Προστασία προσωπικών δεδομένων: Κατευθυντήριες γραμμές του ENISA για λύσεις κρυπτογράφησης

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δημοσιεύει σήμερα δύο εκθέσεις. Η έκθεση του 2014 με τίτλο «Αλγόριθμοι, μέγεθος κλειδιών και παράμετροι» αποτελεί έγγραφο αναφοράς που παρέχει σειρά κατευθυντήριων γραμμών στους υπευθύνους λήψης αποφάσεων και συγκεκριμένα στους ειδικούς που σχεδιάζουν και εφαρμόζουν λύσεις κρυπτογράφησης για προστασία των προσωπικών δεδομένων σε εμπορικές επιχειρήσεις ή κυβερνητικές υπηρεσίες για τους πολίτες. Η «Μελέτη για τα πρωτόκολλα κρυπτογράφησης» προσφέρει μια προοπτική εφαρμογής, καλύπτοντας κατευθυντήριες γραμμές σχετικά με τα πρωτόκολλα που απαιτούνται για προστασία των εμπορικών ηλεκτρονικών επικοινωνιών που περιέχουν προσωπικά δεδομένα.

«Αλγόριθμοι, μέγεθος κλειδιών και παράμετροι»

Αυτή η έκθεση παρουσιάζει σειρά προτάσεων σε εύχρηστη μορφή, με έμφαση στις εμπορικές ηλεκτρονικές υπηρεσίες που συλλέγουν, αποθηκεύουν και επεξεργάζονται τα προσωπικά δεδομένα πολιτών της ΕΕ. Αποτελεί ενημερωμένη έκδοση της έκθεσης του 2013 για τις κατευθυντήριες γραμμές κρυπτογράφησης σχετικά με τα μέτρα ασφαλείας που απαιτούνται για προστασία των προσωπικών δεδομένων σε ηλεκτρονικά συστήματα. Σε σύγκριση με την έκδοση του 2013, η έκθεση έχει επεκταθεί ώστε να περιλαμβάνει ενότητα για τις επιθέσεις πλευρικών καναλιών σε υλικό και λογισμικό, τις γεννήτριες τυχαίων αριθμών και τη διαχείριση του κύκλου ζωής των κλειδιών, ενώ το τμήμα για τα πρωτόκολλα επεκτάθηκε για το 2014 και αποτελεί αυτόνομη μελέτη των πρωτοκόλλων κρυπτογράφησης.

Η έκθεση εξηγεί δύο πτυχές των μηχανισμών κρυπτογράφησης:

- το κατά πόσον ένα δεδομένο αρχέγονο ή σύστημα μπορεί να ληφθεί υπόψη για χρήση σήμερα, εάν έχει ήδη αναπτυχθεί
- το κατά πόσον ένα αρχέγονο ή σύστημα είναι κατάλληλο για ανάπτυξη σε νέα ή μελλοντικά συστήματα.

Τα θέματα της μακροπρόθεσμης διατήρησης δεδομένων αναλύονται μαζί με σειρά γενικών θεμάτων που σχετίζονται με την ανάπτυξη αρχέγονων και συστημάτων κρυπτογράφησης. Όλοι οι μηχανισμοί που περιγράφονται στην έκθεση είναι σε κάποιο βαθμό τυποποιημένοι, ενώ είτε έχουν ήδη αναπτυχθεί είτε σχεδιάζεται η ανάπτυξή τους σε πραγματικά συστήματα.

«Μελέτη για τα πρωτόκολλα κρυπτογράφησης»

Η δεύτερη έκθεση επικεντρώνεται στην τρέχουσα κατάσταση στα πρωτόκολλα κρυπτογράφησης και ενθαρρύνει την περαιτέρω έρευνα. Παρουσιάζεται σύνοψη των πρωτοκόλλων που χρησιμοποιούνται σε σχετικά περιορισμένους τομείς εφαρμογής, όπως ασύρματα δίκτυα, κινητές επικοινωνίες ή τραπεζικά συστήματα, (Bluetooth, WPA/WEP, UMTS/LTE, ZigBee, EMV) και σε συγκεκριμένα περιβάλλοντα που επικεντρώνονται στο υπολογιστικό νέφος.

