Το site μου έπεσε θύμα κακόβουλης επίθεσης. Τι να κάνω;

- 2019-03-07 - Error Pages

Όταν ένα site είναι online, υπάρχει η περίπτωση να πέσει θύμα κακόβουλης επίθεσης (hacking). Παρακάτω θα δούμε τους λόγους που προκαλούν αυτή την κακόβουλη επίθεση, τις ενέργειες που θα πρέπει να κάνετε έτσι ώστε να αποκαταστήσετε το πρόβλημα αλλά και να το αποφύγετε μελλοντικά.

Αρχικά, θα πρέπει να κάνετε επαναφορά στο site σας σε ημερομηνία που ήταν λειτουργικό. Την επαναφορά αυτή μπορείτε να την πραγματοποιήσετε μέσα από το myTophost Panel σας.

Λόγοι που μπορεί να προκάλεσαν το Hacking και ενέργειες που θα πρέπει να κάνετε:

- Η web εφαρμογή που έχετε χρησιμοποιήσει πιθανό να είχε κάποιο κενό ασφαλείας.

Σε αυτή την περίπτωση, θα πρέπει να αναβαθμίσετε την εφαρμογή σας στην τελευταία της έκδοση

- Έχει γίνει υποκλοπή κωδικών.

Θα πρέπει να αλλάξετε όλους τους κωδικούς που αφορούν τη φιλοξενία σας (FTP/plesk/databases/administrator περιβάλλον της ίδιας της εφαρμογής)

- Δεν έχει αναβαθμιστεί η web εφαρμογή ή τα plugins και themes σε τελευταίες εκδόσεις τους.

Αυτό που θα πρέπει να κάνετε, είναι να αναβαθμίσετε τα plugins και Themes σας στις τελευταίες τους εκδόσεις.

- Υπάρχει κάποιο malware στο PC σας.

Θα πρέπει να σαρώσετε τον υπολογιστή, από τον οποίο ανεβάζετε και κατεβάζετε αρχεία στο site σας.

- Χρησιμοποιείτε κάποιο πειρατικό ή ανεπίσημο λογισμικό.

θα πρέπει να τα προγράμματα που χρησιμοποιείτε να μην είναι σπασμένα, όπως επίσης και να τα αποδέχεται το λειτουργικό του υπολογιστή σας.

- Λάθος δικαιώματα σε αρχεία ή φακέλλους.

Εξετάστε τα δικαιώματα των αρχείων που υπάρχουν στο site σας. Αρχεία στα οποία ο οποιοσδήποτε μπορεί να γράψει (έχουν full permissions ή 777 και φαίνονται στην αντίστοιχη στήλη να έχουν permissions "rwx rwx rwx" στον File Manager του Plesk), θεωρούνται ως τα μεγαλύτερα κενά ασφαλείας. Στην πλειοψηφία των περιπτώσεων τα αρχεία σας θα πρέπει να έχουν 755 permissions (ή "rwx r-x r-x").

Γιατί κάποιος κάνει επίθεση στο site μου;

Κάποιος θέλει να χρησιμοποιήσει το χώρο μας για παράνομες ενέργειες, όπως μαζική αποστολή spam (ανεπιθύμητης αλληλογραφίας) ή υποκλοπή στοιχείων μέσω "ηλεκτρονικού ψαρέματος"- phishing. Τέτοιες ενέργειες επηρεάζουν την αξιοπιστία των υπηρεσιών του server. Για παράδειγμα, αν κάποιο site προκαλεί αποστολή spam αλληλογραφίας, η IP address του server κινδυνεύει να μπει σε blacklist με αποτέλεσμα δυσλειτουργία στην αποστολή email από όλα τα sites που φιλοξενούνται στον συγκεκριμένο server. Σε αρκετές περιπτώσεις αποστέλλεται καταγγελία (abuse) για ύπαρξη phishing σελίδας ή αποστολής spam από το data center.

Τι μπορώ να κάνω για να μην έχω πάλι πρόβλημα στο μέλλον;

Πέρα από τις παραπάνω ενέργειες που θα πρέπει να κάνετε άμεσα, καλό θα είναι να εγκαταστήσετε κάποια security plugin. Παρακάτω θα δούμε περιπτώσεις για τα δύο από τα δημοφιλέστερα CMS, το WordPress και το Joomla.

Σε περίπτωση που χρησιμοποιείτε Joomla, μπορείτε να δείτε security extensions εδώ.

Ένα χρήσιμο Extension του Joomla που ανιχνεύει κακόβουλα αρχεία είναι το Antivirus Website Protection.

Σε περίπτωση που χρησιμοποιείτε WordPress, μπορείτε να δείτε security plugins εδώ.

Τέλος, υπάρχουν site, όπως το sucuri, που απλά δηλώνετε το site σας και πατώντας το scan your site, σας εμφανίζει μία αναλυτική αναφορά για τυχών κακόβουλο λογισμικό επάνω στο χώρο σας.