II

(Μη νομοθετικές πράξεις)

ΚΑΝΟΝΙΣΜΟΙ

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 1179/2011 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 17ης Νοεμβρίου 2011

για τη θέσπιση τεχνικών προδιαγραφών για επιγραμμικά συστήματα συγκέντρωσης σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 211/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την πρωτοβουλία πολιτών

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 211/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Φεβρουαρίου 2011, σχετικά με την πρωτοβουλία πολιτών [1], και ιδίως το άρθρο 6 παράγραφος 5,

Κατόπιν διαβούλευσης με τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων,

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) αριθ. 211/2011 προβλέπει ότι στην περίπτωση επιγραμμικής συγκέντρωσης των δηλώσεων υποστήριξης, το σύστημα που χρησιμοποιείται για αυτόν τον σκοπό πρέπει να ικανοποιεί ορισμένες απαιτήσεις ασφάλειας, καθώς και τεχνικές απαιτήσεις, και να πιστοποιείται από την αρμόδια αρχή του οικείου κράτους μέλους.

(2) Ένα επιγραμμικό σύστημα συγκέντρωσης κατά την έννοια του κανονισμού (ΕΕ) αριθ. 211/2011 είναι ένα σύστημα πληροφοριών που αποτελείται από λογισμικό, εξοπλισμό, περιβάλλον φιλοξενίας, επιχειρηματικές διεργασίες και προσωπικό προκειμένου να επιτευχθεί η επιγραμμική συγκέντρωση δηλώσεων υποστήριξης.

(3) Ο κανονισμός (ΕΕ) αριθ. 211/2011 ορίζει τις απαιτήσεις προς τις οποίες πρέπει να συμμορφώνονται τα επιγραμμικά συστήματα συγκέντρωσης προκειμένου να λαμβάνουν πιστοποίηση και προβλέπει ότι η Επιτροπή θεσπίζει τεχνικές προδιαγραφές για την εφαρμογή αυτών των απαιτήσεων.

(4) Το σχέδιο Top 10 2010 του Open Web Application Security Project (OWASP) παρέχει επισκόπηση των σημαντικότερων κινδύνων ασφάλειας εφαρμογών διαδικτύου, καθώς και των εργαλείων για την αντιμετώπιση αυτών των κινδύνων· ως εκ τούτου, οι τεχνικές προδιαγραφές αξιοποιούν τα πορίσματα αυτού του σχεδίου.

(5) Η εφαρμογή των τεχνικών προδιαγραφών εκ μέρους των διοργανωτών θα πρέπει να διασφαλίζει την πιστοποίηση των επιγραμμικών συστημάτων συγκέντρωσης από τις αρχές των κρατών μελών και να συμβάλει στη διασφάλιση της εφαρμογής των κατάλληλων τεχνικών και οργανωτικών μέτρων που απαιτούνται προκειμένου να συμμορφώνονται προς τις υποχρεώσεις της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [2] σχετικά με την ασφάλεια επεξεργασίας, κατά τη στιγμή τόσο του σχεδιασμού των τεχνικών επεξεργασίας όσο και της εκτέλεσης της επεξεργασίας, προκειμένου να υπάρξουν εγγυήσεις για την ασφάλειά τους και να εμποδίζεται έτσι κάθε ανεπίτρεπτη επεξεργασία και να προστατεύονται τα δεδομένα προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση.

(6) Προκειμένου να διευκολύνουν τη διαδικασία πιστοποίησης οι διοργανωτές θα πρέπει να χρησιμοποιούν το λογισμικό που παρέχεται από την Επιτροπή σύμφωνα με το άρθρο 6 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 211/2011.

(7) Οι διοργανωτές πρωτοβουλιών πολιτών, ως υπεύθυνοι ελέγχου των δεδομένων, κατά την επιγραμμική συγκέντρωση δηλώσεων υποστήριξης θα πρέπει να εφαρμόζουν τις τεχνικές προδιαγραφές που ορίζονται στον παρόντα κανονισμό προκειμένου να διασφαλίζουν την προστασία των επεξεργασμένων δεδομένων προσωπικού χαρακτήρα. Εάν η επεξεργασία διεξάγεται από εργολήπτη, οι διοργανωτές θα πρέπει να διασφαλίζουν ότι αυτός ενεργεί αποκλειστικά βάσει των οδηγιών των διοργανωτών και ότι εφαρμόζει τις τεχνικές προδιαγραφές που ορίζονται στον παρόντα κανονισμό.

