Inhalt

Wie schütze ich meinen WordPress Blog?

(Dieser Artikel bezieht sich auf Wordpress-Anwendungen, die auf einem Webhosting-Produkt von Host Europe betrieben werden. Bitte beachten Sie, dass die nachfolgenden Links auf externe Seiten führen. Host Europe übernimmt für die Richtigkeit und die Aktualität der Inhalte keine Verantwortung.)

Leider hört man in den letzten Monaten immer öfter von gehackten Webseiten die mit dem CMS (Content Management System) WordPress erstellt wurden. Aber was genau bedeutet es eigentlich für die Betreiber und Besucher, wenn die Webseite gehackt wurde?

Fremde haben über verschiedene Wege Zugriff auf Ihre Webseite erlangt um diese in unterschiedlichen Weisen zu missbrauchen und anderen zu schaden. Dies kann damit beginnen, dass unter Ihrer Domain plötzlich Werbung für Potenzsteigernde Mittel gemacht wird bis hin zu tausenden Emails mit fragwürdigem Inhalt. Weiterhin werden infizierte WordPress Blogs immer öfter dazu genutzt um gezielte Angriffe auf Systeme dritter auszuüben. Am Ende fällt dies auf Sie zurück, daher ist es wichtig sich im Vorfeld auch über den Aspekt Sicherheit Gedanken zu machen.

Hier möchten wir Ihnen einige wenige, einfache aber sehr wirksame Wege nahelegen, wie Sie sich und auch Ihre Besucher schützen können.

1) Verwenden Sie sichere Passwörter & Benutzernamen

Bitte verwenden Sie immer sichere Passwörter und nach Möglichkeiten auch sichere Benutzernamen. So ist es z.B. nicht ratsam als Benutzernamen „admin“ zu verwenden, auch wenn dies bei der Installation vorgeschlagen wird. **Warum?**
Ganz einfach, weil die meisten Administratoren „admin“ verwenden, so hat der Angreifer schon mal 50% der Daten die erbraucht um sich im Administratorbereich anzumelden. Nehmen Sie aber z.B. „HostEurope2013“ als Benutzername und dann idealerweise noch „my%pass&is!safe“ als Passwort, macht man es dem Angreifer schwerer an die Daten zukommen. Allgemein kann man sagen, verwenden Sie kein Wort als Passwort was in irgendeinem Wörterbuch der Welt vor kommt!
Das gleiche gilt ebenfalls bei den FTP Zugängen oder auch bei den Datenbanken, wobei Sie hier bezüglich des Benutzernamens seitens Host Europe nicht zu 100% frei wählen können, da wir einen Teil bereits vorgeben. Umso wichtiger ist hier die Verwendung sicherer Passwörter.
Bitte verwenden Sie nicht die oben angegebenen Daten, diese sollen lediglich verdeutlichen wie Sie eine sichere Konfiguration erstellen! Verwenden Sie bitte eigene Benutzernamen sowie Passwörter!
Einen guten Passwortgenerator finden Sie auf: http://www.gaijin.at/olspwgen.php

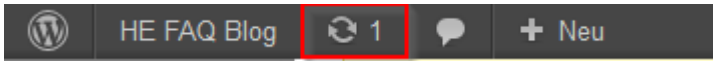
2) Halten Sie Ihre Webseite aktuell!

Dies gilt nicht nur für den redaktionellen Teil sondern mindestens genauso für den technischen. Die Entwickler veröffentlichen in unregelmäßigen Abständen Aktualisierungen für dieses CMS. Diese sollten zeitnah auf Ihrer Webseite eingespielt werden, da mit diesen Aktualisierungen Sicherheitslücken geschlossen werden, die im Laufe des Betriebs aufgefallen sind.
Es gibt inzwischen mehrere Hauptversionen des beliebten CMS WordPress

Wie Sie an der Auflistung oben sehen können werden die Versionen 1 & 2 nicht mehr unterstützt. Das bedeutet, dass es für diese Versionen keine Aktualisierungen mehr geben wird. Es ist daher wichtig, auf die aktuellste Version 3.x umzustellen. Eine ausführliche Beschreibung, wie man bei einem Upgrade von der 2er Version auf die 3er Version am besten vorgeht, finden Sie unter dem folgenden Link:

http://dokupress.de/wordpress-benutzerhandbuch/installation/upgrade-bestehender-installationen/upgrade/

