[έρευνα Kaspersky] Ενας στους τρεις χρήστες mobile συσκευών στην Ευρώπη δεν αισθάνεται ασφαλής με τις e-συναλλαγές

Προβληματίζουν οι αγορές μέσω tablets ή smartphones

Της Μελίνας Καλαμπόκα
mkal@naftemporiki.gr

Σοβαρά εμπόδια για τις ηλεκτρονικές αγορές μέσα από τα tablets ή τα smartphones υπογραμμίζει η πρόσφατη έρευνα Kaspersky Consumer Security Risks, καθώς ανέδειξε ότι ένας στους τρεις χρήστες mobile συσκευών στην Ευρώπη δεν αισθάνεται ασφαλής να πραγματοποιεί ηλεκτρονικές πληρωμές με smartphones ή tablets. Ο βασικότερος λόγος είναι ότι δεν πιστεύουν πως οι φορητές συσκευές είναι επαρκώς προστατευμένες όσον αφορά αγορές στο διαδίκτυο ή όταν χρησιμοποιούν online banking. Τα ηλεκτρονικά καταστήματα, οι ηλεκτρονικές πληρωμές και τα συστήματα e-banking έχουν κάνει τις οικονομικές συναλλαγές ευκολότερες. Σήμερα, οι χρήστες μπορούν να πληρώσουν λογαριασμούς, να αγοράσουν σπάνια αντικείμενα και να πραγματοποιήσουν συναλλαγές με μερικά μόνο κλικ, χωρίς να σπαταλούν χρόνο σε ουρές. Η ευρεία χρήση των smartphones και των tablets κάνει τις online τραπεζικές συναλλαγές ακόμα πιο εύκολες. Με τα ειδικά χαρακτηριστικά αυτών των gadgets, οι χρήστες μπορούν να διαχειριστούν τα πάντα, όχι μόνο όταν βρίσκονται στο σπίτι ή στο γραφείο, αλλά απ' όπου υπάρχει πρόσβαση στο Internet ή σήμα στο κινητό.

Online πωλήσεις

Σύμφωνα με την έρευνα, όμως, το 33% των ερωτηθέντων στην Ευρώπη δεν θα χρησιμοποιούσε μια φορητή συσκευή για online συναλλαγές, όπως η αγορά προϊόντων σε online καταστήματα. Ενα ελαφρώς μικρότερο, αλλά καθόλου ευκαταφρόνητο, ποσοστό κατόχων smartphones και tablets (31%) δεν αισθάνεται άνετα με τη χρήση των συσκευών του για ηλεκτρονικές τραπεζικές συναλλαγές. Μόνο το 23% των χρηστών smartphones και το 45% των χρηστών tablets δεν ανησυχούν με την εισαγωγή οικονομικών πληροφοριών στα gadgets τους. Το Android είναι το πιο δημοφιλές λειτουργικό σύστημα φορητών συσκευών στον κόσμο και -ως εκ τούτου- αποτελεί συχνότερα θύμα επιθέσεων από ψηφιακούς εγκληματίες. Αυτό είναι λογικό, δεδομένου του ότι όσο περισσότεροι χρήστες στοχοποιούνται, τόσο πιο εύκολο είναι για τους απατεώνες να αντλήσουν παράνομα έσοδα. Σύμφωνα με την Kaspersky Lab, το 99% των δειγμάτων mobile malware έχει αναπτυχθεί για το Android. Το 2012 οι ειδικοί της εταιρείας εντόπισαν 35.000 δείγματα malware για Android. Στο πρώτο εξάμηνο του 2013 ο αριθμός αυτός αυξήθηκε και ξεπέρασε τα 47.000.

> Επερχόμενοι κίνδυνοι

Αλλες απειλές αποτελούν η νέα εξάπλωση κακόβουλου κώδικα με τη μορφή ransomware, τα botnets που εξακολουθούν να εμφανίζονται και μάλιστα ακόμη πιο περίπλοκα, οι απειλές 64-bit, οι κακόβουλοι κώδικες που προσπαθούν να αποκτήσουν κέρδη από την κλοπή ηλεκτρονικών νομισμάτων κ.ά. Τέλος, μία πληθώρα μη παραδοσιακών συσκευών, όπως έξυπνα αυτοκίνητα, κονσόλες παιχνιδιών, έξυπνες τηλεοράσεις κ.α., αποτελούν μία κατηγορία στην οποία μελλοντικά υπάρχει η πιθανότητα να εμφανιστούν απειλές.

