Ασφάλεια καταστημάτων εφαρμογών – πέντε γραμμές άμυνας – Νέα έκθεση από τον Οργανισμό Κυβερνοασφάλειας ENISA

Ο ENISA δημοσιεύει σήμερα μία νέα έκθεση σχετικά με την Ασφάλειατωνκαταστημάτων εφαρμογώνστην οποία τάσσεται υπέρ της υιοθέτησης μίας βασικής ομάδας 'Πέντε γραμμών άμυνας 'ενάντια στο κακόβουλο λογισμικό (malware).

Η εκρηκτικά αυξανόμενη βιομηχανία έξυπνων τηλεφώνων χρησιμοποιεί μία ειδική μέθοδο για την παροχή λογισμικού στους τελικούς χρήστες: τα καταστήματα εφαρμογών γνωστά και ως *app-stores*. Τα δημοφιλή καταστήματα εφαρμογών έχουν εκατοντάδες χιλιάδες εφαρμογές που καλύπτουν τα πάντα, από ηλεκτρονικές τραπεζικές συναλλαγές μέχρι εντομοαπωθητικά, με τα πλέον δημοφιλή καταστήματα (π.χ. Apple app-store, Google Android market) να απαριθμούν δισεκατομμύρια λήψεις εφαρμογών.

Τα καταστήματα εφαρμογών όμως δεν έχουν διαφύγει της προσοχής των εισβολέων του κυβερνοχώρου. Καθ' όλη τη διάρκεια του 2011 εντοπίστηκανπολυάριθμεςεφαρμογές κακόβουλου λογισμικού, που στόχευαν ένα πλήθος από μοντέλα έξυπνων τηλεφώνων. ΟΔρ. Marnix Dekker και ο Δρ. Giles Hogben, συντάκτες της έκθεσης, αναφέρουν: «*Χρησιμοποιώντας εφαρμογές κακόβουλου λογισμικού, οι εισβολείς μπορούν εύκολα να αποκτήσουν πρόσβαση στις τεράστιες ποσότητες προσωπικών δεδομένων που επεξεργάζονται τα έξυπνα τηλέφωνα, όπως για παράδειγμα απόρρητες επιχειρηματικές διευθύνσεις ηλεκτρονικού ταχυδρομείου, δεδομένα εντοπισμού θέσης, τηλεφωνικές κλήσεις, μηνύματα SMS και ούτω καθεξής. Οι καταναλωτές σχεδόν πάντα έχουν πλήρη άγνοια ότι συμβαίνει κάτι τέτοιο.*»

«Πέντε γραμμές άμυνας» για την ασφάλεια των καταστημάτων εφαρμογών

Ξεκινώντας από ένα μοντέλο απειλής για τα ηλεκτρονικά καταστήματα εφαρμογών, η έκθεση προσδιορίζει αυτό που ονομάζει «**πέντε γραμμές άμυνας**» που πρέπει να υφίστανται για να προστατεύονται τα καταστήματα εφαρμογών από το κακόβουλο λογισμικό: **η αξιολόγηση της εφαρμογής, η καλή φήμη, οι μηχανισμοί απενεργοποίησης, η ασφάλεια της συσκευής** και **οι απομονώσεις**. «*Η παρούσα αναφορά προσφέρει μία άκρως πρακτική και τεχνική ανάλυση των απειλών κακόβουλου λογισμικού για τα καταστήματα εφαρμογών σε λιγότερο από 20 σελίδες. Ο Οργανισμός έχει προβεί σε μία εξαιρετική επιλογή τεχνικών προστασίας, και οι προτάσεις του είναι άμεσα υλοποιήσιμες,*» δήλωσε ο Raoul Chiesa, ένας Ιταλός ηθικός hacker και ειδικός στην κυβερνοασφάλεια.

Χωρίς να παραβλέπει τις διαφορές ανάμεσα στα διάφορα μοντέλα έξυπνων τηλεφώνων και τα αντίστοιχα καταστήματα εφαρμογών, ο ENISA προτείνει μία συνολική προσέγγιση για την αντιμετώπιση των επισφαλών και κακόβουλων εφαρμογών. «*Ο αριθμός των επιθέσεων κακόβουλου λογισμικού απευθείας στα έξυπνα τηλέφωνα ωχριά ακόμα σε σχέση με τις επιθέσεις που δέχονται οι ηλεκτρονικοί υπολογιστές. Η παρούσα έκθεση είναι ένα προσχέδιο για τον τρόπο διατήρησης του εν λόγω πλεονεκτήματος και την αντιμετώπιση της ασφάλειας σε*

όλα τα καταστήματα εφαρμογών.» δήλωσε ο καθηγητής Udo Helmbrecht, Εκτελεστικός Διευθυντής του ENISA.

Για την πλήρη έκθεση:

Ιστορικό: Το κακόβουλο λογισμικό στα καταστήματα εφαρμογών δεν αποτελεί τη μοναδική απειλή για τους χρήστες έξυπνων τηλεφώνων. Ο ENISA δημοσίευσε πρόσφατα μίαπλήρη επισκόπηση των κινδύνων των έξυπνων τηλεφώνων.

Πηγή: ENISA - Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών

Για συνεντεύξεις: Ulf Bergstrom, Εκπρόσωπος, ENISA, press@enisa.europa.eu, Κινητό τηλ.: +30-6948-460-143 ή Δρ. Marnix Dekker, Εμπειρογνώμονας, ENISA marnix.dekker@enisa.europa.eu

Η αγγλική έκδοση είναι η μόνη έγκυρη έκδοση.