(8) Ο παρών κανονισμός σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που περιλαμβάνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ιδίως το άρθρο 8, βάσει του οποίου κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

(9) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που συστάθηκε βάσει του άρθρου 20 του κανονισμού (ΕΕ) αριθ. 211/2011,

[1] ΕΕ L 65 της 11.3.2011, σ. 1.

[2] ΕΕ L 281 της 23.11.1995, σ. 31.

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Οι τεχνικές προδιαγραφές που αναφέρονται στο άρθρο 6 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 211/2011 καθορίζονται στο παράρτημα.

Άρθρο 2

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 17 Νοεμβρίου 2011.

Για την Επιτροπή
Ο Πρόεδρος
José Manuel BARROSO

ΠΑΡΑΡΤΗΜΑ

1. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΠΟΥ ΑΠΟΣΚΟΠΟΥΝ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΑΡΘΡΟΥ 6 ΠΑΡΑΓΡΑΦΟΣ 4 ΣΤΟΙΧΕΙΟ α) ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) αριθ. 211/2011

Για την αποφυγή της αυτόματης υποβολής δήλωσης υποστήριξης μέσω του συστήματος, ο υπογράφων ακολουθεί κατάλληλη διαδικασία επαλήθευσης σύμφωνα με την τρέχουσα πρακτική πριν από την υποβολή της δήλωσης υποστήριξης. Μια πιθανή διαδικασία επαλήθευσης είναι η χρήση ισχυρού «captcha».

2. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΠΟΥ ΑΠΟΣΚΟΠΟΥΝ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΑΡΘΡΟΥ 6 ΠΑΡΑΓΡΑΦΟΣ 4 ΣΤΟΙΧΕΙΟ β) ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) αριθ. 211/2011

Πρότυπα διασφάλισης πληροφοριών

2.1. Οι διοργανωτές παρέχουν τεκμηρίωση που αποδεικνύει ότι πληρούν τις απαιτήσεις του προτύπου ISO/IEC 27001, εκτός από την απαίτηση υιοθέτησής του. Γι' αυτόν τον σκοπό:

α) διεξήγαγαν πλήρη εκτίμηση κινδύνων που αναγνωρίζει το πεδίο εφαρμογής του συστήματος, επισημαίνει τις επιπτώσεις στις δραστηριότητες σε περίπτωση διάφορων παραβάσεων ως προς τη διασφάλιση των πληροφοριών, απαριθμεί τις απειλές και τα προβλήματα ευπάθειας του συστήματος πληροφοριών, παράγει ένα έγγραφο ανάλυσης κινδύνων το οποίο επίσης καταγράφει αντίμετρα για την αποφυγή αυτών των απειλών και λύσεις σε περίπτωση εμφάνισης μιας απειλής, και τέλος συντάσσει έναν κατάλογο βελτιώσεων κατά προτεραιότητα·

β) σχεδίασαν και εφάρμοσαν μέτρα για την αντιμετώπιση κινδύνων σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία της οικογενειακής και της ιδιωτικής ζωής και μέτρα που θα λαμβάνονται σε περίπτωση εμφάνισης κινδύνου·

γ) προσδιόρισαν γραπτώς τους υπολειπόμενους κινδύνους·

δ) παρείχαν τα οργανωτικά μέσα για τη λήψη παρατηρήσεων σχετικά με νέες απειλές και βελτιώσεις ασφάλειας.

2.2. Οι διοργανωτές επιλέγουν τους ελέγχους ασφάλειας βάσει της ανάλυσης κινδύνων στην παράγραφο 2.1 στοιχείο α) των παρακάτω προτύπων:

1. ISO/IEC 27002 ή

2. «Πρότυπο καλής πρακτικής» του φόρουμ ασφάλειας των πληροφοριών

για να διαχειριστούν τα ακόλουθα ζητήματα:

α) εκτιμήσεις κινδύνων (προτείνεται το ISO/IEC 27005 ή άλλη ειδική και κατάλληλη μεθοδολογία εκτίμησης κινδύνων)·

β) υλική και περιβαλλοντική ασφάλεια·

γ) ασφάλεια ανθρώπινων πόρων·

δ) διαχείριση επικοινωνιών και επιχειρησιακών δραστηριοτήτων·

ε) τυποποιημένα μέτρα ελέγχου της πρόσβασης, εκτός από τα μέτρα που ορίζονται στον παρόντα εκτελεστικό κανονισμό·