Nun ist es leider so, dass sobald es eine Aktualisierung gibt, auch die potenziellen Angreifer davon erfahren und diese suchen dann nach ggf. vorhandenen neuen Sicherheitslücken. Es ist hier also wirklich wichtig, dass man regelmäßig prüft, ob es Aktualisierungen gibt. Im WordPress-Backend wird Ihnen in der Menüleiste angezeigt, ob ein Update zur Verfügung steht.



Klicken Sie nun einfach auf das Symbol und Ihnen werden alle verfügbaren Aktualisierungen angezeigt. In der Version 3.x werden Ihnen über die eigentlichen Wordpress Updates hinaus auch die Aktualisierungen für die Templates sowie die installierten Plug-Ins angezeigt.

Ganz wichtig: Bevor Sie die Aktualisierungen durchführen, erstellen Sie eine Sicherung Ihres Blogs. Falls bei dem Update etwas schief geht, können Sie die Sicherung wieder einspielen und verlieren nicht Ihren gesamten Blog!
Sie können gerne über das KIS ein Backup „on the fly“ starten. Einen ausführlichen FAQ Artikel dazu finden Sie im FAQ-Bereich.
http://faq.hosteurope.de/index.php?cpid=2543

3) Datensicherung, Datensicherung & nochmal Datensicherung!

Host Europe erstellt jede Nacht eine Sicherung Ihrer Webseite. Dazu zählen die Daten die auf dem Server liegen und ebenso die dazugehörigen Datenbanken. Sie haben Zugriff auf die Sicherungen der letzten 14 Tage und können diese über Ihren

KIS Zugang jederzeit wieder einspielen. Eine Beschreibung zu dieser Funktion finden Sie im FAQ-Bereich. http://faq.hosteurope.de/index.php?cpid=10977

Ein Datenbank-Restore kann aufgrund manueller Aktionen nur innerhalb der Geschäftszeiten (Mo-Fr 9-17 Uhr) ausgeführt werden.

Manchmal muss aber eine Webseite schnell wieder online gehen, und man hat nicht die Zeit, im schlimmsten Fall bis Montag abzuwarten. Hier ist man dann glücklich, wenn man eigene Sicherungen erstellt hat.
Hierzu gibt es nützliche Komponenten, wie z.B. BackUpWordPress. Mit dieser Komponente können Sie zu definierten Zeiten Sicherungen erstellen lassen - und das vollautomatisch.

Sie finden dieses Plug-In unter dem Link:
http://wordpress.org/plugins/backupwordpress/

4) Schützen Sie Ihren Administrationsbereich!

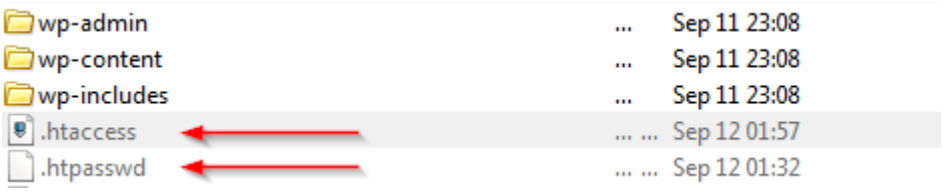
Jeder, der sich mit WordPress einmal beschäftigt hat, weiß, wie man den Administratorbereich erreichen kann. Dieser ist immer erreichbar unter http://meinedomain.de/wp-admin und ebenfalls unter http://meinedomain.de/wp-login.php.

Dies ist auch den Angreifern bekannt. Eine einfache aber wirksame Methode sich zu schützen ist der Schutz dieses Bereiches mit einem Zugriffsschutz.

