3 Σεπτεμβρίου 2014

Πώς να διατηρήσετε την επιχείρησή σας “ιντερνετικά” ασφαλή

/ Πεμπτουσία· Ορθοδοξία-Πολιτισμός-Επιστήμες

Μετά τα πρόσφατα γεγονότα που σημάδεψαν τη «ζωή» στο διαδίκτυο και όχι μόνο, εννοώντας τις αποκαλύψεις του Wikileaks, πολλές επιχειρήσεις και οργανισμοί άρχισαν να «τρέμουν» για την ασφάλεια των εταιρικών δεδομένων.

Η αυξημένη χρήση των κοινωνικών δικτύων αλλά και νέων τεχνολογιών, όπως οι υπηρεσίες cloud κερδίζουν όλο και περισσότερο την προσοχή των επιχειρήσεων και των εργαζομένων. Αυτό έχει ως αποτέλεσμα να χρησιμοποιούνται ακόμη και στο χώρο εργασίας, χωρίς να ληφθούν τα κατάλληλα μέτρα προστασίας, που θα εξασφαλίσουν το έργο των επιχειρήσεων έναντι των hackers.

Σας παραθέτουμε τρείς σημαντικούς τρόπους για να αντιμετωπίσετε αυτούς τους κινδύνους παρακάτω:

Βήμα 1ο: Αυθεντικοποίηση

Η αυθεντικοποίηση χρησιμοποιεί ένα σύστημα για να επικυρώνει την ταυτότητα του χρήστη. Για περισσότερα από 10 χρόνια οι επιχειρήσεις χρησιμοποιούν αυτό το σύστημα παρέχοντας στους χρήστες – εργαζόμενους κωδικούς πρόσβασης και ονόματα χρηστών, έτσι ώστε να έχουν πρόσβαση διαδικτυακές εφαρμογές και στο εταιρικό πληροφοριακό σύστημα Με αυτόν τον τρόπο κατορθώνεται να δίνονται συγκεκριμένα δικαιώματα στους χρήστες σε εταιρικές εφαρμογές και να γνωρίζετε κάθε φορά ποιος τις χρησιμοποίησε. Μπορείτε να διαχωρίσετε την

πολιτική πρόσβασης ανάλογα με το είδος του χρήστη, δηλ. άλλη για τους εργαζόμενους, διαφορετική για τους συνεργάτες και άλλη για τους πελάτες.

Βήμα 2ο: Εξουσιοδότηση
Η εξουσιοδότηση αφορά την πολιτική ασφάλειας που καθορίζει το είδος των δεδομένων στο οποίο ο χρήστης έχει πρόσβαση. Η αποκάλυψη των εγγράφων στο Wikileaks αποτελεί ένα πολύ καλό παράδειγμα για την κακή διαχείριση της εξουσιοδότησης. Αυτό σημαίνει ότι πολλοί λίγοι είναι εκείνοι που θα έπρεπε να έχουν πρόσβαση σε εμπιστευτικές πληροφορίες, κάτι που δεν ίσχυε στην προκείμενη περίπτωση.

Βήμα 3ο: Καταγραφή και διαχείριση Συμβάντων
Ουσιαστικά η καταγραφή αποτελεί τον έλεγχο και την αξιοπιστία του πληροφοριακού συστήματος. Η πιο διαδεδομένη μέθοδος για να γίνει αυτό εφικτό είναι η ηλεκτρονική ανακάλυψη (e-discovery), μέσω της οποίας όχι μόνο διατηρούμε ιστορικό των αρχείων και των ενεργειών μας, αλλά επίσης βοηθάει και στην εύρεση διαπιστευτηρίων σε περίπτωση συμβάντος. Υπάρχουν πολλές εφαρμογές που μπορούν να σας βοηθήσουν σε αυτό και λειτουργούν συνήθως με την αποστολή ηλεκτρονικού μηνύματος κάθε φορά που καταγράφουν κάτι. Νέες δυνατότητες όμως έρχονται και στο προσκήνιο.

Τα οφέλη που θα αποκομίσετε από τη χρήση αυτών των τεχνολογιών είναι τεράστια σε σύγκριση με τις προσπάθειες που θα καταβάλετε για να τις χρησιμοποιήσετε. Μην αφήσετε το Wikileaks να σας τα «βγάλει στη φόρα»…

Πηγή: SecNews.gr