SICHERHEIT IST EINE HALTUNG UND KEIN ZUSTAND

TEXT: Torsten Landsiedel

WordPress ist das meistgenutzte Content-Management-System weltweit. Bei so vielen Benutzern nimmt auch die Zahl der Einbruchsversuche zu. Je nach Paranoia-Level kann das Blog nun so sehr geschützt werden, bis es gar nicht mehr benutzbar ist. Sie können WordPress aber auch absichern, ohne auf eine einfache Bedienung zu verzichten.

Die schlechte Nachricht zuerst: 100%ige Sicherheit gibt es nicht. Webworker sollten das Bemühen um Sicherheit immer als einen Prozess sehen, der dauerhaft betrieben wird. Jede Änderung am Quelltext, jedes neue Plug-in kann eine Sicherheitslücke darstellen. Alle Maßnahmen, die dazu führen, dass ein System sicherer wird, sind daher sinnvoll. Sie sind aber nie abschließend. Oft denken Nutzer auch, dass ein Einbruch im eigenen Blog unwahrscheinlich ist. Meine Webseite ist doch nicht wichtig! Ich habe doch kaum Besucher! Was wollen die denn ausgerechnet mit meinen Daten? Es gibt jedoch genug Gründe, warum ein Computerkrimineller trotzdem in eine Webseite einbricht:

- Hosting von Phishing-Seiten
- Spam-Versand
- Werbe-Einblendungen
- Einfügen von Backlinks
- Virenverbreitung
- Vandalismus/Wettbewerb
- etc.

GRUNDLEGENDE SICHERHEITSTIPPS

Was gibt es also für Maßnahmen, die Ihre WordPress-Webseite wirkungsvoll absichern?

Updaten, updaten, updaten! Der wichtigste Punkt überhaupt ist es, die WordPress-Installation auf allen Ebenen aktuell zu halten. Das heißt, der WordPress-Core, die Themes und die Plug-ins sollten auf dem aktuellen Stand sein. Alte Versionen enthalten oft Sicherheitslücken, die bei Veröffentlichung der Nachfolge-Version bekannt werden. Somit können diese Lücken bei veralteten Blogs ausgenutzt werden.

Aber wie hält ein vielbeschäftigter Blogger seine Webseite aktuell? Über ein Core-Update wird breit berichtet, aber nicht über jedes Plug-in-Update. Damit Sie nicht über ein Sicherheitsloch in einem Plug-in stolpern, empfiehlt es sich über jedes Plug-in-Update per E-Mail informiert zu werden. Zum Beispiel mit dem Plug-in „Mail on Update" [goo.gl/rt3Rp]. Für Webworker und Agenturen, die viele WordPress-Installationen zu betreuen haben, gibt es eine noch bessere Lösung: InfiniteWP [goo.gl/nO2xX] und das kostenpflichtige ManageWP [/goo.gl/Es9J2] bieten die Zusammenlegung mehrerer WordPress-Administrationsbereiche in ein gemeinsames Backend. So können Sie mit wenigen Klicks alle Ihre WordPress-Seiten aktualisieren. Wenn Sie bei einer älteren WordPress-Version bleiben müssen, können Sie schauen, ob das Hotfix-Plug-in [goo.gl/Ssbmm] für diese Version Bugs behebt, die erst nach dem Release bekannt wurden.

