10/12/2010

www.enisa.europa.eu

Ασφάλεια. Υπάρχει κάποια εφαρμογή γι' αυτό; Ο ευρωπαϊκός οργανισμός ασφάλειας του κυβερνοχώρου τονίζει τους κινδύνους και τις ευκαιρίες που παρουσιάζουν τα έξυπνα τηλέφωνα

Μια νέα έκθεση του ENISA αναγνωρίζει τους κορυφαίους κινδύνους και ευκαιρίες της χρήσης έξυπνων τηλεφώνων και προσφέρει πρακτικές συμβουλές ασφαλείας για επιχειρήσεις, ιδιώτες και κρατικούς φορείς. Οι κορυφαίοι κίνδυνοι περιλαμβάνουν λογισμικό κατασκόπευσης, κακή εκκαθάριση δεδομένων κατά την ανακύκλωση των τηλεφώνων, τυχαία διαρροή δεδομένων, και μη εξουσιοδοτημένες κλήσεις και αποστολή SMS σε αριθμούς υψηλής χρέωσης.

Οι πωλήσεις έξυπνων τηλεφώνων διπλασιάστηκαν παγκοσμίως πέρυσι (Gartner) ενώ 80 εκατομμύρια πωλήθηκαν μόνο το τρίτο τρίμηνο του 2010 σε όλο τον κόσμο. Η νέα έκθεση του ENISA σχετικά με τους κινδύνους και τις ευκαιρίες ασφαλείας των έξυπνων τηλεφώνων έρχεται την κατάλληλη στιγμή. Αν είστε ένας από τους εκατοντάδες εκατομμύρια χρήστες έξυπνων τηλεφώνων παγκοσμίως, μάλλον περνάτε περισσότερο χρόνο με το τηλέφωνό σας απ' ό,τι με τη σύζυγό σας. Ενώ με τη μεγάλη σειρά εφαρμογών και αισθητήρων, ίσως να γνωρίζει περισσότερα για εσάς απ' ό,τι εκείνη. Αυτοί οι σύντροφοι ζωής αποτελούν πλέον ένα απαραίτητο εργαλείο σε όλους τους κοινωνικούς χώρους, από τους υψηλά ιστάμενους κρατικούς αξιωματούχους έως τις επιχειρήσεις και τους καταναλωτές. Είναι διάσημα για την ποικιλία λειτουργιών που προσφέρουν. Ένα έξυπνο τηλέφωνο μπορεί να είναι ένα πορτοφόλι που δεν χρειάζεται να αγγίξετε, τηλέφωνο με φωτογραφική μηχανή ή βίντεο, συσκευή ανάγνωσης γραμμικού κώδικα, συσκευή αποστολής και λήψης ηλεκτρονικού ταχυδρομείου, ή τρόπος πρόσβασης κοινωνικών δικτύων. «Δεδομένης της όλο και αυξανόμενης σημασίας των έξυπνων τηλεφώνων για τις ευρωπαϊκές επιχειρήσεις, τα κράτη και τους πολίτες, θεωρούμε απαραίτητη την αξιολόγηση των θεμάτων ασφάλειας και ιδιωτικότητας» λέει ο καθηγητής Dr.Udo Helmbrecht, Εκτελεστικός Διευθυντής του ENISA.

Στη νέα έκθεση, ο ENISA αναλύει τους βασικούς κινδύνους και ευκαιρίες που αφορούν την ασφάλεια. Ορισμένοι από τους βασικούς κινδύνους είναι:

- Τυχαία διαρροή ευαίσθητων δεδομένων –π.χ. δεδομένα GPS προσαρτημένα σε εικόνες.
- Κλοπή δεδομένων από κακόβουλες εφαρμογές και από κλεμμένα, απωλεσθέντα ή εκτός λειτουργίας τηλέφωνα.
- Λογισμικό υποκλοπής «Diallerware» - κακόβουλο λογισμικό που κλέβει χρήματα μέσω μη εξουσιοδοτημένων τηλεφωνικών κλήσεων.
- Υπερφόρτωση υποδομών δικτύων λόγω των εφαρμογών έξυπνων τηλεφώνων.

Όσον αφορά τις ευκαιρίες, η δημιουργία εφεδρικών αντιγράφων είναι συχνά πολύ καλά ενσωματωμένη στις πλατφόρμες των έξυπνων τηλεφώνων, καθιστώντας έτσι εύκολη την ανάκτηση δεδομένων αν το τηλέφωνο χαθεί ή κλαπεί. Μια άλλη ευκαιρία βρίσκεται στη χρήση των καταστημάτων εφαρμογών. «Οι περισσότεροι χρήστες έξυπνων τηλεφώνων εγκαθιστούν λογισμικό τρίτων μόνο διαμέσου των ελεγχόμενων καναλιών διανομής λογισμικού» λέει ο Dr. Marnix Dekker, ένας από τους συντάκτες της έκθεσης.

Το σημαντικότερο αποτέλεσμα της έκθεσης είναι ένα ολοκληρωμένο σύνολο στρατηγικών για τη διασφάλιση των έξυπνων τηλεφώνων. «Τα έξυπνα τηλέφωνα αποτελούν θησαυροφυλάκιο ευαίσθητων και προσωπικών στοιχείων – είναι ζωτικής σημασίας να κατανοήσουμε τον τρόπο διατήρησης του ελέγχου αυτών των στοιχείων. Οι προτάσεις μας έχουν σχεδιαστεί ώστε να ταιριάζουν με συνήθεις πολιτικές ασφαλείας» λέει ο Dr. Giles Hogben, ένας από τους συντάκτες της έκθεσης. Η έκθεση περιλαμβάνει προτάσεις για επιχειρήσεις, ανώτατους αξιωματούχους και καταναλωτές, όπως και για την αντιμετώπιση κινδύνων ασφαλείας όταν οι ρόλοι αυτοί αναμιγνύονται.

Διαβάστε ολόκληρη την έκθεση.

Πρόσθετο υλικό: video clips

Συχνές ερωτήσεις σχετικά με την ασφάλεια των έξυπνων τηλεφώνων

Για συνεντεύξεις: Ulf Bergstrom, Εκπρόσωπος Τύπου, ENISA, press@enisa.europa.eu , Κινητό: +30-6948-460143, ή για περαιτέρω πληροφορίες: Dr Marnix Dekker, marnix.dekker@enisa.europa.eu.

Μετάφραση. Το αγγλικό πρωτότυπο είναι η μόνη έγκυρη εκδοχή.