Διαδικτυακή ασφάλεια: Ο οργανισμός της ΕΕ για την κυβερνοασφάλεια, ENISA, επισημαίνει τις επιδιορθώσεις ασφαλείας για τα νέα πρότυπα διαδικτύου

Σε μια κρίσιμη στιγμή της ανάπτυξης του HTML5, του νέου βασικού προτύπου για το διαδίκτυο, ο ENISA προτείνει σήμερα σημαντικές επιδιορθώσεις ασφαλείας για 13 επικείμενα πρότυπα του διαδικτύου. Ο ENISA έχει εντοπίσει 50 απειλές για την ασφάλεια και πρότεινε τον τρόπο αντιμετώπισής τους.

Τραπεζική, κοινωνική δικτύωση, αγορές, πλοήγηση, πληρωμές καρτών, ακόμη και διαχείριση υποδομών ζωτικής σημασίας όπως τα δίκτυα ηλεκτρικής ενέργειας – σχεδόν κάθε δραστηριότητα πραγματοποιείται σήμερα μέσα από ένα παράθυρο προγράμματος περιήγησης του διαδικτύου.

«*Το πρόγραμμα περιήγησης διαδικτύου αποτελεί πλέον ένα από τα σημαντικότερα από την άποψη της ασφάλειας στοιχεία των πληροφοριακών υποδομών μας – ένας ολοένα και πιο επικερδής στόχος για τους δράστες των κυβερνοεπιθέσεων*», παρατηρεί ο καθηγητής Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA.

Με σκοπό τη συμπερίληψη καινοτομιών στις διαδικτυακές εφαρμογές και στα επιχειρηματικά μοντέλα τους και προκειμένου να παράσχει τη δυνατότητα σε περισσότερους ανθρώπους να χρησιμοποιούν το διαδίκτυο, η W3C (η κοινοπραξία παγκόσμιου ιστού) πραγματοποιεί επί του παρόντος μείζονες αναθεωρήσεις επί των βασικών προτύπων της.

Ο ENISA άδραξε την ευκαιρία για να επανεξετάσει τις προδιαγραφές και να προτείνει βελτιώσεις με σκοπό την ενίσχυση της ασφάλειας των προγραμμάτων περιήγησης διαδικτύου για όλους τους χρήστες. «*Πολλές από αυτές τις προδιαγραφές φθάνουν σε σημείο μη αναστρέψιμο. Έχουμε, επιτέλους, την ευκαιρία να σκεφθούμε εις βάθος το θέμα της ασφάλειας, πριν παγιωθεί το πρότυπο, αντί να προσπαθούμε να το μπαλώσουμε εκ των υστέρων. Πρόκειται για μοναδική ευκαιρία να ενσωματώσουμε την ασφάλεια μέσω του σχεδιασμού*», δηλώνει ο Giles Hogben, ο οποίος συνεργάστηκε στη σύνταξη της έκθεσης.

«*Χαιρετίζουμε αυτή την ιδιαίτερα επίκαιρη αναθεώρηση ασφαλείας από τον ENISA. Έχουμε ενθαρρύνει τον ENISA να αναφέρει τα προβλήματα που εντοπίζει στις αρμόδιες ομάδες εργασίας της W3C*», δηλώνει ο Thomas Roessler, επικεφαλής ασφαλείας της W3C.

Η ανάλυση του **ENISA** **αποκαλύπτει 50 απειλές για την ασφάλεια** και σχετικά ζητήματα, μεταξύ των οποίων:

- Μη προστατευμένη πρόσβαση σε ευαίσθητες πληροφορίες
- Νέοι τρόποι ενεργοποίησης υποβολής εντύπων για τους δράστες κυβερνοεπιθέσεων
- Προβλήματα στον προσδιορισμό και την εφαρμογή πολιτικών για την ασφάλεια
- Δυνητικές αναντιστοιχίες με τη διαχείριση αδειών λειτουργικών συστημάτων
- Ανεπαρκώς προσδιορισμένες λειτουργίες, με πιθανή συνέπεια ασύμβατες ή επισφαλείς εφαρμογές
- Νέοι τρόποι αποφυγής των μηχανισμών ελέγχου πρόσβασης και της προστασίας από το «click-jacking» (η παραπλάνηση του χρήστη με σκοπό αυτός να κάνει κλικ σε επικίνδυνους συνδέσμους και κουμπιά)

«*Ένα σημαντικό συμπέρασμα αυτής της μελέτης είναι ότι εντοπίστηκαν πολύ λιγότερα προβλήματα ασφαλείας στις προδιαγραφές οι οποίες έχουν ήδη υποβληθεί σε αναλυτική επανεξέταση της ασφάλειας. Αυτό καταδεικνύει την αξία της εις βάθος επανεξέτασης της ασφάλειας των επερχόμενων προδιαγραφών»,* δηλώνει ο Marnix Dekker, ο οποίος συνεργάστηκε στη σύνταξη της έκθεσης.

Ιστορικό: Ψηφιακό θεματολόγιο για την Ευρώπη, (2.3, Εμπιστοσύνη και ασφάλεια).

Για την πλήρη εργασία

Για συνεντεύξεις ή περισσότερες πληροφορίες: Ulf Bergstrom, Εκπρόσωπος τύπου, ENISA, press@enisa.europa.eu , Κινητό: + 30-6948-460-143, ή Dr Giles Hogben, Εμπειρογνώμων, ENISA, giles.hogbenQ enisa.europa.eu

«Η αγγλική μετάφραση του παρόντος δελτίου τύπου είναι η μόνη έγκυρη έκδοση».