Brute-Force-Attacken verhindern: Ein möglicher Angriff auf eine Webseite ist der Versuch, den Log-in zu erraten; dabei werden verschiedene Benutzernamen und Passwörter einfach durchprobiert. Hierbei werden Wörterbücher benutzt, die einfach auf den Log-in losgelassen werden – auch Brute-Force-Attacke genannt. Um so einen Angriff zu verhindern, sollten zu häufige falsche Anmeldeversuche mit einer Strafpause belegt werden. Das Plug-in Limit Login Attempts [goo.gl/E0cgV] erfüllt genau diesen Zweck. Als Zusatznutzen gibt WordPress nun auch nicht mehr preis, ob der Benutzername stimmt und nur das Passwort falsch ist. Die

```
34
35 /**#@+
36  * Sicherheitsschlüssel
37  *
38  * Ändere jeden KEY in eine beliebige, möglichst einzigartige Phrase.
39  * Auf der Seite {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service} kannst du dir
 . alle KEYS generieren lassen.
40  * Bitte trage für jeden KEY eine eigene Phrase ein. Du kannst die Schlüssel jederzeit wieder ändern, alle angemeldeten
 . Benutzer müssen sich danach erneut anmelden.
41  *
42  * @seit 2.6.0
43  */
44 define('AUTH_KEY',         'put your unique phrase here');
45 define('SECURE_AUTH_KEY',  'put your unique phrase here');
46 define('LOGGED_IN_KEY',    'put your unique phrase here');
47 define('NONCE_KEY',        'put your unique phrase here');
48 define('AUTH_SALT',        'put your unique phrase here');
49 define('SECURE_AUTH_SALT', 'put your unique phrase here');
50 define('LOGGED_IN_SALT',   'put your unique phrase here');
51 define('NONCE_SALT',       'put your unique phrase here');
52
```

Abb 1: Eine wp-config.php ohne eingetragene Sicherheitsschlüssel

Anzahl an Versuchen ist einstellbar. Bei einer Sperrung können Sie sich als Administrator auch per E-Mail benachrichtigen lassen. Aber die Grenzen des Plug-ins sollten Ihnen auch bewusst sein. Wenn der Angreifer ein ganzes Botnet nutzen kann, dann ist ein verteilter Angriff möglich, der nach drei Versuchen den Einbruchsversuch einfach durch einen anderen Rechner mit einer anderen IP-Adresse weiter durchführen lässt. So wird der Schutz ausgehebelt.

Qwerty, 123456, P@ssw0rd … lieber nicht: Besser als jedes Plug-in schützt ein richtig gutes Passwort. Mit der Qualität des Passwortes steht und fällt die gesamte Sicherheit. WordPress bietet ein automatisches Tool, welches die Passwortstärke anzeigt. Nutzen Sie es! Ein Passwort sollte eine Mindestlänge von 10 Zeichen haben, aber es muss nicht unbedingt megakryptisch daher kommen. WordPress erlaubt zum Beispiel Leerzeichen in Passwörtern. Nehmen Sie einfach einen kompletten Satz als Passwort, der lässt sich auch einfacher merken als Zeichenfolgen wie diese: „F3g&74§bZ!". Alternativ kombinieren sie einfach mehrere Wörter, wie „Hutsahneregalhüpfburg". Das ist lang, kaum zu erraten und somit erstaunlich schwierig zu knacken. Was Sie auf jeden Fall vermeiden sollten ist das mehrfache Verwenden eines Passwortes für verschiedene Dienste. Wer sich viele Passwörter merken muss, benutzt zur Organisation am besten ein Werkzeug, wie das Open-Source-Tool Keepass [goo.gl/4dXNF]. Damit werden die Passwörter verschlüsselt gespeichert, müssen nicht aufgeschrieben werden, und es genügt, sich an das Master-Passwort zu erinnern. Einzelne Wörter, die im Wörterbuch stehen, sollten auf jeden Fall als Passwort vermieden werden. Das Gleiche gilt für typische Zeichenfolgen, wie „Passwort", „123456", „qwerty" oder „abc123". Eine ebenso typische Pseudo-Absicherung ist das Verwenden von Ersetzungen, „o" wird zu „0" und „a" wird zu „@". Ein Passwort wie „P@ssw0rt" ist also ebenfalls nicht sicher, denn diese Taktik wird inzwischen bei den Einbruchsversuchen auch durchprobiert. Auch von typischen Mustern wie Vorname und Jahreszahl („Bernd2013") sollten Sie besser absehen. Ein genereller Tipp: Behandeln Sie Passwörter am besten wie Zahnbürsten – nicht teilen und regelmäßig wechseln!

