tibdil, żvelar jew aċċess mhux awtorizzat ta' dejta personali pproċessata;

(i) Konformità;

(j) Sigurtà tan-netwerk tal-kompjuter (ISO/IEC 27033 jew l-SoGP huma rrakkomandati).

L-applikazzjoni ta' dawn l-istandards tista' tkun limitata għall-partijiet tal-organizzazzjoni li huma rilevanti għas-sistema ta' ġbir onlajn. Pereżempju, is-sigurtà tar-riżorsi umani tista' tkun limitata għal kwalunkwe persunal li jkollu aċċess fiżiku jew permezz tan-netwerk għas-sistema ta' ġbir onlajn, u s-sigurtà fiżika/ambjentali tista' tkun limitata għall-bini fejn isir il-hosting tas-sistema.

Rekwiżiti funzjonali

2.3. Is-sistema ta' ġbir onlajn tkun tikkonsisti f'applikazzjoni bbażata fuq il-web stabbilita bl-għan li jinġabru dikjarazzjonijiet ta' appoġġ għal inizjattiva waħda taċ-ċittadini.

2.4. Jekk l-amministrazzjoni tas-sistema tkun teħtieġ rwoli differenti, f'dan il-każ jiġu stabbiliti livelli differenti ta' kontroll tal-aċċess skont il-prinċipju tal-inqas privileġġ.

2.5. Il-karatteristiċi aċċessibbli pubblikament ikunu mifruda b'mod ċar mill-karatteristiċi destinati għall-għanijiet ta' amministrazzjoni. L-ebda kontroll fuq l-aċċess ma jkun ifixkel il-qari tal-informazzjoni disponibbli fiż-żona pubblika tas-sistema, inkluża l-informazzjoni fuq l-inizjattiva u l-formola elettronika tad-dikjarazzjoni ta' appoġġ. Wieħed ikun jista' jiffirma inizjattiva permezz ta' din iż-żona pubblika biss.

2.6. Is-sistema tkun tagħraf u tipprevjeni s-sottomissjoni ta' dikjarazzjonijiet ta' appoġġ duplikati.

Il-livell ta' sigurtà tal-applikazzjoni

2.7. Is-sistema tkun protetta b'mod adegwat kontra l-vulnerabbiltajiet u l-isfruttar magħrufa. Għal dan il-għan, din tkun tissodisfa, inter alia, ir-rekwiżiti li ġejjin:

2.7.1. Is-sistema tkun toffri protezzjoni kontra l-"injection flaws" bħal mistoqsijiet fil-forma ta' Structured Query Language (SQL), Lightweight Directory Access Protocol (LDAP), XML Path Language (XPath), commands tal-Operating System (OS) jew argumenti tal-program. Għal dan il-għan, din tkun teħtieġ mill-inqas li:

(a) L-input kollu tal-utenti jkun ivvalidat.

(b) Minn tal-inqas il-validazzjoni ssir mil-loġika tan-naħa tas-server.

(ċ) Kull użu tal-interpreti ikun jissepara b'mod ċar dejta mhux affidabbli mill-kmand jew mistoqsija. Għall-SQL calls, dan ifisser l-użu ta' varjanti li jorbtu fid-dikjarazzjonijiet ippreparati u l-proċeduri maħżuna kollha, u jiġu evitati l-mistoqsijiet dinamiċi.

2.7.2. Is-sistema tkun tipprovdi protezzjoni kontra l-Cross-Site Scripting (XSS). Għal dan il-għan, hija tkun teħtieġ mill-inqas li:

(a) L-input kollu pprovdut mill-utenti li jintbagħat lura lill-brawżer jiġi vverifikat li hu mingħajr periklu (permezz ta' validazzjoni tal-input).

(b) L-input kollu tal-utenti jkun "escaped" b'mod tajjeb qabel ma jiġi inkluż fil-paġna tal-output.

(ċ) Kodifikazzjoni tal-output b'mod xieraq tiżgura li tali input ikun dejjem meqjus bħala text fil-brawżer. L-ebda kontenut attiv ma jkun użat.

