

Zur Sicherheit: Leitfaden für WordPress-Kunden

Für Einsteiger in ein Content Management System (CMS) und ambitionierte Website-Betreiber hat WordPress einige Vorteile: Neben der geringen Lernkurve sind es die zahlreichen Plugins, die diese Weblog-Software so verlockend machen. Leider ergeben sich daraus auch Nachteile, die manchem Wordpress-Nutzer erst dann bewusst werden, wenn es zu spät ist.

Deshalb gebe ich meinen Kunden, die WordPress einsetzen wollen, einen Leitfaden mit. Der zeigt ihnen, auf was sie bei WordPress achten sollten und was für Aufgaben auf sie zukommen, damit es nicht zu bösen Überraschungen kommt (weiterführende Links am Ende des Artikels).

Ich unterscheide zwei Gruppen von WordPress-Nutzern. Die erste benutzt zum ersten Mal ein Content Management System und möchte lediglich in unregelmäßigen Abständen neue Inhalte einbinden. Die zweite Gruppe gehört den experimentierfreudigen, ambitionierten Nutzern an, die mit ihren Weblogs und Projekten intensiv Kontakte, Kunden und Austausch suchen, aber die Templates nicht selbst erstellt haben.

Der Gelegenheitsnutzer

Die Gruppe der gelegentlichen Nutzer macht sich in der Regel keine Gedanken über Updates der Weblog-Software. Entsprechend kommt es vor, dass eine WordPress-Installation über Monate ja Jahre nicht aktualisiert wurde. Im schlechtesten Fall wird dieses alte WordPress ein Opfer von Kriminellen und der Schreck ist groß, wenn Google vor dieser Site warnt und die Inhalte aus dem Index verschwinden läßt. In diesem Zusammenhang gebe ich dem Kunden folgende Hinweise:

1. Prüfen Sie regelmäßig im Administrationsbereich (Backend) von WordPress, ob es Aktualisierungen gibt.
2. Da es sich nicht selten um Sicherheits-Updates handelt, sollten diese Aktualisierungen zeitnah mit der Automatik-Funktion von WordPress installiert werden. Dazu ist ein FTP-Login mit einem Benutzernamen und Passwort erforderlich.
3. Das FTP-Login sollte ein Passwort mit mindestens 12 Zeichen haben.
4. Bevor ein automatisches Update gemacht wird, sollten in jedem Fall vorher folgende Sicherheitsmaßnahmen getroffen werden:
 - Die Datenbank sichern
 - Alle Plugins deaktivieren
5. Nach der erfolgreichen Aktualisierung: Jedes Plugin einzeln aktivieren, um zu prüfen, ob es noch funktioniert. Wenn es Probleme gibt, auch die murrenden Plugins aktualisieren.
6. Vor allem aus Punkt 4 darf geschlossen werden, daß Folgekosten auf den Betreiber zukommen, wenn er mit diesen Maßnahmen überfordert ist. In diesem Fall sollte ein externer Dienstleister die Aufgabe übernehmen. Der zeitliche und damit finanzielle Aufwand hält sich Grenzen, da ein automatisches Update in einigen Minuten realisiert ist, selbst wenn nach dem Update einige Plugins aktualisiert werden müssten.
7. Es ist ratsam, nur notwendige Plugins zu installieren. Eine einfache Website kommt je nach Ansprüchen mit fünf bis zehn Plugins aus.

- Bei größeren Versionsprüngen wäre zu prüfen, ob sich die Serveranforderungen von WordPress geändert haben. Ist eine höhere PHP oder MySQL-Version nötig und bietet diese mein Server? Zudem schadet es nicht, einige Tage zu warten, bis man ein größeres Update installiert, um zu schauen, ob in Weblogs und Foren über Update-Probleme oder Komplikationen berichtet werden.

Der ambitionierte Nutzer

Beim ambitionierten Blogger dürfen wir nicht selten von Experimentierfreude und einem hohen Bedarf an Plugins ausgehen. Videos und Audiofiles wollen integriert und Bildergalerien leicht erstellt werden. Alle möglichen Daten für die Webpromotion und die sozialen Netzwerke wollen verknüpft und Suchmaschinenoptimierung betrieben werden.

So kommen schnell eine Menge an Zusatzprogrammen zum Einsatz. Diese erhöhen nicht nur das Sicherheitsrisiko - da Plugins Schadcode enthalten können -, sondern blähen zudem nicht selten die Datenbank auf. Manche Website wird so recht behäbig und ein höherer Versionssprung von WordPress kann zu Problemen führen.