Sicherheitsschlüssel in der wp-config.php

Um die Passwörter einer WordPress-Installation noch besser zu schützen, sollten in jedem Fall die Cookie-Sicherheitsschlüssel alle vorhanden sein. Bei der aktuellen Version 3.5 sind es momentan acht. Die Schlüssel stehen in der Konfigurationsdatei wp-config.php und sollten am besten mit dem in dieser Datei erwähnten Online-Generator erstellt worden sein [goo.gl/Ips0r]. Dadurch werden die im Log-in-Cookie gespeicherten Passwörter zusätzlich verschlüsselt. Sollte tatsächlich einmal in Ihre Webseite eingebrochen werden, können Sie die Log-in-Cookies mit dem Ändern dieser Sicherheitsschlüssel ganz einfach für ungültig erklären, sodass ein noch eingeloggter Eindringling automatisch abgemeldet wird. Wer die wp-config.php durch WordPress selbst hat erstellen lassen, der braucht sich um nichts mehr kümmern. In diesem Fall hat WordPress die notwendigen Schlüssel schon selbst generiert. Alle anderen sollten diese Einstellung auf jeden Fall überprüfen und, wenn sie nicht vorhanden ist, schnell nachtragen.

Zugriffsrechte: Insbesondere bei Shared-Hosting-Anbietern besteht die Gefahr, dass die Lücke gar nicht durch einen eigenen Fehler entsteht sondern durch eine andere Seite auf dem gleichen Server. Um Infizierungen durch diese „Cross-Site-Contamination" zu verhindern, sollten die Zugriffsrechte so niedrig wie möglich eingerichtet sein. Die Faustregel besagt: UNIX-Berechtigung 755 für Verzeichnisse und 644 für Dateien. Dies ist jedoch kein Muss. Je nach Server können andere Einstellungen besser sein und mehr Sicherheit bieten. Im Prinzip gilt: Nehmen Sie die geringsten Rechte, bei denen noch alles ohne Probleme läuft. Plug-ins, wie WP Security Scan [goo.gl/HxCVK] helfen Ihnen dabei, die Dateirechte zu prüfen und schlagen Änderungen vor.

SSL-Verschlüsselung: Das Aktivieren der SSL-Verschlüsselung für den Administrationsbereich ist eine einfache und sinnvolle Möglichkeit, die Kommunikation mit dem Server abzusichern. Das ist natürlich nur dann sinnvoll, wenn Sie ein SSL-Zertifikat erworben haben. Die Kosten von etwa 60 Euro im Jahr für solch ein Zertifikat sind eine gute Investition in die Sicherheit.

PHP / Absicherung in der wp-config.php

```
define[,FORCE_SSL_ADMIN', true];
```

Die obige Einstellung allein, ohne das Zertifikat, verhindert jedoch keinen Man-in-the-Middle-Angriff, denn ohne das gültige

```
34
35 /**#@+
36  * Sicherheitsschlüssel
37  *
38  * Ändere jeden KEY in eine beliebige, möglichst einzigartige Phrase.
39  * Auf der Seite {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service} kannst du dir
    alle KEYS generieren lassen.
40  * Bitte trage für jeden KEY eine eigene Phrase ein. Du kannst die Schlüssel jederzeit wieder ändern, alle angemeldeten
    Benutzer müssen sich danach erneut anmelden.
41  *
42  * @seit 2.6.0
43  */
44 define('AUTH_KEY',         'sux:EFc5?t.<v^Kh5EU6Mvlf*rU3/-RUjzz.,-!(sI?Xk>F;HK+mvYONVNX$myq{');
45 define('SECURE_AUTH_KEY',  'f*,!ij8z/J+_N9KOp5AzXFh*m-,XX3L[Nh:S=L=o;WGe!l6oIF?6,04{@+- (Ks]');
46 define('LOGGED_IN_KEY',    '#n<x>)IHORtSB*Z8yMV8N~~nih>R'.oFvMJ!9Yl~f64W?wi+NT?]tC2)q9#V8dYh');
47 define('NONCE_KEY',        'xRNplk,-D@gs)/m 3!~}kd`d7M;Wd#WMLO-{XNB3/2/BqhMY%/Ag-+W9mLQSMqy2');
48 define('AUTH_SALT',        'xnG`sAsUQ4/c@L!W?d7x-X-K*U(.X(-DebK(hT3!0ViEV=$hs2Q#8xC+=?2SF>$s');
49 define('SECURE_AUTH_SALT', '295;SUEe,g9<M)njS;C4.{MBA2dJC/XwpFk>-&.z`@j_tx;3i.s&Q;mtx8OQwico');
50 define('LOGGED_IN_SALT',   '^Q.H}+$QK;$uKyb2A<_SC}+xw YB>!%A4D9$k)IVilk 9NjPQse]nv}+^@dKOxIO');
51 define('NONCE_SALT',       '(Z5%$,MHs3-(zjSYjBU;1iwN[_Bleq5~IW+_,)+(RLkqZ,khzH*#8F8~F;M<P-EX');
52
```

