Drupal Website gehackt?

Automatisierte Angriffe auf ältere Drupal-Versionen (Älter als Version 7.32)

Es ist davon auszugehen, dass alle Drupal 7 Webseiten die auf einer älteren Version als 7.32 basieren im Oktober 2014 gehackt wurden.

Bin ich auch betroffen?

Sehr wahrscheinlich. Dieser automatisierte Angriff hat jede Drupal 7 Website getroffen, die online geschaltet war. Es kommt vor, dass die Angreifer Spuren hinterlassen. Beispielsweise befinden sich neue Administratoren im Backend oder infizierte Dateien im Webspace. In der Regel jedoch, versuchen die Angreifer ihre Spuren zu verwischen und entscheiden erst später, was mit Ihrer Website und den Daten passiert.

Ein nachträgliches Update bringt nichts

Wichtig! Ein nachträgliches Update bringt nicht die nötige Sicherheit. Wurde das Update nicht bis zum 15. Oktober 2014 eingespielt, ist davon auszugehen, dass die Website gehackt worden ist.

Das bedeutet, sämtliche Dateien und Datenbanken können gesichert und gesteuert werden. Die Benutzerdaten und Passwörter liegen offen. Jederzeit kann der Angreifer die Website-Inhalte ändern, kopieren oder offline setzen.
Spam Emails können über Ihre Website gesendet werden.
Hier stehen Sie in der Pflicht.

Hintertüren sind sehr schwer zu finden

Ein nachträgliches Bereinigen der Dateien und Datenbanken, lässt ebenfalls Risiken offen. Es gibt tausende Möglichkeiten, sogenannte Backdoors (Hintertüren) zu hinterlassen und die Website zum späteren Zeitpunkt **auszuspähen und zu steuern**. Diese zu finden ist fast unmöglich.

Sie haben jetzt zwei Möglichkeiten

Um **100%ig sicherzugehen**, dass auch zukünftig nichts mit Ihrer Website passiert,

gibt es zwei Möglichkeiten:

- Ihnen liegt ein **FTP- und Datenbank-Backup**, welches **vor dem 15. Oktober 2014 erstellt** worden ist, vor und Sie spielen dieses inklusive der neuen Drupal-Version ein.
- **Wiederaufbauen:** Sie löschen den kompletten FTP sowie Datenbanken. Ändern sämtliche Passwörter und konstruieren Ihre Website, basierend auf der neuesten Drupal Version nach. Mit unserer **Drupal-Spezialisierung** übernehmen wir das für Sie.

Sollten Sie bereits mit einem Webdesigner zusammenarbeiten ist dies auch kein Problem. Gerne kümmern wir uns um die **Wartung und Sicherheit Ihrer Website [1]**, während Design und Inhalt von Ihrem ursprünglichen Webdesigner gepflegt wird.

Informationsquellen zum großen Drupal-Hack finden Sie hier:

- PHP Magazin - Drupageddon Auswirkungen [2]
- heise online - Drupal 7 schließt Worst Case Sicherheitslücke [3]
- DrupalCenter.de - "... Empfohlen wird nach Möglichkeit das Einspielen eines Updates aus der Zeit vor Bekanntwerden der Sicherheitslücke..." [4]
- ZDNet - Drupal warns unless you patched within seven hours, you're hacked [5]

Kategorie:
Drupal [6]
Tags:
Drupal [7]
Hack [8]
SQL-Injection [9]
Drupageddon [10]

Links
[1] https://internetaces.com/de/wartung-pflege
[2] http://www.php-mag.de/news/drupageddon-auswirkungen-177151
[3] http://www.heise.de/security/meldung/Update-fuer-Drupal-7-schliesst-Worst-Case-Sicherheitsluecke-2425878.html
[4] http://www.drupalcenter.de/node/52041
[5] http://www.zdnet.com/article/drupal-warns-unless-you-patched-within-seven-hours-youre-hacked/
[6] https://internetaces.com/de/blog-kategorien/drupal
[7] https://internetaces.com/de/tags/drupal
[8] https://internetaces.com/de/tags/hack

[9] https://internetaces.com/de/tags/sql-injection
[10] https://internetaces.com/de/tags/drupageddon