2.7.3. Is-sistema ikollha ġestjoni tal-awtentikazzjoni u tas-sessjoni qawwija, li tkun teħtieġ mill-inqas li:

(a) Il-kredenzjali jkunu mħarsa dejjem meta maħżuna bl-użu tal-"ħashing" jew il-kriptaġġ. Ir-riskju li xi ħadd jagħmel awtentikazzjoni permezz ta' "pass-the-hash" ikun imrażżan.

(b) Ħadd ma jkun jista' jaqta' x'inhuma l-kredenzjali jew iħassarhom b'dejta ġdida permezz ta' funzjonijiet tal-ġestjoni tal-kont dgħajfa (pereżempju l-ħolqien tal-kont, il-bdil ta' password, l-irkupru tal-password, l-identifikaturi ta' sessjoni dgħajfa (IDs)).

(ċ) L-IDs tas-sessjoni u d-dejta tas-sessjoni ma jkunux esposti fil-Uniform Resource Locator (URL).

(d) L-IDs tas-sessjoni ma jkunux vulnerabbli għall-attakki ta' fissar tas-sessjoni.

(e) L-IDs tas-sessjoni jiskadu, li jiżgura li l-utenti jagħmlu log out.

(f) L-IDs tas-sessjoni ma jkunux "rotated" wara li jillogġjaw b'suċċess.

(g) Il-passwords, l-IDs tas-sessjoni, u kredenzjali oħra jintbagħtu biss permezz ta' Transport Layer Security (TLS).

(h) Il-parti tal-amministrazzjoni tas-sistema tkun protetta. Jekk tkun protetta minn awtentikazzjoni b'fattur wieħed, f'dan il-każ il-password tkun magħmula minn minimu ta' 10 karattri, li tinkludi mill-inqas ittra waħda, numru wieħed u karattru speċjali wieħed. Alternattivament tista' tintuża awtentikazzjoni b'żewġ fatturi. Fejn tintuża biss awtentikazzjoni b'fattur wieħed, din tkun tinkludi mekkaniżmu ta' verifika fuq żewġ fażijiet għall-aċċess tal-parti tal-amministrazzjoni tas-sistema permezz tal-Internet, fejn il-fattur waħdieni jkun awmentat permezz ta' mezz ieħor ta' awtentikazzjoni, bħal pass-phrase/kodiċi ta' darba permezz ta' SMS jew xi "random challenge string" kriptata b'mod assimetriku li trid tiġi dekriptata permezz ta' "key" privata tal-orgnizzaturi/amministraturi li ma tkunx magħrufa għas-sistema.

2.7.4. Is-sistema ma jkollhiex referenzi diretti għall-oġġetti li mhumiex żguri. Għal dan il-għan, hija tkun teħtieġ mill-inqas li:

(a) Għal referenzi diretti għal riżorsi ristretti, l-applikazzjoni tkun tivverifika li l-utent huwa awtorizzat biex jaċċessa r-riżorsi eżatti mitluba.

(b) Jekk ir-referenza tkun referenza indiretta, l-immappjar għar-referenza diretta ikun limitat għal valuri awtorizzati għall-utent attwali.

2.7.5. Is-sistema tkun tipprovdi protezzjoni kontra difetti relatati ma' talbiet ta' falsifikazzjoni "cross-site".

2.7.6. Il-konfigurazzjoni tas-sigurtà xierqa tkun fis-seħħ, li tirrikjedi, minn tal-inqas, li:

(a) Il-komponenti kollha tas-softwer ikunu aġġornati, inklużi l-OS, is-server tal-web/applikazzjoni, is-Sistema ta' Ġestjoni tal-Bażi tad-Dejta (DBMS), l-applikazzjonijiet, u l-kodiċi kollha tal-libreriji.

(b) Is-servizzi mhux neċessarji tal-OS u s-server tal-web/applikazzjoni ikunu diżattivati, jitneħħew, jew ma jkunux installati.

(ċ) Id-defaults tal-passwords tal-kont ikunu mibdula jew diżattivati.

(d) It-trattament tal-iżbalji ikun issettjat biex jipprevjeni "stack traces" u messaġġi b'wisq informazzjoni milli jinfiltraw.

(e) Is-settings ta' sigurtà fl-oqfsa u l-libreriji tal-iżvilupp ikunu kkonfigurati skont l-aħjar prattika, bħal-linji gwida tal-OWASP.