στ) απόκτηση, ανάπτυξη και συντήρηση συστημάτων πληροφοριών·

ζ) διαχείριση περιστατικών ασφάλειας πληροφοριών·

η) μέτρα για την επίλυση και τον περιορισμό των παραβάσεων σε συστήματα πληροφοριών που θα είχαν ως αποτέλεσμα την καταστροφή ή τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση των επεξεργασμένων δεδομένων προσωπικού χαρακτήρα·

θ) συμμόρφωση·

ι) ασφάλεια δικτύου υπολογιστή [προτείνεται το ISO/IEC 27033 ή το Πρότυπο καλής πρακτικής (SoGP)].

Η εφαρμογή αυτών των προτύπων μπορεί να περιορίζεται σε μέρη της οργάνωσης που αφορούν το επιγραμμικό σύστημα συγκέντρωσης. Για παράδειγμα, η ασφάλεια των ανθρώπινων πόρων μπορεί να περιορίζεται σε τυχόν μέλη του προσωπικού που έχουν φυσική ή δικτυακή πρόσβαση στο επιγραμμικό σύστημα συγκέντρωσης και η υλική/περιβαλλοντική ασφάλεια μπορεί να περιορίζεται στο κτίριο που φιλοξενεί το σύστημα.

Λειτουργικές απαιτήσεις

2.3. Το επιγραμμικό σύστημα συγκέντρωσης αποτελείται από ένα αναγνωριστικό εμφάνισης εφαρμογής μέσω web που εγκαθίσταται για τη συγκέντρωση δηλώσεων υποστήριξης για μία πρωτοβουλία πολιτών.

2.4. Εάν η διαχείριση του συστήματος προϋποθέτει διαφορετικούς ρόλους, τότε τα διαφορετικά επίπεδα ελέγχου της πρόσβασης δημιουργούνται σύμφωνα με την αρχή των ελάχιστων προνομίων.

2.5. Τα χαρακτηριστικά στα οποία έχει πρόσβαση το κοινό διαχωρίζονται σαφώς από τα χαρακτηριστικά τα οποία προορίζονται για σκοπούς διαχείρισης. Η απουσία ελέγχου της πρόσβασης εμποδίζει την ανάγνωση των πληροφοριών που τίθενται στη διάθεση του κοινού από το σύστημα, συμπεριλαμβανομένων πληροφοριών σχετικά με την πρωτοβουλία και το ηλεκτρονικό έντυπο δήλωσης υποστήριξης. Η προσυπογραφή μιας πρωτοβουλίας είναι δυνατή μόνο μέσω αυτού του χώρου που είναι διαθέσιμος στο κοινό.

2.6. Το σύστημα εντοπίζει και αποτρέπει την υποβολή διπλών δηλώσεων υποστήριξης.

Ασφάλεια εφαρμογής

2.7. Το σύστημα προστατεύεται κατάλληλα από γνωστά προβλήματα ευπάθειας και προγράμματα εκμετάλλευσης ευπάθειας. Προς τούτο, ικανοποιεί, μεταξύ άλλων τις παρακάτω απαιτήσεις:

2.7.1. Το σύστημα προστατεύεται από ελαττώματα παρεμβολής, όπως ερωτήματα της γλώσσας Structured Query Language (SQL), ερωτήματα του πρωτοκόλλου Lightweight Directory Access Protocol (LDAP), ερωτήματα της γλώσσας XML Path Language (XPath), εντολές του λειτουργικού συστήματος ή ορίσματα προγράμματος. Γι' αυτόν τον σκοπό, απαιτούνται τουλάχιστον τα παρακάτω:

α) Όλα τα στοιχεία που εισάγονται από τον χρήστη είναι επικυρωμένα.

β) Η επικύρωση διεξάγεται τουλάχιστον από τη λογική του διακομιστή.

γ) Η χρήση ερμηνευτών διαχωρίζει σαφώς τα αναξιόπιστα δεδομένα από την εντολή ή το ερώτημα. Οι κλήσεις SQL προϋποθέτουν τη χρήση μεταβλητών δέσμευσης σε όλες τις συνταχθείσες δηλώσεις και τις αποθηκευμένες διαδικασίες, και την αποφυγή δυναμικών ερωτημάτων.