Hier kann man mit einer .htaccess Datei arbeiten, die den Zugriff auf die wp-login.php sowie auf das Unterverzeichnis /wp-admin unterbindet. Die in den meisten Fällen bereits vorhandene Server-Datei .htaccess (meist von WordPress für die Steuerung der Permalinks verwendet) wird um 2 Code-Blöcke mit minimaler Pfadanpassung erweitert. Zusätzlich benötigen Sie noch eine Datei .htpasswd mit Zugangsdaten die ebenfalls in das Hauptverzeichnis Ihres Blogs gehört.

Hinweis: Nachfolgend erhalten Sie ein Beispiel einer solchen htaccess-Datei. Bitte beachten Sie, dass dieser Zugriffschutz in der .htaccess **nicht** greift, wenn Sie ein WebPack M verwenden, da hier nur Permalink-Regeln ausgeführt werden.

Anleitung für einen Zugriffsschutz via .htaccess



1. Bitte legen Sie eine leere Datei mit dem Namen .htpasswd im Hauptverzeichnis Ihres Blogs an.
2. Die erstellte Datei öffnen Sie nun bitte mit einem Editor. Wir empfehlen notepad++ oder pspad. In unserem FAQ-Bereich steht pspad unter dem Punkt Downloads>HTML-Editoren zur Verfügung.
3. Rufen Sie den htaccess Generator unter dem folgenden Link auf http://www.htaccesstools.com/htpasswd-generator/ und geben in den Eingabefeldern den gewünschten Nutzernamen und ein sicheres Passwort ein – diese Kombination aus Benutzernamen und Passwort ist der Zugang für die .htaccess Abfrage. Die vom htpasswd Generator erzeugte Zeichenfolge wird in die geöffnete Datei .htpasswd eingefügt und gespeichert.
4. Die Datei .htaccess im Editor öffnen und um den nachfolgenden Code erweitern. Bitte beachten Sie, dass der Pfad zu .htpasswd angepasst werden muss, damit der Server diese Datei auch finden und laden kann. Sollten Sie den korrekten Pfad nicht kennen, finden Sie hier eine Anleitung wie Sie diesen ermitteln können:

   http://www.htaccesstools.com/articles/full-path-to-file-using-php/

5. Änderungen speichern und das Ergebnis kontrollieren.

Zugriffsschutz + Interner Schutz für Systemdateien

###Start der .htaccess###

```
<Files wp-login.php>
  AuthName "Admin-Bereich"
  AuthType Basic
  AuthUserFile /is/htdocs/wpxxxxxxxx_1YSU5QDCCL/www/wordpress/.htpasswd
  require valid-user
</Files>
<FilesMatch "(\.htaccess|\.htpasswd|wp-config\.php|liesmich\.html|readme\.html)">
  order deny,allow
  deny from all
</FilesMatch>
```

###Ende der .htaccess ###

Bitte nur den Teil zwischen ###Start der .htaccess### und ###Ende der .htaccess ### in Ihren Dateien eintragen! In der Datei muss dann noch der Pfad zur htpasswd korrekt eintragen werden. Die Pfadangabe finden Sie im KIS unter

Administration > *IHR PRODUKT* > Konfigurieren > Allgemeines > Allgemeine Informationen

Hier finden Sie in der Tabelle „Allgemeines“ einen Eintrag „Pfad“. Dies ist der Pfad auf unserem Server zu Ihrem Paket.

Es gibt viele weitere Optionen das Backend vor Zugriff zu schützen, von URL

Erweiterung bis Wordpress Firewall etc. Da dies aber alles über Plug-Ins generiert wird, und man nie sicher sagen kann, ob nicht am Ende genau diese Plug-Ins zu einem Sicherheitsproblem führen, konzentrieren wir uns hier auf die simplen Wege, die meistens dann noch die besten und effektivsten sind.

5) Sichern Sie Ihre Erweiterungen durch Captcha Abfragen!

Wenn Sie Formulare, Gästebücher oder Foren unter WordPress betreiben ist es wichtig, dass Sie diese entsprechend absichern. Hier stehen Ihnen unterschiedliche Captcha Plug-Ins zur Verfügung. Es empfiehlt sich im Vorfeld zu recherchieren, ob es für die eingesetzten Plug-Ins Empfehlungen gibt. Manchmal sind sogar schon in dem Plug-In Captchas integriert bzw. vorbereitet.

