So schützen Sie Ihr WordPress vor Hackern – 6 einfache Schritte

Sie sind geschockt? Ihr WordPress Blog wurde gehackt? Dabei haben Sie alle aktuellen WordPress Updates gemacht und dachten Ihr Hoster wäre sicher. Genauso ging es mir auch und das war auch der Grund für mich blogVault einzusetzen. Damit Ihnen das nicht (mehr) passiert, möchte ich Ihnen 6 einfache Schritte zeigen, wie Sie Ihr WordPress vor Hackern schützen können.

1.) Sichern Sie Ihr WordPress jeden Tag

Erstellen Sie Backups von Ihrem WordPress-Blog, am besten jeden Tag oder mindestens einmal die Woche. Auch wenn einige Webhoster versprechen Ihre Daten nächtlich zu sichern, würde ich mich nicht 100% darauf verlassen. Was ist wenn Ihr Webhoster nicht erreichbar ist? Was passiert wenn er pleite geht, gehackt wird, von einer DDOS-Attacke erwischt wird, die Festplatte Ihres Servers crasht….. u.s.w.. Sicherlich gibt es Möglichkeiten manuell oder halb-automatisch Backups von Ihrem WordPress zu erstellen.

Fragen Sie sich:

- Können Sie Ihre Backups innerhalb weniger Minuten wieder auf Ihre Webseite zurückspielen?
- Möchten Sie wirklich einem kostenlosen WordPress-Plugin alle Ihre Daten sowie die Zukunft Ihrer Firma oder Webseite überlassen?
- Was passsiert, wenn die gesicherten WordPress-Daten doch nicht vollständig sind, Themedaten, Bilder oder Plugins fehlen?
- Wie sichern Sie eine WordPress-Webseite, die mehr als 1GB groß ist?
- Sie machen jeden Tag ein vollständiges Backup, inklusive aller Änderungen? Nicht wirklich ! 

Das ist einer der Gründe, warum ich blogVault einsetze, da kann ich sicher sein, dass meine Daten mindestens einmal am Tag gesichert werden. Sicherlich kostet blogVault Geld, aber 9€ pro Monat ist mir das Backup meiner Webseiten schon wert. Sie haben noch kein Backup Ihrer WordPress Webseite? Probieren Sie uns 7 Tage kostenlos aus – melden Sie sich hier an!

2.) Hacker müssen draußen bleiben – sichere Passwörter für WordPress einsetzen

Sie können sich keine Passwörter merken? Ihr WordPress Passwort ist vielleicht “admin” oder “passwort” oder sogar “1234″? **Ändern Sie es jetzt sofort!** Sie glauben gar nicht, wie viele Leute solch einfache Passwörter einsetzen. Das ist das Gleiche, wie wenn Sie Ihre Haustür offen stehen lassen würden und noch ein Schild aufstellen “Diebe hereinspaziert”. So einfach wollen wir es den Hackern nicht machen.

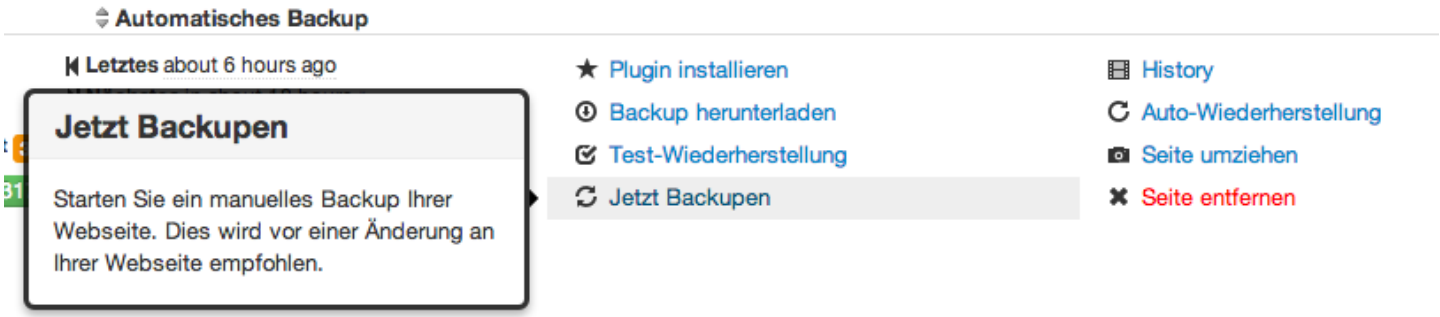
Ihr Passwort sollte mindestens 8 Zeichen lang und Buchstaben, Zahlen sowie Sonderzeichen enthalten. Verwenden Sie ausserdem noch Groß- und Kleinschreibung. Ihr neues Passwort könnten dann z.B. so aussehen: “T1r$iU76D3s§”. Wenn Sie sich das Passwort nicht merken können, verwenden Sie einfach einen kostenlosen Passwort-Manager wie z.B. KeePass (http://keepass.info). Dieser speichert nicht nur Ihre Passwörter, sondern kann diese auch direkt in Ihrem Browser wieder einfügen sowie sichere Passwörter für Ihr WordPress generieren.