2.7.2. Το σύστημα προστατεύεται από επιθέσεις μέσω δέσμης ενεργειών από άλλη τοποθεσία (XSS). Γι' αυτόν τον σκοπό, απαιτούνται τουλάχιστον τα παρακάτω:

α) Όλα τα στοιχεία που εισάγονται από τον χρήστη τα οποία αποστέλλονται στο πρόγραμμα περιήγησης επαληθεύονται ως προς την ασφάλειά τους (μέσω επικύρωσης στοιχείων εισαγωγής).

β) Έχει πραγματοποιηθεί κατάλληλη έξοδος όλων των στοιχείων εισαγωγής από τον χρήστη πριν συμπεριληφθούν στη σελίδα εξόδου.

γ) Η κατάλληλη κωδικοποίηση εξόδου διασφαλίζει ότι αυτά τα στοιχεία εισαγωγής αντιμετωπίζονται πάντα ως κείμενο στο πρόγραμμα περιήγησης. Δεν χρησιμοποιείται ενεργό περιεχόμενο.

2.7.3. Το σύστημα διαθέτει ισχυρή διαχείριση ελέγχου ταυτότητας και περιόδου λειτουργίας που προϋποθέτει τουλάχιστον τα παρακάτω:

α) Τα διαπιστευτήρια προστατεύονται πάντα κατά την αποθήκευση χρησιμοποιώντας κλείδωμα ή κρυπτογράφηση. Ο κίνδυνος ελέγχου ταυτότητας περιορίζεται με τη χρήση του εργαλείου «pass-the-hash».

β) Δεν είναι δυνατή η πρόβλεψη ή η αντικατάσταση διαπιστευτηρίων μέσω λειτουργιών επισφαλούς διαχείρισης λογαριασμού (π.χ. δημιουργία λογαριασμού, αλλαγή κωδικού πρόσβασης, ανάκτηση κωδικού πρόσβασης, επισφαλή αναγνωριστικά περιόδου λειτουργίας).

γ) Τα αναγνωριστικά περιόδου λειτουργίας και τα δεδομένα περιόδου λειτουργίας δεν εκτίθενται στο ενιαίο προσδιοριστικό πόρου (URL).

δ) Τα αναγνωριστικά περιόδου λειτουργίας δεν είναι ευπαθή σε επιθέσεις δέσμευσης της περιόδου λειτουργίας.

ε) Τα αναγνωριστικά περιόδου λειτουργίας έχουν χρονικό όριο το οποίο διασφαλίζει ότι οι χρήστες αποσυνδέονται.

στ) Τα αναγνωριστικά περιόδου λειτουργίας δεν εναλλάσσονται μετά την επιτυχή σύνδεση.

ζ) Οι κωδικοί πρόσβασης, τα αναγνωριστικά περιόδου λειτουργίας και λοιπά διαπιστευτήρια αποστέλλονται μόνο με ασφάλεια επιπέδου μεταφοράς (TLS).

η) Το μέρος διαχείρισης του συστήματος προστατεύεται. Εάν προστατεύεται από έλεγχο ταυτότητας με έναν παράγοντα, τότε ο κωδικός πρόσβασης αποτελείται από τουλάχιστον 10 χαρακτήρες, συμπεριλαμβανομένου τουλάχιστον ενός γράμματος, ενός αριθμού και ενός ειδικού χαρακτήρα. Εναλλακτικά, είναι δυνατή η χρήση ελέγχου ταυτότητας με δύο παράγοντες. Η περίπτωση ελέγχου ταυτότητας με έναν παράγοντα περιλαμβάνει μηχανισμό επαλήθευσης με δύο βήματα για την πρόσβαση του μέρους διαχείρισης του συστήματος μέσω του διαδικτύου, στον οποίο ο μοναδικός παράγοντας επαυξάνεται από άλλο μέσο ελέγχου ταυτότητας, όπως μια μοναδική φράση/κωδικό πρόσβασης μέσω SMS ή μια ασύμμετρα κρυπτογραφημένη τυχαία συμβολοσειρά που αποκρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί των διοργανωτών/διαχειριστών που είναι άγνωστο στο σύστημα.

2.7.4. Το σύστημα δεν διαθέτει μη ασφαλείς άμεσες αναφορές αντικειμένου. Γι' αυτόν τον σκοπό, απαιτούνται τουλάχιστον τα παρακάτω:

α) Για άμεσες αναφορές σε περιορισμένους πόρους, η εφαρμογή επαληθεύει ότι ο χρήστης έχει εξουσιοδοτημένη πρόσβαση στον ακριβή πόρο που αιτήθηκε.