Eine kleine Übersicht bewährter Captchas für Wordpress Blogs finden Sie hier:

http://www.vouchsafe.com/downloads/plugins-for-cmss-and-apps/24-vouchsafe-for-wordpress
http://wordpress.org/plugins/funcaptcha/
http://wordpress.org/support/view/plugin-reviews/sweetcaptcha-revolutionary-free-captcha-service

Prüfen Sie weiterhin auch, ob Sie alle installierten Plug-Ins und Module tatsächlich auf Ihrer Webseite verwenden. Oftmals testet man während der Erstellung der Webseite unterschiedliche Erweiterungen, setzt diese aber schlussendlich gar nicht ein. Diese Erweiterungen werden dann in der Regel auch nicht gepflegt und bieten Fremden so leichte Wege Ihre Webseite zu infizieren. Diese, nicht verwendeten Erweiterungen, deinstallieren Sie bitte über das Backend.

6) Ändern Sie die Sicherheitsschlüssel in der wp-config.php!

Sobald man sich in WordPress einloggt, werden durch Cookies verschiedene Informationen im Browser zwischengelagert. Die Sicherheitsschlüssel spielen bei der Verschlüsselung der Informationen, die in den Cookies abgelegt werden, eine wichtige Rolle. Sie sorgen dafür, dass Manipulationen seitens eines Angreifers erheblich erschwert werden und tragen damit zu einer höheren Sicherheit bei.

Mit Version 2.5 wurde in WordPress erstmals ein Sicherheitsschlüssel (SECRET_KEY) eingeführt. Dieser wurde ab Version 2.6 durch drei andere Schlüssel (AUTH_KEY, SECURE_AUTH_KEY und LOGGED_IN_KEY) ersetzt und mit Version 2.7 kam schlussendlich ein weiterer Schlüssel (NONCE_KEY) hinzu.

Diese Sicherheitsschlüssel müssen in der Konfigurationsdatei wp-config.php eingetragen werden. Bei einer Neuinstallation wird man derzeit noch nicht aufgefordert diese Schlüssel anzugeben – an keiner Stelle des Installationsvorgangs wird man über die Sicherheitsschlüssel informiert und lediglich im Quelltext der Datei wp-config-sample.php (bzw. wp-config.php) gibt es einen Hinweis. Auch bei einer Aktualisierung wird nicht überprüft ob die Sicherheitsschlüssel vorhanden sind.

WordPress bietet Ihnen auf https://api.wordpress.org/secret-key/1.1/salt/ den Service, diese Keys zu generieren. Nutzen Sie ihn daher, da diese Schlüssel wirklich zur Sicherheit Ihrer Webseite beitragen.
Tauschen Sie den generierten Zeichenblock einfach gegen den Originalblock in der wp-config.php aus.

```
/**#@+
 * Sicherheitsschlüssel.
 *
 * Ändere jeden KEY in eine beliebiege, möglichst einzigartige Phrase.
 * Auf der Seite {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key
 * Bitte trage für jeden KEY eine eigene Phrase ein. Du kannst die Schlüssel jederzeit wieder än
 *
 * @seit 2.6.0
 */
define('AUTH_KEY',         '`.T9)>y+USgNBM-hs*3mBZOCu2bM!=H2,/yX`D=Qq7`u}t&dV)PcNc`+36L,cj+#');
define('SECURE_AUTH_KEY',  'tA.dD0o_q;E7;X-s%_xKYSnw@&r=)zwR|F(-W/|{ZWh>Ovsm`A`-5?RjhjZ$|hb$');
define('LOGGED_IN_KEY',    'n$I1]<A{*qM%ic.MeQqI)Gfl<dtb1gWIsa28+u7+|6Tmfe|i<9bCG^]>6b[C^64z');
define('NONCE_KEY',        'VRr r^Z;Jq%%|3XKep-wd$s?`_qV,p5G6z1`]E7||4:+:ZR+*{6vEm,GtTSe$y-G');
define('AUTH_SALT',        'IxWfu`B-sXW#/U$@)Yu-ES:H--MQE$%@t~Hu,+{|(jBDo3T54OO]E|k1r>]-Xo42');
define('SECURE_AUTH_SALT', 'ob>**>rs3-2AC(-0ha(I*-KxHA@[cr-CZ^Nzh%pOli1EU[<Y&.|hoUCLhPtLN61U');
define('LOGGED_IN_SALT',   '=2)KdI<wCcsve~eE?}$_XD]tR=~TGXiKm+0jG$SsX/)ct^;u_U/ pP5x}[evWv]+');
define('NONCE_SALT',       '$#dpvvK/<8-bg+:OJ4MO0^HwZ_].:fF!iQpsXu,@|05aJ$5K)L6zD}x:-Vk?e@N$');
```

