Anleitungen
Tipps für ein sicheres WordPress

WordPress ist eine ziemlich populäre Software, die sich zum Betrieb eines Blogs ebenso eignet, wie als Content-Management-Systems. Doch dadurch, dass es so populär ist, ist es auch häufig Ziel verschiedener Attacken von Personen, die sich Zugriff auf fremde Accounts verschaffen wollen um von dort unerkannt Spam zu verschicken oder weitere Angriffe durchzuführen.
In diesem Beitrag versuchen wir Ihnen ein paar nützliche Tipps zu geben, um Ihre WordPress-Installation möglichst sicher zu gestalten.

Natürlich sind die hier angegeben Vorschläge keine Garantie dafür, dass nichts geschieht, denn Sicherheit ist ein Prozess und kein Zustand. Ein befolgen der Hinweise entbindet Sie nicht von Ihrer Eigenverantwortung.

Zugangsdaten

Erster Angriffspunkt vieler Hacker sind die Zugangsdaten. Dementsprechend empfiehlt es sich selbstverständlich diese möglichst sicher zu gestalten. Hier finden Sie einen Beitrag der Ihnen bei der sicheren Gestaltung von Passwörtern helfen kann.

Darüber hinaus kann auch der Username angepasst werden. In einer Standard-Installation ist der User-Name des Administrators admin. Damit hat ein möglicher Angreifer schonmal einen Namen und muss nur noch das Passwort knacken. Daher empfiehlt es sich, diesen Standard-Benutzer möglichst frühzeitig umzubenennen.

Updates

Wird eine Sicherheitslücke bekannt, dann wird diese häufig innerhalb kürzester Zeit ausgenutzt. Doch auch die Software-Entwickler erfahren von der Lücke und stellen oft zeitnah Updates zur Verfügung um diese Lücken zu schließen. Daher ist es besonders wichtig ein einmal installiertes System nicht verwaisen zu lassen, sondern regelmäßig Updates einzuspielen. WordPress macht es einem da recht einfach, da es eine Auto-Update-Funktion bietet. Mehr dazu finden Sie im offiziellen Support-Forum von WordPress.

Doch nicht nur WordPress selbst sollte aktuell gehalten werden. Auch Plugins und Themes können Sicherheitslücken enthalten und sollten daher ebenso regelmäßig auf Updates überprüft werden.

Plugins minimieren

Der beste Schutz gegen Sicherheitslücken ist, diese gar nicht erst entstehen zu lassen. Dementsprechend sollte man nur so viele Plugins installieren, wie man tatsächlich benötigt. Bevor Sie ein Plugin installieren sollten Sie sich also überlegen, ob Sie diese Funktionalität auch tatsächlich benötigen.

Benutzerrechte einschränken

Auch bei den Benutzeraccounts gilt: Vergeben Sie nur die Rechte, die auch notwendig sind. Sofern Sie WordPress mit mehreren Nutzern verwenden, überlegen Sie sich, welche Person welche Rechte benötigt und sperren Sie Accounts, wenn diese nicht mehr benötigt werden.

Verzeichnisse schützen

Für die WordPress-Ordner /wp-content/ und /wp-includes/ empfiehl es sich den Zugriff auf die nötigsten Dateien zu beschränken. Dies erreicht man durch das Anlegen einer Datei .htaccess in den jeweiligen Ordnern, die den Zugriff regelt. Als Beispiel wäre folgender Inhalt möglich:

```
Order deny,allow
Deny from all
<Files ~ ".(php|lock|xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

Auch das Verzeichnis /wp-admin/, in dem all die Skripte für die Administration liegen, kann besonders geschützt werden. Wenn Sie eine feste IP-Adresse besitzen, wie es z.B. bei einigen Kabel-Anbietern der Fall ist, können Sie mit folgender .htaccess-Datei den Zugriff auf das Verzeichnis so einschränken, dass nur noch sie selbst in das Administrator-Interface gelangen:

```
rder deny,allow

Deny from all

# Folgende IP-Adresse durch Ihre eigene ersetzen

Allow from 89.110.129.51
```

Wenn Sie sich mit der Syntax von .htaccess auskennen, können Sie hier sogar einen zusätzlichen Passwortschutz konfigurieren.

Regelmäßige Überprüfungen

Wie bereits geschrieben: „Sicherheit ist kein Zustand, sondern ein Prozess“. Daher ist es wichtig, dass Sie Ihre Seiten regelmäßig überprüfen. Am besten kombinieren Sie dies mit regelmäßigen Backups, die sich ebenso empfehlen. Je früher Sie unberechtigte Änderungen an Ihren Dateien, oder verdächtige Seitenabrufe in den Logdateien feststellen, desto geringer ist der Schaden, den Sie ggf. zu beheben haben.

Anleitungen

Eindeutige ID: #1120
Verfasser: Patrick Schneider
Letzte Änderung: 2022-04-05 14:49