Abb 2: Und hier mit korrekt gesetzten Sicherheitschlüsseln

Zertifikat können Sie einen Angreifer eben nicht von einem berechtigten Kommunikationsteilnehmer unterscheiden. Sollte die SSL-Verbindung langsam sein, so können Sie auch nur den Log-in absichern, um die Versendung der Passwörter zu verschlüsseln:

PHP / Login-Absicherung in der wp-config.php

```
define('FORCE_SSL_LOGIN', true);
```

Verschlüsselte FTP-Übertragung: Auch an anderen Stellen werden Passwörter übertragen. Die Übermittlung von neuen Themes oder Plug-ins findet per FTP statt. Ein Protokoll, das leider Passwörter im Klartext versendet. Sofern es möglich ist, sollten Sie also immer eine der verschlüsselten FTP-Varianten nutzen. SFTP (Secure File Transfer Protocol) oder FTP over TLS (eine Kombination von FTP und Transport Layer Security). Sollte dies nicht möglich sein, dann wechseln Sie besser Ihren Webhoster.

Gute Hoster, schlechte Hoster: Überhaupt ist die Wahl des Hosters entscheidend für die allgemeine Sicherheit. Wie schnell und wie regelmäßig werden Sicherheitsupdates bei der Software, wie PHP und MySQL, eingespielt? Ist dort eine offene Sicherheitslücke vorhanden, dann nützt auch die beste WordPress-Absicherung nichts mehr.

Zweimal abschließen – sicher ist sicher! Damit der WordPress-Administrationsbereich wirklich sicher ist, können Sie noch einen Schritt weiter gehen und beim Log-in eine zusätzliche Autorisierung einbauen. Sei es über eine Server-Passwort-Abfrage per htaccess oder über eine Zwei-Faktor-Absicherung mit Plug-ins wie dem Google Authenticator [goo.gl/CLJy3] – damit kann auch nur das Administrator-Konto abgesichert werden. Alle anderen Benutzer melden sich weiterhin normal an.

Was nicht da ist, kann auch nicht missbraucht werden … Sollte tatsächlich ein Fremder Zugang zum Blog haben, dann hilft es, wenn die Möglichkeiten des Nutzers, der geknackt wurde, nicht zu weitreichend ausfallen. Das bedeutet: Sie sollten immer nur die Zugriffsrechte einräumen, die benötigt werden. Es müssen nicht alle Benutzer eines Blogs Administratoren sein, und zum alltäglichen Schreiben muss nicht das Admin-Konto benutzt werden, dafür reicht auch ein Redakteur aus.