β) Εάν η αναφορά είναι έμμεση, η αντιστοίχηση στην άμεση αναφορά περιορίζεται σε τιμές που εξουσιοδοτούνται για τον τρέχοντα χρήστη.

2.7.5. Το σύστημα προστατεύεται από επιθέσεις τύπου cross-site request forgery (πλαστογράφηση αίτησης μεταξύ θέσεων).

2.7.6. Η κατάλληλη διαμόρφωση ασφάλειας υπάρχει, πράγμα που προϋποθέτει τουλάχιστον τα παρακάτω:

α) Όλα τα στοιχεία λογισμικού είναι ενημερωμένα, μεταξύ άλλων το λειτουργικό σύστημα, ο διακομιστής web/εφαρμογών, το σύστημα διαχείρισης βάσης δεδομένων, οι εφαρμογές και όλες οι βιβλιοθήκες κωδικών.

β) Οι περιττές υπηρεσίες του λειτουργικού συστήματος και του διακομιστή web/εφαρμογών απενεργοποιούνται, καταργούνται ή δεν εγκαθίστανται.

γ) Οι προεπιλεγμένοι κωδικοί πρόσβασης των λογαριασμών τροποποιούνται ή απενεργοποιούνται.

δ) Εγκαθίσταται χειρισμός σφαλμάτων για την αποτροπή διαρροής των ιχνηλατήσεων στοίβας και λοιπών εξαιρετικά πληροφοριακών μηνυμάτων σφάλματος.

ε) Οι ρυθμίσεις ασφάλειας στα πλαίσια ανάπτυξης και τις βιβλιοθήκες διαμορφώνονται σύμφωνα με τις βέλτιστες πρακτικές, όπως τις κατευθυντήριες γραμμές του OWASP.

2.7.7. Το σύστημα προβλέπει την κρυπτογράφηση δεδομένων ως εξής:

α) Τα προσωπικά δεδομένα σε ηλεκτρονική μορφή κρυπτογραφούνται κατά την αποθήκευση ή μεταφορά στις αρμόδιες αρχές των κρατών μελών σύμφωνα με το άρθρο 8 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 211/2011, ενώ για τα κλειδιά ακολουθείται χωριστή διαχείριση και δημιουργία αντιγράφων ασφάλειας.

β) Οι ισχυροί πρότυποι αλγόριθμοι και τα ισχυρά κλειδιά χρησιμοποιούνται σύμφωνα με τα διεθνή πρότυπα. Υπάρχει διαχείριση κλειδιού.

γ) Οι κωδικοί πρόσβασης κλειδώνονται με ισχυρό πρότυπο αλγόριθμο και χρησιμοποιείται ένα κατάλληλο αλάτι.

δ) Όλα τα κλειδιά και οι κωδικοί πρόσβασης προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.

2.7.8. Το σύστημα περιορίζει την πρόσβαση URL η οποία βασίζεται σε επίπεδα πρόσβασης και άδειες του χρήστη. Γι' αυτόν τον σκοπό, απαιτούνται τουλάχιστον τα παρακάτω:

α) Εάν χρησιμοποιούνται εξωτερικοί μηχανισμοί ασφάλειας για τον έλεγχο ταυτότητας και έλεγχοι εξουσιοδότησης για την πρόσβαση σελίδων, πρέπει να διαμορφώνονται κατάλληλα για κάθε σελίδα.

β) Εάν χρησιμοποιείται προστασία επιπέδου κωδικού, η προστασία επιπέδου κωδικού πρέπει να διατίθεται για κάθε απαιτούμενη σελίδα.

2.7.9. Το σύστημα χρησιμοποιεί επαρκή προστασία επιπέδου μεταφοράς. Γι' αυτόν τον σκοπό διατίθενται όλα τα παρακάτω μέτρα ή μέτρα τουλάχιστον ισάξιας ισχύος:

α) Το σύστημα απαιτεί την τρέχουσα έκδοση της ασφάλειας πρωτοκόλλου μεταφοράς υπερκειμένου (HTTPS) για την πρόσβαση σε τυχόν ευαίσθητο πόρο μέσω πιστοποιητικών που είναι έγκυρα, δεν έχουν λήξει, δεν έχουν ανακληθεί και αντιστοιχούν σε όλους τους τομείς οι οποίοι χρησιμοποιούνται από την τοποθεσία.