Η έκθεση δίνει ιδιαίτερη έμφαση στις κατευθυντήριες γραμμές προς τους ερευνητές και τις οργανώσεις του τομέα, όπου περιλαμβάνονται:

- πρωτόκολλα κρυπτογράφησης και ασφάλειας που πρέπει να σχεδιαστούν από ειδικούς στα πρωτόκολλα κρυπτογράφησης παρά από ειδικούς στη δικτύωση και τα πρωτόκολλα. Επιπρόσθετα, οι ερευνητές πρέπει να απλοποιήσουν την ανάλυση και να δώσουν στα αυτοματοποιημένα εργαλεία τη δυνατότητα να παρέχουν ισχυρές υπολογιστικές εγγυήσεις.
- Απαιτείται να δοθεί μεγαλύτερη προσοχή στην αυτοματοποιημένη επαλήθευση, ώστε η εφαρμογή ενός πρωτοκόλλου να μπορεί να επιτυγχάνει δεδομένους στόχους ασφαλείας, αλλά και να εξεταστεί το πώς τα αυτοματοποιημένα εργαλεία μπορούν να εγγυηθούν σωστή εφαρμογή ενός σχεδίου πρωτοκόλλου.
- Οι μικρές αμελητέες αλλαγές στα πρωτόκολλα μπορούν να οδηγήσουν σε ακύρωση των αποδείξεων της εγγύησης.

- Μελλοντικά πρωτόκολλα θα πρέπει να σχεδιαστούν χρησιμοποιώντας αφενός αξιόπιστες και αναγνωρισμένες αρχές μηχανικής και αφετέρου ευκολία τυπικής ανάλυσης ασφάλειας, ενώ σε συνδυασμό με την ανάπτυξη τυπικών αποδείξεων, να σχεδιαστούν με κρυπτανάλυση των αρχέγονων συστατικών μερών τους.
- Τα μελλοντικά πρωτόκολλα δεν θα πρέπει να είναι πολυπλοκότερα απ' όσο χρειάζεται.
- Χρειάζεται περισσότερη δουλειά σε σχέση με την επαλήθευση των διεπαφών προγράμματος εφαρμογής (API) για τα πρωτόκολλα εφαρμογής.

Ο Udo Helmbrecht δήλωσε σχετικά με τις εκθέσεις: *«Αυτό που επισημαίνεται είναι η ανάγκη συστημάτων πιστοποίησης σε όλες τις φάσεις του τεχνολογικού κύκλου ζωής. Οι ενσωματωμένες διαδικασίες και τα προϊόντα που χαρακτηρίζονται από 'ασφάλεια εκ κατασκευής ή εξ ορισμού' αποτελούν βασικές αρχές εμπιστοσύνης. Η τυποποίηση της διαδικασίας είναι απαραίτητο στοιχείο για να διασφαλιστεί η σωστή εφαρμογή της μεταρρύθμισης για προστασία των δεδομένων στην υπηρεσία των πολιτών και της εσωτερικής αγοράς της ΕΕ. Οι κατευθυντήριες γραμμές του ENISA επιδιώκουν να παράσχουν το σωστό πλαίσιο για διασφάλιση των ηλεκτρονικών συστημάτων».*

Ο Κανονισμός (ΕΕ) αριθ. 611/2013 αναφέρει τον ENISA ως συμβουλευτικό όργανο, το οποίο βρίσκεται σε διαδικασία συγκρότησης καταλόγου κατάλληλων προστατευτικών μέτρων κρυπτογράφησης για προστασία των προσωπικών δεδομένων. Οι κατευθυντήριες γραμμές του ENISA για την κρυπτογράφηση θα πρέπει να χρησιμεύσουν ως έγγραφο αναφοράς. Στο πλαίσιο αυτό, οι παρεχόμενες κατευθυντήριες αρχές είναι μάλλον συντηρητικές με βάση την τρέχουσα σύγχρονη έρευνα, ενώ έχουν ως αντικείμενο την κατασκευή νέων εμπορικών συστημάτων με μεγάλο κύκλο ζωής.

Για τις πλήρεις εκθέσεις: «Αλγόριθμοι, μέγεθος κλειδιών και παράμετροι» & «Μελέτη για τα πρωτόκολλα κρυπτογράφησης»

Για συνεντεύξεις και περαιτέρω πληροφορίες: press[at]enisa.europa.eu