Fazit: Je mehr Maßnahmen getroffen werden, die es Angreifern der erlangen von Infos über WordPress-Installationen oder Zugänge erschweren, desto besser. Diese Maßnahmen werden von manchem in Frage gestellt, weil es Profihacker nicht gänzlich behindert. Wir sehen das anders und vergleichen die Situation gerne mit Häusern: Nur weil ein Einbrecher auch eine Fensterscheibe einschlagen könnte um in ein Haus einzubrechen, lässt man nicht die Haustür sperrangelweit offen.

7) Dateiberechtigung anpassen, optimieren und sichern !

Viele Anwender setzen die Dateiberechtigung sehr hoch, da Sie so Probleme mit Ihrem WordPress-Blog bzw. den installierten Komponenten, Modulen oder Plug-Ins verhindern können. Dies ist zwar verständlich, aber nicht sinnvoll, da Sie so auch Angreifern ermöglichen, diese Rechte zu missbrauchen.

Wir empfehlen daher folgende Rechtevergabe:

→ Benutzer: FTPXXXXX
→ Gruppe: WPXXXXX
→ alle Verzeichnisse erhalten die Rechte 750
→ alle Dateien erhalten die Rechte 640

Folgende Verzeichnisse benötigen die Rechte 770 damit WordPress fehlerfrei arbeiten kann:

/wp-admin/index.php
/wp-content/
/wp-content/plugins
/wp-content/upgrade
/wp-content/uploads
/wp-content/cache
./wp-cache-config.php
/wp-content/backup/

Bei diesen Verzeichnissen setzen Sie die Berechtigung bitte rekursiv (dies bedeutet, dass diese Rechte für das Verzeichnis und alle Unterverzeichnisse gilt):

/wp-admin/
/wp-includes/
/wp-content/themes/
/wp-content/

	NAME	TYP	GRÖSSE IN MBYTES	RECHTE	BENUTZER	GRUPPE	ZULETZT GEÄNDERT	
↘Ebene höher								
☐	↘wp-admin	-dir-	0	770	wp12624920	wp12624920	2014-12-19 15:47	
☐	↘wp-content	-dir-	0	770	wp12624920	wp12624920	2014-12-19 15:47	
☐	↘wp-includes	-dir-	0	770	wp12624920	wp12624920	2014-12-19 15:47	
☐	licens.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	licenza.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	liesmich.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	lisenssi.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	readme.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	readme-ja.html	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	index.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-activate.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-blog-header.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-comments-post.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-config.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-config-sample.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-cron.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-links-opml.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-load.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-login.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-mail.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-settings.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-signup.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	wp-trackback.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	xmlrpc.php	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	LEGGIMI.txt	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	licencia.txt	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐	license.txt	-file-	0	640	wp12624920	wp12624920	2014-12-19 12:47	
☐ Alle				x x 0	nicht ändern	nicht ändern	☐rekursiv Ändern	Löschen

Unterstützende Hilfe zum Thema Dateiberechtigung finden Sie im nachfolgenden FAQ-Artikel.

https://www.hosteurope.de/faq/webhosting/hochladen-von-webinhalten-ftp/dateiverwaltung/

Wir hoffen, dass Ihnen diese Tipps helfen, Ihren WordPress Blog abzusichern und damit vor Angreifern weitestgehend zu schützen.

Für weitere Anfragen stehen wir Ihnen gerne über support@hosteurope.de oder telefonisch unter 0800 467 8387 zur Verfügung.