2.7.7. Is-sistema tkun tipprovdi għall-kriptaġġ tad-dejta hekk kif ġej:

(a) Id-dejta personali fil-format elettroniku tkun kriptata meta maħżuna jew trasferita lill-awtoritajiet kompetenti tal-Istati Membri skont l-Artikolu 8 (1) tar-Regolament (UE) Nru 211/2011, filwaqt li l-"keys" jiġu amministrati u bbekkjati b'mod separat.

(b) Algoritmi standard qawwija u "keys" qawwija jkunu użati f'konformità mal-istandards internazzjonali. Il-ġestjoni tal-"keys" tkun fis-seħħ.

(ċ) Il-passwords ikunu "hashed" b'algoritmu standard qawwi u "salt" xieraq ikun użat.

(d) Il-"keys" u l-passwords kollha jkunu protetti minn aċċess mhux awtorizzat.

2.7.8. Is-sistema tkun tirrestrinġi l-aċċess tal-URL skont il-livelli u l-permessi ta' aċċess tal-utent. Għal dan il-għan, hija tkun teħtieġ mill-inqas li:

(a) Jekk jintużaw mekkaniżmi esterni tas-sigurtà biex ikunu provduti l-kontrolli tal-awtentikazzjoni u l-awtorizzazzjoni għall-aċċess tal-paġna, dawn iridu jkunu kkonfigurati għal kull paġna.

(b) Jekk tintuża l-protezzjoni tal-livell tal-kodiċi, il-protezzjoni tal-livell tal-kodiċi trid tkun fis-seħħ għal kull paġna meħtieġa.

2.7.9. Is-sistema tkun tuża Transport Layer Protection b'mod suffiċjenti. Għal dan il-għan, il-miżuri kollha li ġejjin jew miżuri li jkollhom ta' mill-inqas saħħa ugwali jkunu fis-seħħ:

(a) Is-sistema tkun teħtieġ l-aktar verżjoni riċenti tal-Hypertext Transfer Protocol Secure (HTTPS) biex taċċessa kwalunkwe riżorsi sensittivi bl-użu ta' ċertifikati li huma validi, mhux skaduti, mhux revokati, u jaqblu mad-domains kollha użati mis-sit.

(b) Is-sistema tkun tissettja l-bandiera ta' "sigurtà" fuq il-cookies sensittivi kollha.

(ċ) Is-server ikun jikkonfigerja l-fornitur tat-TLS biex jiġu aċċettati biss algoritmi ta' kriptaġġ skont l-aħjar prattika. L-utenti jkunu infurmati li għandhom jippermettu l-appoġġ mit-TLS fil-brawżer tagħhom.

2.7.10. Is-sistema tkun tipprovdi protezzjoni kontra "redirects" u "forwards" mhux ivvalidati.

Is-sigurtà tal-bażi tad-dejta u l-integrità tad-dejta

2.8. Fejn is-sistemi ta' ġbir onlajn użati għal inizjattivi taċ-ċittadini differenti jaqsmu bejniethom il-ħardwer u r-riżorsi tas-sistema operattiva, dawn ma jaqsmu l-ebda dejta, inklużi l-kredenzjali tal-aċċess/kriptaġġ. Barra minn hekk, dan huwa rifless fil-valutazzjoni tar-riskju u fil-kontromiżuri implimentati.

2.9. Ir-riskju li xi ħadd jagħmel awtentikazzjoni fuq il-bażi tad-dejta billi juża l-"pass-the-hash" ikun imrażżan.

2.10. Id-dejta pprovduta mill-firmatarji tkun aċċessibbli biss għall-amministratur/organizzatur tal-bażi tad-dejta.

2.11. Il-kredenzjali amministrattivi, id-dejta personali miġbura minn firmatarji u l-backup tagħha jkunu garantiti permezz ta' algoritmi ta' kriptaġġ qawwija skont il-punt 2.7.7 (b). Madankollu, l-Istat Membru fejn se jsir l-għadd tad-dikjarazzjoni ta' appoġġ, id-data ta' sottomissjoni tad-dikjarazzjoni ta' appoġġ u l-lingwa li biha firmatarju jkun mela l-formola tad-dikjarazzjoni ta' appoġġ jistgħu jinħażnu fis-sistema mingħajr kriptaġġ.

