24 Ιουλίου 2014

Προστασία από επιθέσεις hacking σε ιστοσελίδες WordPress

/ Πεμπτουσία

Image not found or type unknown

Το hacking έχει ξεκινήσει από τη «γέννηση» του Διαδικτύου, αλλά τον τελευταίο καιρό οι διαδικτυακοί εγκληματίες έχουν μεταφέρει τις επιθέσεις σε ένα νέο επίπεδο. Οι διαδικτυακοί εγκληματίες, όχι μόνο παραβιάζουν λογαριασμούς e-mail, προφίλ κοινωνικής δικτύωσης και τραπεζικούς λογαριασμούς, αλλά πλέον επιτίθενται σε ιστοσελίδες για πολλούς λόγους.

Μερικοί hackers προσπαθούν να παραβιάσουν την ιστοσελίδα σας για να έχουν πρόσβαση στο κοινό σας και συνήθως αποστέλλουν spam με άχρηστους συνδέσμους και πολύ αντιεπαγγελματικό περιεχόμενο. Άλλοι hackers απλά ψάχνουν να εισχωρήσουν πιο πολύ στα δεδομένα σας ή να χρησιμοποιήσουν την ιστοσελίδα σας για διασπορά κακόβουλου λογισμικού. Επίσης, οι hackers συνήθως χρησιμοποιούν υπολογιστές-ρομπότ που σχεδιάστηκαν για να εισχωρούν στο WordPress γρήγορα και χωρίς καν να το αντιληφθείτε.

Εάν χρησιμοποιείτε το WordPress για να φιλοξενήσετε την ιστοσελίδα σας, οι πιθανότητες να σας παραβιάσουν είναι υψηλές, καθώς τα υφιστάμενα μέτρα

ασφάλειας δεν είναι αρκετά. Οι hackers γνωρίζουν ακριβώς πώς να σπάσουν τους κωδικούς πρόσβασης, να προσπεράσουν το σύστημα ασφάλειάς σας και να χρησιμοποιήσουν την ιστοσελίδα σας κατά βούληση. Αυτό μπορεί να προκαλέσει τεράστιες απώλειες σε κοινό, αξιοπιστία και πραγματικά να κάνει εσάς ή την επιχείρησή σας να φανεί απίστευτα ευάλωτη. Αν ψάχνετε για καλύτερους τρόπους για την προστασία της ιστοσελίδας σας διαβάστε τα παρακάτω βήματα:

1. **Χρησιμοποιήστε plugin:** Η εγκατάσταση ενός συστήματος ασφάλειας WordPress είναι ότι καλύτερο μπορείτε να κάνετε για να παραμείνετε ασφαλείς και μακριά από hackers. Υπάρχουν μερικές επιλογές, αλλά διαπιστώνουμε ότι το plugin Better WP Security, φαίνεται να καλύπτει περισσότερα κενά από τα υπόλοιπα plugins, προσφέροντας μεγαλύτερη σιγουριά.
2. **Ενισχύστε τον κωδικό πρόσβασης:** Δεν υπάρχει τίποτα άλλο, που οι hackers να μην αγαπούν περισσότερο, παρά ένας απλός κωδικός πρόσβασης, όπως το “1234″ ή το “password”. Αποφύγετε τέτοιους κωδικούς πρόσβασης, και καταλήξτε σε κάτι προσωπικό, περίπλοκο και που δεν θα ξεχάσετε όμως εύκολα.
3. **Δημιουργήστε αντίγραφα ασφαλείας πριν σας παραβιάσουν**: Δεν έχει σημασία τι είδος ιστοσελίδας διαθέτετε, αλλά είναι μια καλή ιδέα να διατηρείτε τακτικά αντίγραφα ασφαλείας για να αποθηκεύσετε τα δεδομένα σας και να εξασφαλίσετε ότι αν δεχθείτε επίθεση, θα εξακολουθεί να υπάρχει όλο το περιεχόμενο της ιστοσελίδας σας.

Πηγή: SecNews.gr