β) Το σύστημα τοποθετεί τη σημαία «ασφάλεια» σε όλα τα ευαίσθητα cookies.

γ) Ο διακομιστής διαμορφώνει την υπηρεσία παροχής ασφάλειας επιπέδου μεταφοράς προκειμένου να υποστηρίξει μόνο τους αλγόριθμους κρυπτογράφησης σύμφωνα με τις βέλτιστες πρακτικές. Οι χρήστες ενημερώνονται ότι πρέπει να ενεργοποιήσουν την υποστήριξη TLS στο πρόγραμμα περιήγησής τους.

2.7.10. Το σύστημα αποτρέπει μη επικυρωμένες ανακατευθύνσεις και προωθήσεις.

Ασφάλεια βάσης δεδομένων και ακεραιότητα δεδομένων

2.8. Στις περιπτώσεις που επιγραμμικά συστήματα συγκέντρωσης τα οποία χρησιμοποιούνται για διαφορετικές πρωτοβουλίες πολιτών έχουν κοινό υλικό και πόρους λειτουργικού συστήματος, δεν χρησιμοποιούν από κοινού τυχόν δεδομένα, συμπεριλαμβανομένων των διαπιστευτηρίων πρόσβασης/κρυπτογράφησης. Επιπλέον, αυτό αντανακλάται στην εκτίμηση κινδύνων και στα εφαρμοζόμενα αντίμετρα.

2.9. Ο κίνδυνος ελέγχου ταυτότητας στη βάση δεδομένων περιορίζεται με τη χρήση του εργαλείου «pass-the-hash».

2.10. Τα δεδομένα που παρέχονται από τους υπογράφοντες είναι προσβάσιμα μόνο στον διαχειριστή/διοργανωτή της βάσης δεδομένων.

2.11. Τα διαπιστευτήρια διαχειριστή, τα δεδομένα προσωπικού χαρακτήρα που συγκεντρώνονται από υπογράφοντες και τα αντίγραφα ασφάλειάς τους προστατεύονται με ισχυρούς αλγόριθμους κρυπτογράφησης σύμφωνα με το σημείο 2.7.7.β). Ωστόσο, το κράτος μέλος στο οποίο θα προσμετράται η δήλωση υποστήριξης, η ημερομηνία υποβολής της δήλωσης υποστήριξης και η γλώσσα στην οποία ο υπογράφων συμπλήρωσε το έντυπο της δήλωσης υποστήριξης θα αποθηκεύονται μη κρυπτογραφημένα στο σύστημα.

2.12. Οι υπογράφοντες έχουν πρόσβαση στα δεδομένα που υποβάλλονται μόνο κατά την περίοδο λειτουργίας στην οποία ολοκληρώνουν το έντυπο της δήλωσης υποστήριξης. Μετά την υποβολή του εντύπου της δήλωσης υποστήριξης, η ανωτέρω περίοδος λειτουργίας κλείνει και τα υποβληθέντα δεδομένα δεν είναι πλέον προσβάσιμα.

2.13. Τα δεδομένα προσωπικού χαρακτήρα των υπογραφόντων είναι διαθέσιμα στο σύστημα, συμπεριλαμβανομένων των αντιγράφων ασφάλειας, μόνο σε κρυπτογραφημένη μορφή. Για την επαλήθευση των δεδομένων ή την πιστοποίηση από τις εθνικές αρχές σύμφωνα με το άρθρο 8 του κανονισμού (ΕΕ) αριθ. 211/2011, οι διοργανωτές μπορούν να εξάγουν τα κρυπτογραφημένα δεδομένα σύμφωνα με το σημείο 2.7.7.α).

2.14. Η διατήρηση των δεδομένων που εισάγονται στο έντυπο της δήλωσης υποστήριξης είναι μεμονωμένη. Δηλαδή, αφού ο χρήστης εισάγει όλες τις απαιτούμενες λεπτομέρειες στο έντυπο της δήλωσης υποστήριξης και επικυρώσει την απόφασή του να υποστηρίξει την πρωτοβουλία, το σύστημα είτε δεσμεύει επιτυχώς όλα τα δεδομένα του εντύπου στη βάση δεδομένων, ή, σε περίπτωση σφάλματος, αποτυγχάνει χωρίς να αποθηκεύσει κανένα από τα δεδομένα. Το σύστημα ενημερώνει τον χρήστη για την επιτυχία ή αποτυχία του αιτήματός του.