2.12. Il-firmatarji jkollhom biss aċċess għad-dejta sottomessa matul is-sessjoni li fiha jkunu mlew il-formola tad-dikjarazzjoni ta' appoġġ. Ladarba formola tad-dikjarazzjoni ta' appoġġ tkun sottomessa, is-sessjoni t'hawn fuq tingħalaq u d-dejta sottomessa ma tkunx aktar aċċessibbli.

2.13. Id-dejta personali tal-firmatarji tkun disponibbli biss fis-sistema, inkluż il-backup, f'forma kriptata. Għall-iskop ta' konsultazzjoni jew ta' ċertifikazzjoni tad-dejta mill-awtoritajiet nazzjonali f'konformità mal-Artikolu 8 tar-Regolament (UE) Nru 211/2011, l-organizzaturi jistgħu jesportaw id-dejta kriptata f'konformità mal-punt 2.7.7 (a)

2.14. Il-persistenza tad-dejta mdaħħla fil-formola tad-dikjarazzjoni ta' appoġġ tkun atomika. Jiġifieri, ladarba l-utent ikun daħħal id-dettalji meħtieġa kollha fil-formola tad-dikjarazzjoni ta' appoġġ, u jivvalida d-deċiżjoni tiegħu/tagħha biex jappoġġja l-inizjattiva, is-sistema jew tivverifika b'suċċess il-formola kollha għall-bażi tad-dejta, jew, fil-każ ta' żball, ma tissejvja l-ebda dejta. Is-sistema tinforma lill-utent bis-suċċess jew l-iżball tat-talba tiegħu/tagħha.

2.15. Id-DBMS użata tkun aġġornata u armata kontinwament għal kontra attivitajiet mhux tas-soltu ġodda li jkunu individwati

2.16. Il-logs tal-attività tas-sistema jkunu kollha fis-seħħ. Is-sitema tkun tiżgura li l-logs ta' verifika li jirreġistraw l-eċċezzjonijiet u l-avvenimenti l-oħra rilevanti għas-sigurtà elenkati hawn taħt jistgħu jiġu prodotti u miżmuma sakemm id-dejta tiġi meqruda skont l-Artikolu 12(3) jew (5) tar-Regolament (UE) Nru 211/2011. Il-logs ikunu protetti b'mod xieraq, pereżempju bil-ħażna fuq midja kriptata. L-organizzaturi/amministraturi jiċċekkjaw b'mod regolari l-logs għal attività suspettuża. Il-kontenut tal-log ikun jinkludi mill-inqas

(a) Id-dati u l-ħinijiet tal-log-on u l-log-off mill-organizzaturi/amministraturi;

(b) Il-backups li jkunu saru;

(ċ) Il-bidliet u l-aġġornamenti kollha tal-bażi tad-dejta li jsiru mill-amministraturi.

Is-sigurtà tal-infrastruttura – il-post fiżiku, l-infrastruttura tan-netwerk u l-ambjent tas-server

2.17. *Is-sigurtà fiżika*

Irrispettivament mit-tip ta' hosting li jintuża, l-apparat involut għall-hosting tal-applikazzjoni jkun protett kif xieraq, li jipprovdi:

(a) Kontroll tal-aċċess taż-żona tal-hosting u log tal-verifika;

(b) Protezzjoni fiżika tal-backup tad-dejta għal kontra s-serq jew it-tqegħid fejn mhux suppost b'mod aċċidentali;

(ċ) Li l-hosting server tal-applikazzjoni jkun installat f'rack sigura.

2.18. *Is-sigurtà tan-netwerk*

2.18.1. Il-hosting tas-sistema jsir fuq server li jkun jiffaċċja l-Internet installat fuq żona li mhix militarizzata (DMZ) u protett permezz ta' Firewall.

2.18.2. Meta aġġornamenti u patches rilevanti tal-prodott tal-Firewall isiru pubbliċi, tali aġġornamenti jew patches jiġu installati b'mod espedjenti.

2.18.3. It-traffiku kollu li jidħol u joħroġ għas-server (li jkun destinat għas-sistema ta' ġbir onlajn) jiġi spezzjonat permezz tar-regoli tal-Firewall u jiġi llogjat. Ir-regoli tal-Firewall ikunu jipprojbixxu kull traffiku li mhux meħtieġ għall-użu u l-amministrazzjoni b'sigurtà tas-sistema.

