31 Ιανουαρίου 2017

Πόσος χρόνος χρειάζεται για να παρακαμφθεί η ασφάλεια της πιστωτικής σας κάρτας;

/ Επιστήμες, Τέχνες & Πολιτισμός



Μόλις 6 δευτερόλεπτα απαιτούνται, για να μαντέψει κάποιος hacker τα στοιχεία της.

Οι διαδικτυακές συναλλαγές αποτελούν πλέον κομμάτι της καθημερινότητάς μας,

ενώ έχουν χωρίς αμφιβολία διευκολύνει σημαντικά τη ζωή μας, αφού μας επιτρέπουν να αγοράσουμε αγαθά και υπηρεσίες με μόλις λίγα κλικ του ποντικιού και σε ελάχιστο χρόνο. Αυτό βέβαια δεν σημαίνει ότι δεν έχουν και ορισμένα μειονεκτήματα. Το σημαντικότερο είναι ο κίνδυνος υποκλοπής των στοιχείων της πιστωτικής ή της χρεωστικής μας κάρτας από επιτήδειους, που με αυτό τον τρόπο μπορούν να μας αποσπάσουν χρήματα – με άμεσο ή έμμεσο τρόπο.

Φυσικά, για να αποφευχθεί η οποιαδήποτε κακόβουλη ενέργεια, υπάρχουν αρκετοί μηχανισμοί ασφαλείας, που θεωρητικά προστατεύουν τις ηλεκτρονικές συναλλαγές. Όμως φαίνεται ότι στην περίπτωση των καρτών Visa, αυτοί δεν επαρκούν για να προστατέψουν τους χρήστες.

Αναρίθμητες προσπάθειες

Συγκεκριμένα, ερευνητές του Πανεπιστημίου του Νιουκάστλ ανακάλυψαν δύο νέες ευπάθειες του συστήματος της εταιρείας, που μπορούν να επιτρέψουν την έκθεση των στοιχείων μιας κάρτας μέσα σε μόλις 6 δευτερόλεπτα.

Τα συγκεκριμένα κενά ασφαλείας συνοψίζονται στα παρακάτω σημεία:

Ο μηχανισμός ασφαλείας του συστήματος Visa δεν μπορεί να διακόψει ύποπτα αιτήματα πληρωμών, εάν αυτά πραγματοποιηθούν διαδοχικά σε διαφορετικές ιστοσελίδες.

Οι ρουτίνες ελέγχου πολλών websites δεν είναι σταθερές, με αποτέλεσμα να ζητούνται διαφορετικά στοιχεία μιας κάρτας, κάθε φορά που αυτή χρησιμοποιείται.

Έτσι, είναι εύκολο κάποιος με την κατάλληλη τεχνογνωσία και ειδικά σχεδιασμένο λογισμικό, να αποκτήσει πρόσβαση σε πληροφορίες, όπως η ημερομηνία λήξης μιας πιστωτικής κάρτας, ο κωδικός επαλήθευσης CVV [Card Verification Code] και ο ταχυδρομικός κώδικας που σχετίζεται με αυτή. Το CCS2015 είναι ένα software εργαλείο που μπορεί να συλλέξει όλα αυτά τα δεδομένα αυτόματα, καλώντας διαδοχικά τα συστήματα online πληρωμών πολλών ιστοσελίδων. Στην πράξη δηλαδή αξιοποιεί μια μέθοδο Brute Force, που επιχειρεί να μαντέψει τα σωστά στοιχεία μέσω συνεχών δοκιμών.

Ευάλωτος μηχανισμός ασφαλείας

Για να εξαχθεί η ημερομηνία λήξης μιας κάρτας Visa δεν χρειάζονται περισσότερες από 60 προσπάθειες, ενώ για την εύρεση του κωδικού CVV απαιτούνται λιγότερες από 1.000 απόπειρες. Λαμβάνοντας υπόψιν ότι υπάρχουν εκατοντάδες χιλιάδες εμπορικές ιστοσελίδες στο Διαδίκτυο, καταλαβαίνετε ότι

μέσω της συγκεκριμένης προσέγγισης, ο επιτιθέμενος δεν θα δυσκολευτεί ιδιαίτερα να αποσπάσει, σε σύντομο χρονικό διάστημα, όλα τα δεδομένα που χρειάζεται.

Αυτό πάντως που καθιστά την εν λόγω τεχνική ακόμα πιο επικίνδυνη, είναι ότι ο μηχανισμός ασφαλείας του συστήματος Visa – και συνεπώς οι τράπεζες με τις οποίες αυτό συνδέεται, δεν μπορούν να ανιχνεύσουν μια τέτοια κακόβουλη ενέργεια. Με λίγα λόγια, ο hacker μπορεί να αποκτήσει τον πλήρη έλεγχο μιας πιστωτικής κάρτας και να προλάβει να την χρησιμοποιήσει, πολύ πριν ο κάτοχός της αντιληφθεί ότι κάτι δεν πάει καλά.

Αξίζει να σημειωθεί ότι η Mastercard μπλοκάρει τη χρήση μιας κάρτας μετά από 10 αποτυχημένες απόπειρες υποκλοπής στοιχείων, περιορίζοντας έτσι σημαντικά τον κίνδυνο απώλειας χρημάτων.

Ο Δρ. Martin Emms, ένας από τους ερευνητές που αποκάλυψαν το συγκεκριμένο πρόβλημα, εξήγησε ότι μέχρι η Visa και τα διάφορα εμπορικά websites να δημιουργήσουν ένα ικανό αντίμετρο στις επιθέσεις αυτού του τύπου, οι χρήστες θα πρέπει μόνοι τους να φροντίζουν για την ασφάλεια της πιστωτικής τους κάρτας, αλλά και να είναι προετοιμασμένοι να αντιδράσουν άμεσα, εάν υποψιαστούν ότι τα στοιχεία της έχουν εκτεθεί.

Πηγή: gr.pcmag.com