27 Απριλίου 2015

IT Security: αμελείς users, κακοί hackers…

/ Πεμπτουσία

Image not found or type unknown

IT Security: Πώς οι χρήστες και τα endpoints τους γίνονται αντικείμενο εκμετάλλευσης από τους «κακούς hackers», οι οποίοι θα βρουν τελικά το δρόμο τους στα κρίσιμα δεδομένα τους.

Είναι γνωστό ότι οι χρήστες είναι ο πιο αδύναμος κρίκος όσον αφορά το IT Security chain σε παγκόσμιο επίπεδο, και ιδιαίτερα οι αμελείς ή οι αμόρφωτοι χρήστες. Αλλά πώς ακριβώς οι «κακοί hackers» εκμεταλλεύονται αυτήν την άγνοια ή την αμέλεια για να «σπάσουν» τα endpoints των χρηστών και να εισβάλλουν σε εταιρικούς λογαριασμούς; Πολλές από τις μεθόδους που χρησιμοποιούν αφορούν μόνο ένα μικρό κομμάτι της ψυχολογικής ταχυδακτυλουργίας, διότι το phishing και το social engineering τείνουν να διαδραματίσουν σημαντικό ρόλο στην πλειονότητα των επιθέσεων. Εδώ είναι μερικοί από τους καλύτερους – χειρότερους τρόπους που οι ίδιοι οι χρήστες «αφήνουν τα χαρτιά τους ανοιχτά» σε ενδεχόμενη επίθεση.

1. **Το να «πιαστείτε» σε ένα Phishing δόλωμα**

Το πρώτο στην λίστα και το πιο απλό τέχνασμα που χρησιμοποιούν οι χάκερς για να ξεκινήσουν μια ισχυρή και εξελιγμένη επίθεση στα συστήματα των χρηστών είναι το phishing. Παραμένει ο καλύτερος φίλος ενός χάκερ επειδή απλά

λειτουργεί. Σύμφωνα με το Verizon Data Breach Investigation Report μέσα σε μια εβδομάδα, το 23% των παραληπτών μηνυμάτων phishing ανοίγουν τα κακόβουλα μηνύματα και 11% ανοίγουν τα συνημμένα αρχεία που περιέχονται σε αυτά. Όπως έχουμε αναφέρει και σε πρόσφατο άρθρο μας, χρειάζονται μόλις 82 δευτερόλεπτα από τη στιγμή που μια εκστρατεία phishing ξεκινά, για να αρχίσουν οι χρήστες να «τσιμπούν» τα ψεύτικα δολώματα.

2. **Το να απαντάτε σε ψεύτικες τηλεφωνικές κλήσεις**

Κινούμενοι στο ίδιο μοτίβο, όπως και στο phishing, μερικές φορές ο ευκολότερος τρόπος για τους επιτιθέμενους να αποκτήσουν πρόσβαση στα συστήματα των χρηστών και των λογαριασμών τους, είναι απλώς να ρωτήσουν για αυτό. Η κλασσική μέθοδος του social engineering είναι ένα παλιό stand-by. Πολλές φορές το μόνο που χρειάζεται είναι μια κλήση από τους χάκερς προς το θύμα προσποιούμενοι τον IT και ένα request για το user's login και το password. Ή θα μπορούσαν να προσποιηθούν ότι είναι ένας εσωτερικός υπάλληλος ή επιχειρηματικός συνέταιρος και να ζητήσει από τον εργαζόμενο να ανοίξει ένα συγκεκριμένο έγγραφο, που είναι στην πραγματικότητα ένα remote access σε Trojan.

Πηγή: secnews.gr

(Το παρόν άρθρο αποτελεί το α' μέρος του αφιερώματος «IT Security: Τα 7 θανάσιμα αμαρτήματα που πρέπει να αποφύγετε»)