30 Ιουνίου 2014

Πρόσβαση hackers στον υπολογιστή σας: οι 5 κερκόπορτες…

Επιστήμες / Πληροφορική & Internet

Οι εταιρείες παροχής ασφάλειας έχουν ένα μυστικό που δεν θέλουν να γνωρίζουμε: ακόμα και αν έχεις εγκαταστήσει το καλύτερο λογισμικό ασφάλειας, ο υπολογιστής σου δεν είναι και πάλι ασφαλής από τους hackers. Ακόμα και αν απενεργοποιήσεις τη σύνδεση στο διαδίκτυο και πάρεις το laptop και πας στην έρημο, μπορείς και πάλι να δεχθείς επίθεση.

Παρακάτω σας αναφέρουμε πέντε τρόπους που ο υπολογιστής μας πιθανώς να

είναι ευάλωτος:

Ευπάθεια Νο 1 – Κοινωνική Μηχανική

Εάν έχετε έναν λογαριασμό ηλεκτρονικού ταχυδρομείου, ίσως να λαμβάνετε καθημερινά μερικά ανεπιθύμητα μηνύματα, τα οποία φυσικά θα έχουν προσπεράσει το φίλτρο ανεπιθύμητης αλληλογραφίας. Πολλά από αυτά τα emails, προσπαθούν να σας εξαπατήσουν ζητώντας σας να ανοίξετε κάποιο αρχείο ή να εγκαταστήσετε ένα συγκεκριμένο πρόγραμμα.

Αν το κάνετε αυτό, κατά πάσα πιθανότητα τα αρχεία αυτά καθώς και τα προγράμματα θα μολύνουν τον υπολογιστή σας, διότι ο Η/Υ σας δεν μπορεί να σας προστατεύσει από τον ίδιο σας τον εαυτό. Φυσικά, αυτό δεν ισχύει για όσους έχουν την ικανότητα να αναγνωρίζουν μια απάτη, ακόμη και όταν βλέπουν ένα νόμιμο email το οποίο φαίνεται ακίνδυνο. Δυστυχώς, αυτό δεν είναι αλήθεια για τους περισσότερους χρήστες ηλεκτρονικών υπολογιστών και στην ουσία οι περισσότεροι δίνουν πρόσβαση από μόνοι τους.

Ευπάθεια Νο 2 – Internet Software

Το firewall αποτρέπει την απομακρυσμένη πρόσβαση των hackers τον υπολογιστή σας, αλλά τι συμβαίνει αν εσείς πάτε στους hackers; Το πρόγραμμα περιήγησης, το πρόγραμμα ηλεκτρονικού ταχυδρομείου της επιφάνειας εργασίας, το Adobe Flash player, Java player και αρκετά άλλα διαδικτυακά παιχνίδια μπορούν να συνδεθούν και με άλλους υπολογιστές μέσω διαδικτύου. Αν έστω ένας από αυτούς τους υπολογιστές έχει παραβιασθεί και αν υπάρχει κάποια ευπάθεια στον δικό σας λογισμικό, ο hacker μπορεί να προσπεράσει το firewall και να αποκτήσει πρόσβαση στο σύστημά σας. Γι’ αυτό θα πρέπει να κρατάμε πάντα ενημερωμένο το λογισμικό μας.

Ευπάθεια Νο 3 – Παιδιά και άπειροι χρήστες

Αν τα παιδιά σας θέλουν να εγκαταστήσουν δωρεάν εφαρμογές από το Internet ή ο σύζυγος plugins για λήψεις βίντεο από ιστοσελίδες ενηλίκων, ο υπολογιστής σας πρόκειται πολύ γρήγορα να παραβιαστεί.

Η θεραπεία για το πρόβλημα αυτό είναι να χρησιμοποιήσετε λογαριασμούς διαχειριστή για Windows, Mac ή Linux. Θέστε ένα άτομο από την οικογένειά σας – αυτόν που ενδιαφέρεται περισσότερο για την ασφάλεια – ως διαχειριστή και όλοι θα πρέπει να του ζητάνε πρόσβαση για να μπορέσουν να εγκαταστήσουν κάτι στον υπολογιστή.

Ευπάθεια #4 – Διαμοιρασμός αρχείων με μολυσμένους υπολογιστές

Οι ιοί σήμερα είναι πολύ πιο έξυπνοι. Μπορούν να εξαπλωθούν χωρίς καν να ανοίξετε το ίντερνετ. Απλά αντιγράφουν τον εαυτό τους σε USB drives και σε μακροεντολές εγγράφων, έτσι ώστε όταν αντιγραφεί ένα αρχείο από έναν μολυσμένο υπολογιστή και μεταφερθεί σε έναν καθαρό, να μπορέσει να τον μολύνει.

Όποτε παίρνετε αρχεία από κάποιον άλλον υπολογιστή, βεβαιωθείτε ότι έχετε κάνει σάρωση των αρχείων με το λογισμικό antivirus πριν τα ανοίξετε.

Ευπάθεια No 5 – Cloud Ανασφάλεια

Έχεις συνηθίσει να διατηρείς τα πάντα σε ψηφιακή μορφή, διότι τα χρειάζεσαι στον υπολογιστή σου, αλλά πιθανότατα να έχεις αποθηκεύσει ορισμένα σημαντικά δεδομένα στην υπηρεσία cloud.

Το email σας είναι σε cloud. Τα backup σας είναι σε cloud οι λογαριασμοί σας, ακόμα και οι φωτογραφίες σας. Αν και η υπηρεσία cloud είναι πιο ασφαλής από το desktop σας, μια ευπάθεια στην εφαρμογή της υπηρεσίας μπορεί να επιτρέψει σε κάποιον hacker να αποκτήσει πρόσβαση στα δεδομένα χιλιάδων ή και εκατομμυρίων χρηστών. Αυτό είναι πιο ελκυστικό για τους hackers.

Οι περισσότερες εφαρμογές cloud ισχυρίζονται ότι είναι ασφαλείς, αλλά αν δεν κρυπτογραφήσετε τα δεδομένα σας πριν τα αποθηκεύσετε, είναι ακόμα ένας δελεαστικός στόχο για τους χάκερ.

Ο μόνος τρόπος να είστε ασφαλείς από τους hackers είναι, ο συνδυασμός ενός καλού λογισμικού ασφάλειας και της εκπαίδευσης. Το λογισμικό παροχής ασφάλειας χωρίς την εκπαίδευση είναι άδικος κόπος.

Πηγή: SecNews.gr

http://bit.ly/1rJs07z