So konnte ein Kunde partout keine Kategorien- und Tagseiten mehr aufrufen, obwohl alle Plugins deaktiviert waren und die neueste WordPress-Version installiert war. Am Ende blieb nur eine saubere Neuinstallation mit Portierung der Inhalte sowie die Neueinrichtung aller noch wichtigen Plugins. Um die achtzig Prozent der Datenbanktabellen waren danach überflüssig geworden!

Um sich als ambitionierter Wordpress-Nutzer vor bösen Überraschungen zu schützen, beachtet man schlicht folgende Regeln:

- Die Sorgfalt fängt bei der Erstellung der Datenbanken an. Mehrere MySQL-Datenbanken sind selbst in kleinen Webhosting-Paketen enthalten. Zur leichteren Sicherung und besseren Trennung sollte jede WordPress-Installation eine eigene Datenbank bekommen. Bei der Erstellung der Datenbank ein sicheres Passwort mit mindestens 12 Stellen verwenden und dafür sorgen, dass man alle relevanten Daten wie Datenbankname, Datenbankuser, Datenbankpasswort sowie den internen Serverpfad und Host parat hat. Braucht man einmal professionelle Hilfe, so helfen diese Daten bei der schnellen Umsetzung. Diese sensiblen Daten lassen sich in Passwortmanagern wie *KeePass* und *Roboform* sammeln und verschlüsselt aufbewahren.
- Die gleiche Sorgfalt wie bei der Einrichtung einer Datenbank gelten für das FTP- und das phpMyAdmin-Login: Sichere Passwörter mit mindestens 12 Stellen wählen.
- Während der Installation von WordPress einen unüblichen Benutzernamen und ein kompliziertes Passwort wählen und beides in einer passwortgeschützten Datei aufbewahren. Das gilt auch für weitere Benutzer wie Gastautoren ohne Administrationsrechte.
- Desweiteren zeitnah die kleineren WordPress-Updates installieren und trotzdem grundsätzlich immer zuvor die Datenbank sichern und alle Plugins deaktivieren. Das sind nur ein paar Mausclicks. Eine doppelte Sicherung der Datenbank kann wie folgt nicht schaden:
 - über Wordpress: "Werkzeuge" > "Backup".
 - mit Hilfe von *phpMyAdmin*. Dieses Hilfswerkzeug haben die meisten Webhoster zur Verwaltung von MySQL-Datenbanken installiert. Dort gibt es eine Exportfunktion für die Datenbanktabellen (siehe den Link zur Anleitung unten).
- Sorgfalt bei der Plugin-Installation: Nicht sofort das erstbeste installieren. Zuvor nach weiteren Informationen im Netz suchen, Usermeinungen einholen. Plugins vergleichen. Ist dann eine

Entscheidung getroffen, darauf achten, das Plugin von der offiziellen Wordpress-Plugin-Site zu beziehen.

Ein unterschätztes Problem sind verwaiste Wordpress-Blogs. Man vergisst ein altes Projekt und im Laufe der Zeit wird die Datenbank aufgebläht durch zahlreiche Spam-Kommentare. Eventuell ist die Site auch durch ein Sicherheitsloch gehackt worden und verbreitet Schadsoftware. Um dem zu begegnen, sind auch die alten Projekte auf dem aktuellen Softwarestand zu halten oder in statische Seiten umzuwandeln. Leider gibt es keine Wordpress-Software dafür, die letzteres automatisch machen würden.

Natürlich gibt es auf technischer Seite noch eine Menge Möglichkeiten sein WordPress sicherer zu machen als es ist. Das zeigt Vladimir Simovic in seinem Artikel „So sichern Sie die Blog-Maschine ab“. Darauf kann man den Webdesigner, der das WordPress schön macht und die Templates anpasst, durchaus festnageln. ;-)

Links

- WordPress in 5 Minuten installieren:
http://doku.wordpress-deutschland.org/5_Minuten_Installation
- WordPress sicherer als vermutet:
<http://www.perun.net/2010/08/04/wordpress-sicherer-als-vermutet/>
- Was ist ein Plugin?
<http://blog-anleitung.de/g-plugin.html>
- Plugin Directory von WordPress:
<http://wordpress.org/extend/plugins/>
- Datenbank-Backup mit phpMyAdmin:
http://doku.wordpress-deutschland.org/Backup_der_Datenbank/phpMyAdmin
- KeePass: Kostenfreier Passwortmanager
<http://keepass.info/>
- RoboForm: Passwortmanager mit Integration im Browser
<http://www.roboform.com/de/>
- So sichern Sie die Blog-Maschine ab:
<http://www.spiegel.de/netzwelt/web/0,1518,707286,00.html>