2.15. Η DBMS που χρησιμοποιείται είναι επικαιροποιημένη και συνεχώς ενημερώνεται ο κώδικας για προγράμματα εκμετάλλευσης ευπάθειας που ανακαλύφθηκαν πρόσφατα.

2.16. Διατίθενται όλα τα αρχεία καταγραφής δραστηριοτήτων. Το σύστημα διασφαλίζει ότι τα αρχεία καταγραφής ελέγχου που καταγράφουν τις εξαιρέσεις και λοιπά συμβάντα ασφάλειας που αναφέρονται παρακάτω μπορεί να παράγονται και να φυλάσσονται ως την καταστροφή των δεδομένων σύμφωνα με το άρθρο 12 παράγραφος 3 ή 5 του κανονισμού (ΕΕ) αριθ. 211/2011. Τα αρχεία καταγραφής προστατεύονται επαρκώς, για παράδειγμα με αποθήκευση σε κρυπτογραφημένο μέσο. Οι διοργανωτές/διαχειριστές ελέγχουν τακτικά τα αρχεία καταγραφής για ύποπτες δραστηριότητες. Τα περιεχόμενα καταγραφής περιλαμβάνουν τουλάχιστον:

α) ημερομηνίες και χρόνους σύνδεσης και αποσύνδεσης από διοργανωτές/διαχειριστές·

β) τα αντίγραφα ασφάλειας που δημιουργήθηκαν·

γ) όλες τις τροποποιήσεις και ενημερώσεις της βάσης δεδομένων από τον διαχειριστή.

Ασφάλεια υποδομών — φυσική τοποθεσία, υποδομές δικτύου και περιβάλλον διακομιστή

2.17. *Φυσική ασφάλεια*

Για οποιονδήποτε τύπο φιλοξενίας χρησιμοποιείται, το μηχάνημα που φιλοξενεί την εφαρμογή προστατεύεται κατάλληλα, πράγμα το οποίο συνεπάγεται:

α) έλεγχο πρόσβασης περιοχής φιλοξενίας και αρχεία καταγραφής ελέγχου·

β) φυσική προστασία των δεδομένων σε αντίγραφα ασφάλειας από κλοπή ή τυχαία εσφαλμένη τοποθέτηση·

γ) ότι ο διακομιστής που φιλοξενεί την εφαρμογή εγκαθίσταται σε ασφαλισμένο πλαίσιο.

2.18. *Ασφάλεια δικτύου*

2.18.1. Το σύστημα φιλοξενείται σε έναν διακομιστή επαφών διαδικτύου που εγκαθίσταται σε «αποστρατιωτικοποιημένη» ζώνη (DMZ) και προστατεύεται από τείχος προστασίας.

2.18.2. Όταν δημοσιεύονται οι αντίστοιχες επικαιροποιήσεις και ενημερώσεις κώδικα εφαρμογής του προϊόντος του τείχους προστασίας, τότε αυτές οι επικαιροποιήσεις ή οι ενημερώσεις κώδικα εφαρμογής εγκαθίστανται τάχιστα.

2.18.3. Όλη η εισερχόμενη και εξερχόμενη κυκλοφορία στον διακομιστή (που προορίζεται για το επιγραμμικό σύστημα συγκέντρωσης) επιθεωρείται από τους κανόνες του τείχους προστασίας και καταγράφεται. Οι κανόνες του τείχους προστασίας αρνούνται την κυκλοφορία που δεν απαιτείται για την ασφαλή χρήση και διαχείριση του συστήματος.

2.18.4. Το επιγραμμικό σύστημα συγκέντρωσης πρέπει να φιλοξενείται σε επαρκώς προστατευόμενο τμήμα δικτύου παραγωγής που διαχωρίζεται από τα τμήματα τα οποία χρησιμοποιούνται σε κεντρικά συστήματα μη παραγωγής, όπως περιβάλλοντα ανάπτυξης ή δοκιμών.

2.18.5. Διατίθενται μέτρα ασφάλειας τοπικού δικτύου (LAN), όπως:

α) ασφάλεια λίστας πρόσβασης/εναλλαγής θύρας επιπέδου 2 (L2)·

β) οι αχρησιμοποίητες θύρες εναλλαγής απενεργοποιούνται·

γ) η αποστρατικοποιημένη ζώνη (DMZ) βρίσκεται σε αποκλειστικό εικονικό τοπικό δίκτυο (VLAN)/LAN·

δ) δεν ενεργοποιείται καμία ζεύξη L2 σε περιττές θύρες.