Auch der Plug-in- und Theme-Editor kann komplett deaktiviert werden, um zu verhindern, dass über diesen Weg Template-Dateien verändert werden können:

PHP / Änderung in der wp-config-php:

```
define('DISALLOW_FILE_EDIT',true);
```

Wer noch sicherer sein möchte, der kann seinen gesamten Blog auch überwachen lassen. Mit dem Plug-in WordPress File Monitor Plus [goo.gl/6GVFl] lassen Sie sich einfach über jede Änderung per E-Mail informieren. Problematisch könnte dabei nur die zusätzliche Serverlast sein. Ein Problem, das die nächste Absicherung auch besitzt: Jede Anfrage an die Webseite kann mit einer Blacklist, wie die von Perishable Press [goo.gl/kmX7F], abgeglichen werden. So werden bekannte Spammer und potenzielle Eindringlinge schon „an der Tür" abgewimmelt. Bei trafficstarken Blogs macht sich diese Filterung aber leider durchaus in der Geschwindigkeit bemerkbar. Ob dies die zusätzliche Sicherheit wert ist, müssen Sie selbst entscheiden.

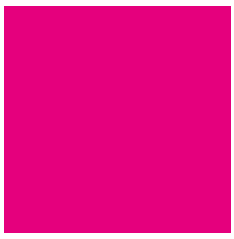
Back-ups retten Leben! Egal wie sicher Ihr WordPress ist; es kann trotzdem passieren, dass etwas schiefläuft. Ruhig schlafen kann derjenige, der weiß, dass er für diesen Fall ein Back-up hat. Ein vollständiges Back-up besteht bei WordPress aus einer vollständigen Kopie aller Dateien auf dem Server und der Datenbank. Die Dateien können mit jedem beliebigen FTP-Programm herunter geladen werden. Manche Back-up-Plugins bieten für so etwas sogar eine Komplettlösung für Dateien und Datenbank. Es ist fast egal, für welche Lösung Sie sich entscheiden. Es gibt sogar Plug-ins, die direkt in die Dropbox und andere ähnliche Dienste sichern. Hauptsache, Sie haben ein Back-up.

Ein paar generelle Tipps: Sichern Sie die Daten besser lokal und nicht auf dem Server. Sollte der Server komplett unbenutzbar werden (Meteoriteneinschlag?) – dann nützt Ihnen ein Back-up auf dem gleichen Server nämlich auch nichts mehr. Ein Back-up sollte regelmäßig stattfinden, und im Idealfall testen Sie das Zurückspielen des Back-ups mal (lokal) durch. Dann sind Sie für den Ernstfall wirklich sicher und bereit. Wer Angst hat, dass die kostenlosen Plug-in-Lösungen irgendwann nicht mehr unterstützt werden, kann mit Vaultpress [goo.gl/rQXGY] auch auf einen kostenpflichtigen Back-up-Service zurückgreifen. Wenn Sie viele verschiedene Datenbanken auf dem Server haben und eine WordPress-unabhängige Lösung bevorzugen, sollten Sie sich das Tool MySQL-Dumper [goo.gl/Mu5ZA] mal anschauen.

FAZIT

Der Großteil aller infizierten Blogs kommt durch veraltete Software und schlechte Zugangsdaten zustande. Diese beiden Einfallstore können leicht geschlossen werden. Für den verbleibenden Teil, die echten Sicherheitslücken, sollten Sie sich auf dem neuesten Stand halten über aktuell kursierende Probleme und Angriffsmöglichkeiten. Ein guter Ort für aktuelle Informationen ist das Blog von Sucuri.net [goo.gl/7IMsi], einer Firma, die sich auf das Bereinigen von infizierten Blogs spezialisiert hat. So gewappnet sollten Sie deutlich ruhiger schlafen können, denn die wichtigsten Schritte sind unternommen. Sie sind für den Ernstfall gut gerüstet und haben Vorkehrungen getroffen.

Twitter-Hashtag: #scg17-84



Torsten Landsiedel ist mit Leib und Seele Webworker. Er erstellt, optimiert und bereinigt Webseiten vor allem für kleine und mittlere Unternehmen. Im Supportforum von WordPress.com hilft er seit 2007 als Moderator und teilt auf WordCamps sein Wissen mit der Community.

Twitter-Account: @zodiac1978