Stellen Sie ausserdem sicher nicht bei jeder Webseite oder WordPress-Blog das gleiche Passwort zu benutzen. Sollte Ihr Passwort dann gehackt werden, sind wenigstens Ihre anderen Seiten sicher.

3.) WordPress Updates installieren

WordPress ist keine Software die man einmalig installiert und dann vergessen kann. Es kommen regelmäßig neue Versionen mit neuen Sicherheitsfunktionen und Updates heraus. Stellen Sie sicher, dass Sie immer die aktuellste WordPress Version installiert haben. Ein Update von WordPress geht meistens einfach per Klick.

TIPP: Bevor Sie ein Haupt-Update, also z.B. 3.4 auf 3.5 einspielen, sollten Sie unbedingt eine Backup erstellen. Wenn Sie blogVault im Einsatz haben geht das ganz einfach.



Gehen Sie, wie oben im Screenshot beschrieben, in Ihrem blogVault Dashboard einfach auf den Punkt “Jetzt Backupen”. Warten Sie einige Minuten und prüfen Sie dann im Punkt “History”, ob Ihre letzten Beiträge gesichert wurden. Im Punkt “History” sehen Sie ausserdem, ob und wann Ihr WordPress das letzte mal gesichert wurde.

Sollte jetzt bei Ihrem WordPress-Update irgendetwas schief gehen, können Sie jederzeit einfach per Klick die letzte Version wieder herstellen. So einfach geht das!

Halten Sie ausserdem alle Ihre Plugins immer auf dem aktuellen Stand. So geben Sie Hacker keine Chance Sicherheitslücken in alten Plugins auszunutzen.

4.) Ändern Sie den Standard-Benutzer “Admin”

Bei der Installation Ihres WordPress-Blogs wird automatisch der Benutzer “Admin” vorgeschlagen. Nehmen Sie bitte einen anderen . Am besten nehmen Sie einen Benutzernamen, den man nicht so einfach erraten kann. Das kann Ihr Spitzname sein oder eine kryptische Nummer, was immer Sie sich eben merken können. Sie können auch eine Variation Ihres Webseiten Titels verwenden. Bei uns wäre das z.B. bv1 oder blogvault_blog oder so etwas Ähnliches. Noch besser ist es, einfach ein Login Namen aus der Offline-Welt zu nehmen, z.B. Ihr Nummernschild.

5.) Installieren Sie Sicherheits-Plugins

Es gibt einige Plugins die die Sicherheit Ihres WordPress-Blogs erhöhen. Diese Plugins schränken z.B. den Zugang zu Ihrem WordPress für Hacker ein. Oftmals versuchen nämlich Hacker einfach alle Benutzernamen und Passwörter durch. Dadurch das Ihre Seite ja immer online ist, haben die Hacker ausserdem alle Zeit der Welt. Mit dem Plugin “Limit Login Attempts” können Sie z.B. einstellen, dass nur bestimmte IP-Adressen Zugriff auf Ihr WordPress-Admin Bereich haben. Oder Sie lassen automatisch IP-Adressen sperren, die versuchen nach einer Anzahl Anmeldungen reinzukommen. Das hält die Hacker auf jeden Fall schonmal auf! Zur Not haben Sie ja ausserdem (hoffentlich) noch ein Backup Ihrer WordPress Webseite.

6.) Sichern Sie Ihre “wp-config” Datei ab

Die wp-config.php Datei ist das Rückrat Ihres WordPress Blogs. Diese Datei haben Sie (oder WordPress selbst) bei der Installation angelegt. Sie beinhaltet nicht nur die Login Daten Ihrer Datenbank, sondern auch viele Einstellungen und Konfigurationsdaten Ihrer Webseite.