2.19. *Ασφάλεια λειτουργικού συστήματος και διακομιστή web/εφαρμογών*

2.19.1. Διατίθεται κατάλληλη διαμόρφωση ασφάλειας, συμπεριλαμβανομένων των στοιχείων που καταγράφονται στο σημείο 2.7.6.

2.19.2. Οι εφαρμογές εκτελούνται με το χαμηλότερο σύνολο δικαιωμάτων που απαιτείται.

2.19.3. Η πρόσβαση του διαχειριστή στη διασύνδεση διαχείρισης του επιγραμμικού συστήματος συγκέντρωσης έχει σύντομο χρονικό όριο περιόδου λειτουργίας (έως 15 λεπτά).

2.19.4. Όταν δημοσιεύονται οι αντίστοιχες επικαιροποιήσεις και ενημερώσεις κώδικα εφαρμογής του λειτουργικού συστήματος, των χρόνων εκτέλεσης εφαρμογής, των εφαρμογών που εκτελούνται στους διακομιστές, ή της προστασίας από λογισμικό κακόβουλης λειτουργίας, τότε αυτές οι επικαιροποιήσεις ή οι ενημερώσεις κώδικα εφαρμογής εγκαθίστανται κατάλληλα.

2.19.5. Ο κίνδυνος ελέγχου ταυτότητας στο σύστημα περιορίζεται με τη χρήση του εργαλείου «pass-the-hash».

2.20. *Ασφάλεια του υπολογιστή-πελάτη του διοργανωτή*

Για λόγους ασφάλειας από τερματικό σε τερματικό, οι διοργανωτές λαμβάνουν τα απαραίτητα μέτρα για να προστατεύσουν την εφαρμογή/συσκευή του πελάτη τους την οποία χρησιμοποιούν για να διαχειρίζονται και να έχουν πρόσβαση στο επιγραμμικό σύστημα συγκέντρωσης, ήτοι:

2.20.1. Οι χρήστες εκτελούν εργασίες μη συντήρησης (όπως αυτοματοποίηση γραφείου) με το χαμηλότερο σύνολο δικαιωμάτων που απαιτείται για εκτέλεση.

2.20.2. Όταν δημοσιεύονται οι αντίστοιχες επικαιροποιήσεις και ενημερώσεις κώδικα εφαρμογής του λειτουργικού συστήματος, τυχόν εγκατεστημένων εφαρμογών ή προστασίας από λογισμικό κακόβουλης λειτουργίας, τότε αυτές οι επικαιροποιήσεις ή οι ενημερώσεις κώδικα εφαρμογής εγκαθίστανται κατάλληλα.

3. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΠΟΥ ΑΠΟΣΚΟΠΟΥΝ ΣΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ ΑΡΘΡΟΥ 6 ΠΑΡΑΓΡΑΦΟΣ 4 ΣΤΟΙΧΕΙΟ γ) ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) αριθ. 211/2011

3.1. Το σύστημα παρέχει τη δυνατότητα εξαγωγής για κάθε κράτος μέλος μιας έκθεσης που καταγράφει την πρωτοβουλία και τα δεδομένα προσωπικού χαρακτήρα των υπογραφόντων που υπόκεινται σε επαλήθευση από την αρμόδια αρχή του εν λόγω κράτους μέλους.

3.2. Η εξαγωγή των δηλώσεων υποστήριξης των υπογραφόντων είναι δυνατή με τη μορφή του παραρτήματος III του κανονισμού (ΕΕ) αριθ. 211/2011. Το σύστημα μπορεί επιπλέον να παρέχει τη δυνατότητα εξαγωγής δηλώσεων υποστήριξης σε διαλειτουργική μορφή, όπως την Επεκτάσιμη Γλώσσα Σήμανσης (XML).

3.3. Οι εξαγόμενες δηλώσεις υποστήριξης επισημαίνονται ως *περιορισμένης διάδοσης* στο αντίστοιχο κράτος μέλος και ονομάζονται *δεδομένα προσωπικού χαρακτήρα*.

3.4. Η ηλεκτρονική διαβίβαση των εξαγόμενων δεδομένων στο κράτος μέλος προστατεύεται από παράνομη παρακολούθηση με τη χρήση κατάλληλης κρυπτογράφησης από τερματικό σε τερματικό.