2.18.4. Il-hosting tas-sistema ta' ġbir onlajn għandu jsir fuq segment tan-netwerk tal-produzzjoni protetta li tkun separata minn segmenti użati għall-hosting ta' sistemi mhux ta' produzzjoni bħal ambjenti tal-iżvilupp jew tal-ittestjar.

2.18.5. Il-miżuri ta' sigurtà tal-Local Area Network (LAN) jkunu jinsabu fis-seħħ bħal:

(a) Is-sigurtà tal-lista tal-Layer 2 (L2) Access/l-iswiċċ tal-Port;

(b) Kull swiċċ mhux użat ikun diżattivat;

(ċ) Id-DMZ tkun fuq Virtual Local Area Network (VLAN)/LAN iddedikata;

(d) L-ebda tranking tal-L2 ma jkun attivat fuq ports mhux neċessarji.

2.19. *Is-sigurtà tal-OS u tas-server tal-web/applikazzjoni*

2.19.1. Konfigurazzjoni tas-sigurtà xierqa tkun fis-seħħ inklużi l-elementi elenkati fil-punt 2.7.6.

2.19.2. L-applikazzjonijiet ikunu jaħdmu bl-inqas sett ta' privileġġi li jeħtieġu biex jaħdmu.

2.19.3. L-aċċess tal-amministratur għall-interfaċċja ta' ġestjoni tas-sistema ta' ġbir onlajn ikollha ħin ta' għeluq tas-sessjoni qasir (massimu ta' 15-il minuta).

2.19.4. Meta aġġornamenti u patches rilevanti tal-OS, ir-runtimes tal-applikazzjoni, l-applikazzjonijiet li jaħdmu fuq is-servers, jew tal-anti-malware isiru pubbliċi, tali aġġornamenti jew patches jiġu installati b'mod espedjenti.

2.19.5. Ir-riskju li xi ħadd jagħmel awtentikazzjoni permezz ta' "pass-the-hash" ikun mitigat.

2.20. *Is-sigurtà tal-klijent tal-organizzatur*

Għal raġunijiet ta' sigurtà minn tarf għall-ieħor, l-organizzaturi jieħdu l-miżuri meħtieġa biex jassiguraw l-applikazzjoni/mezz ta' klijent tagħhom li huma jużaw għall-ġestjoni u l-aċċess tas-sistema ta' ġbir onlajn, bħal:

2.20.1. L-utenti jħaddmu xogħlijiet mhux ta' manutenzjoni (bħal awtomazzjoni tal-uffiċċju) bl-inqas sett ta' privileġġi li huma jeħtieġu biex jaħdmu.

2.20.2. Meta aġġornamenti u patches rilevanti tal-OS, kwalunkwe applikazzjonijiet installati, jew tal-anti-malware isiru pubbliċi, tali aġġornamenti jew patches jiġu installati b'mod espedjenti.

3. SPEĊIFIKAZZJONIJIET TEKNIĊI BIL-GĦAN LI JIMPLIMENTAW L-ARTIKOLU 6(4)(c) TAR-REGOLAMENT (UE) Nru 211/2011

3.1. Is-sistema tkun tipprovdi l-possibbiltà li ssir estrazzjoni għal kull Stat Membru individwali ta' rapport li jelenka l-inizjattiva u d-dejta personali tal-firmatarji soġġetta għall-verifika mill-awtorità kompetenti ta' dak l-Istat Membru.

3.2. L-esportazzjoni tad-dikjarazzjonijiet ta' appoġġ tal-firmatarji tkun possibbli fil-format tal-Anness III tar-Regolament Nru 211/2011. Barra minn hekk, is-sistema tkun tista' tipprovdi għall-possibbiltà ta' esportazzjoni tad-dikjarazzjonijiet ta' appoġġ f'format interoperabbli bħall-Extensible Markup Language (XML).

3.3. Id-dikjarazzjonijiet ta' appoġġ esportati ikunu mmarkati bħala li huma ta' *distribuzzjoni limitata* lill-Istat Membru kkonċernat, u ttikkettjati bħala *dejta personali*.

3.4. It-trażmissjoni elettronika tad-dejta esportata lill-Istati Membri tkun żgurata għal kontra s-smigħ sigriet permezz ta' kriptaġġ minn tarf sa tarf xieraq.