Die 3 folgenden Änderungen sichert Ihre “wp-config.php” Datei vor Hackern ab:

1. **Ändern Sie den Datenbank “Prefix” - ($table_prefix)**
   Das ist quasi das “Wort” welches vor den Datenbankeinträgen von WordPress steht. Standardmäßig lautet es “wp_”. Ändern Sie es ab, am besten zu einem Begriff der nicht so leicht zu erraten ist z.B. “adb_”. Wichtig ist jedoch das auf jeden Fall “_” am Ende des Wortes steht.
2. **“Themes bearbeiten”** ausschalten
   Mit folgendem Befehlt können Sie vermeiden das ein Benutzer, ob Admin oder nicht, per Dashboard Theme Dateien oder Plugins bearbeiten kann. Suchen Sie dafür einfach nach folgendem Begriff: “*define(‘DISALLOW_FILE_EDIT’,true);*” und stellen Sie sicher, dass dort “true” drin steht. Das wird die Hacker wenigsten in Ihrem Dashboard davon abhalten auf Ihre Theme-Dateien oder Plugins ändern zu können.
3. Ändern Sie Ihre Sicherheitsschlüssel ab
   Das ist etwas komplizierter, erhöht aber die Sicherheit in WordPress ungemein.

So ändern Sie die Sicherheitsschlüssel:

In Ihrer wp-config.php Datei befinden sich folgende Zeilen:

define(‘AUTH_KEY’, ‘put your unique phrase here’);
define(‘SECURE_AUTH_KEY’, ‘put your unique phrase here’);
define(‘LOGGED_IN_KEY’, ‘put your unique phrase here’);
define(‘NONCE_KEY’, ‘put your unique phrase here’);
define(‘AUTH_SALT’, ‘put your unique phrase here’);
define(‘SECURE_AUTH_SALT’, ‘put your unique phrase here’);
define(‘LOGGED_IN_SALT’, ‘put your unique phrase here’);
define(‘NONCE_SALT’, ‘put your unique phrase here’);

Obige Schlüssel sollten Sie gegen zufällig generierte austauschen. Das wird jeden Hacker zur Verzweiflung treiben.

1. Gehen Sie auf https://api.wordpress.org/secret-key/1.1/salt/ (öffnet sich in einem neuen Fenster)
2. Kopieren Sie alle Zeilen
3. Markieren Sie obige Zeilen in Ihrer “wp-config.php” Datei
4. Ersetzen Sie diese mit den neu generierten Zeilen. Diese erkennen Sie daran das sie einen komischen “String” hinten enthalten

Das wären die 6 einfachen Schritte, wie Sie Ihr WordPress vor Hackern schützen. Am besten Sie starten jetzt sofort mit den Änderungen an Ihrer WordPress-Seite.

Mein WordPress wurde gehackt, was tun?

Jetzt ist es doch passiert, Ihr WordPress wurde gehackt und ein Schadcode wurde eingeschleust. Atmen Sie als ersten einmal tief durch… Es gibt jetzt mehrere Möglichkeiten:

a.) Sie nutzen unser automatischen WordPress Backup Dienst blogVault?

Dann ist das Ganze sehr einfach.

1. In das blogVault Dashboard einloggen

2. Wählen Sie neben Ihrem Blog “Auto-Wiederherstellung”

3. Folgen Sie den weiteren Schritten
4. **ACHTUNG:** Wählen Sie eine Version Ihres WordPress Backups die **VOR** dem Hack erstellt wurde
5. Stellen Sie Ihre Webseite wieder her
6. Ändern Sie alle Passwörter und gehen Sie obige Anleitung Punkt für Punkt durch, um Ihr WordPress abzusichern.

b.) Sie haben kein blogVault Backup?

Warum nicht? Schon ab 9€ im Monat sichern wir nicht nur Ihre WordPress Datenbank, sondern auch alle Dateien, Bilder, Themes, Plugins etc.. Probieren Sie blogVault völlig kostenlos für 7 Tage aus.

Wir hoffen Ihnen hat unsere kleine und einfache Anleitung gefallen. Wir wünschen Ihnen allezeit eine abgesicherte und Hackerfreie Webseite!

Ihr blogVault Deutschland-Team