Για τον παραπάνω λόγο, το 11% των ερωτηθέντων στην Ευρώπη ανέφερε ότι δεν θα χρησιμοποιούσε το Android για χρηματοοικονομικές συναλλαγές. Οι πλαστές εφαρμογές Android για online τραπεζικές λειτουργίες, οι επιθέσεις phishing και οι επιθέσεις που αναπτύχθηκαν για να υποκλέπτουν τα δεδομένα του χρήστη μέσω του πληκτρολογίου είναι μερικά από τα κακόβουλα εργαλεία που έχουν χρησιμοποιηθεί συχνότερα στις επιθέσεις εναντίον των κατόχων συσκευών Android. Σε γενικές γραμμές η έρευνα αναφέρει ότι δεν μπορεί κάποιος να κατηγορήσει τους κατόχους smartphones και tablets ότι είναι υπερβολικά προσεκτικοί κατά την πραγματοποίηση οικονομικών συναλλαγών. Ωστόσο, παρά την αύξηση του αριθμού των απειλών για το Android, οι χρήστες μπορούν να πραγματοποιούν πληρωμές μέσω φορητών συσκευών, προστατεύοντας τη συσκευή τους με μια αξιόπιστη λύση ασφάλειας. [SID:8426995]

ΣΥΧΝΕΣ ΑΠΕΙΛΕΣ ΚΑΙ ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

▼ Για να προστατεύσει τους χρήστες Android συσκευών από τους ψηφιακούς εγκληματίες, η Kaspersky Lab αναφέρει ότι υπάρχουν λύσεις ασφαλείας που διαθέτουν μια ποικιλία μηχανισμών προστασίας, οι οποίοι είναι σε θέση να παρέχουν υψηλής ποιότητας ασφάλεια στους ιδιοκτήτες φορητών συσκευών. Οι προηγμένες τεχνολογίες ανίχνευσης κακόβουλου λογισμικού εμποδίζουν την εγκατάσταση spyware που «μιμείται» τραπεζικές εφαρμογές, ακόμη και αν αυτό το πρόγραμμα έχει κατέβει από τα επίσημα καταστήματα. Το ενσωματωμένο σύστημα anti-phishing εντοπίζει και μπλοκάρει τις πλαστές σελίδες τραπεζών, ηλεκτρονικών καταστημάτων και συστημάτων ηλεκτρονικών πληρωμών, οι οποίες χρησιμοποιούνται συχνά από τους απατεώνες για να ξεγελαστούν τα θύματα και να αποκαλύψουν στοιχεία σύνδεσης και στοιχεία λογαριασμού. Μια άλλη ειδική λειτουργία που προσφέρει αρκετές λύσεις είναι η δυνατότητα ελέγχου των web links που λαμβάνονται μέσω γραπτών μηνυμάτων, προστατεύοντας τους χρήστες από κακόβουλες επιθέσεις μέσω μαζικής αποστολής SMS, οι οποίες χρησιμοποιούνται συχνά από τους ψηφιακούς εγκληματίες.

Την ίδια στιγμή η ESET παρουσίασε τις ετήσιες προβλέψεις για τις απειλές που θα απασχολήσουν τους χρήστες κατά το επερχόμενο έτος.

Στην έκθεση αναλύονται τρεις κυρίως κατηγορίες, οι οποίες θα απασχολήσουν τους χρήστες κατά το 2014, η απώλεια προσωπικών δεδομένων και οι μηχανισμοί βελτίωσης της προστασίας στο Διαδίκτυο, θέματα όπως η τάση του cloud και πως επηρεάζει τα προσωπικά δεδομένα και οι συζητήσεις σχετικά με το πώς μπορούν οι χρήστες να προστατεύσουν τις πληροφορίες τους στο διαδίκτυο.

Στην έκθεσή της για το 2013, η ESET είχε ήδη προβλέψει τη μεγάλη αύξηση του κακόβουλου λογισμικού στα Android. Συγκρίνοντας τις ανιχνεύσεις που πραγματοποιήθηκαν το 2012 με αυτές του 2013, το ποσοστό εμφανίζεται αυξημένο περισσότερο από 60%. Η σημαντική αυτή αύξηση θα συνεχιστεί και το 2014.