Da wir feststellen das viele Wordpress-Webseiten unzureichend geschützt und deshalb häufig angegriffen werden, hier einmal einige Tips zu Absicherung der Wordpress-Installationen bietet:

http://www.afoma.de/artikel/sicher-ist-wordpress-blog-hacker-angriffe-wp-blogs

Wie schütze ich meinen WordPress-Blog am besten?

Bevor wir beginnen, WordPress zu schützen, muss ich Ihnen gestehen: Einen 100%igen Schutz für Ihren WordPress-Blog wird es nie geben. Zu viele Möglichkeiten bieten Hackern die Chance, Ihren WordPress-Blog anzugreifen. Wichtig hier ist aber auch nicht der 100%ige Schutz. Viel wichtiger ist es, den WordPress-Blog so zu schützen, dass ein Angriff sehr viel Zeit in Anspruch nimmt und es somit lohnendere Ziele gibt. Wenn Sie das erreichen, können Sie zu 99% sicher sein, dass Ihr WordPress-Blog nicht von Hackern übernommen wird.

Kommen wir nun also zu den Schutzmaßnahmen. Zuvor habe ich schon einige der Schwachstellen genannt, die Hacker natürlich gerne ausnützen. Daher müssen als erstes diese Möglichkeiten unterbunden werden.

1.

User-Name admin

Bei der Installation von WordPress können Sie den Standard-Benutzernamen admin umbenennen. Dies sollten Sie natürlich durchführen, doch noch wichtiger ist es, diesen Benutzer später zu löschen und einem anderen Benutzer die Administrations-Rechte zu übertragen. Warum, erfahren wir in Punkt 2.

2.

UserID 1

Der erste Benutzer, der vom System angelegt wird, erhält die ID 1 in der Datenbank. Hacker wissen natürlich, dass viele User den Standard-Benutzernamen mit der ID 1 nicht löschen und versuchen über die ID 1 Zugriff auf den WordPress-Blog zu erhalten. Deshalb sollte der Standard-Benutzer immer gelöscht werden und der Benutzer mit Administrations-Rechten erst als vierter oder fünfter Benutzer angelegt werden.

3.

Tabellen-Präfix

Obwohl es unterschiedliche Meinungen in Bezug auf die Sicherheitsverbesserung durch Änderung des Tabellen-Präfix gibt, empfehle ich, den Tabellen-Präfix bei der Installation zu ändern. Jede Abweichung von den Standard-Einstellungen erhöht meiner Meinung nach die Sicherheit.

4.

Benutzernamen und Passwörter

Erstellen Sie immer starke, kryptische Passwörter und Benutzernamen. Ein Passwort in WordPress sollte immer aus Buchstaben (Groß- und Kleinschreibung), Zahlen und Sonderzeichen bestehen. Wörter, die in einem Wörterbuch stehen, sollten am besten nicht verwendet werden. Weiters sollte ein Passwort mindestens 14 Zeichen lang sein. Je mehr, desto besser. Auch bei den Benutzernamen können Sie Buchstaben, Zahlen und Sonderzeichen verwenden. So kann zB ein Benutzername auch **Rnx 4@ 690Pq# H%** heißen und das Passwort **U3mL+ßEÄ7xPd81LQö9J!5** la uten.

5.

Header-Informationen von WordPress

Standardmäßig gibt WordPress die Information über die verwendete WordPress-Version im Header bekannt. Dies ist für Hacker natürlich von Vorteil, da sie so die Sicherheitslücken von WordPress kennen und somit auch ausnützen können. Steht diese Information nicht zur Verfügung, muss die WordPress-Version erst ermittelt werden, was natürlich wieder ein weiterer Zeit-Aufwand ist.

6.

Die Anmelde-Seite von WordPress schützen.

Besonders die Anmelde-Seite zum internen Bereich von WordPress muss unbedingt geschützt werden. Die wirksamste Methode ist, eine zusätzliche Passwort-Abfrage hinzuzufügen. Eine sehr hilfreiche Anleitung dazu finden Sie auf der Webseite von Sergej Müller unter: http://playground.ebiene.de/adminbereich-in-wordpress-schuetzen/

Zwei weitere Möglichkeiten, einen zusätzlichen Schutz einzubauen, bieten die beiden PlugIns Google Authenticator und yubikey-PlugIn.

7.

WordPress-Updates

Eine der einfachsten aber auch sehr effektiven Schutzmaßnahmen ist, dass WordPress selbst

und die PlugIns bzw. Themes immer auf dem aktuellsten Stand sind. Durch regelmäßige Updates werden die Sicherheitslücken geschlossen und somit die Sicherheit natürlich erhöht. Wichtig ist auch, nur die wichtigsten PlugIns und Themes zu installieren. Alle nicht verwendeten PlugIns und Themes sollten gelöscht werden.

8.

Die wichtigsten Dateien schützen

Wichtige Dateien wie zB wp-config.php oder .htaccess müssen vor Zugriff von außen geschützt werden. Sergej Müller hat dazu ein Beispiel in seinem Beitrag (Link unter Punkt 5) aufgezeigt. Auch die Rechte für Dateien und Ordner sollten überprüft werden. Das PlugIn BulletProof Security zeigt zB an, für welche Dateien und Ordner zu weitreichende Rechte aktiviert sind.

9.

Backup der WordPress-Daten und Datenbank

Auch eine richtige Backup-Strategie ist für die Sicherheit Ihres WordPress-Blogs entscheidend. Nur mit einer funktionierenden Sicherung können Sie im Notfall Ihren WordPress-Blog wieder herstellen. Sichern Sie daher mindestens täglich Ihre WordPress-Datenbank und wöchentlich Ihre WordPress-Daten. Selbstverständlich sollten Sie dies auch vor jeder Änderung durchführen.

Viele Grüsse

diskus