Hilfe bei gehackter WordPress-Seite

Malware finden & Schadcode entfernen.

Rund 35 % aller Internetseiten im Web werden mit WordPress betrieben. Unter den Content-Management Systemen entspricht das einem Marktanteil von satten 62 % (Stand 2020).
Die massive Verbreitung und Beliebtheit von WordPress macht das System zu einem attraktiven Angriffsziel für Hacker. In den allermeisten Fällen finden Angriffe völlig automatisiert statt. Ziel sind nicht einzelne Unternehmen oder Personen, sondern bekannte Schwachstellen im Core und in den Plugins. Die Hauptursache für gehackte Webseiten sind also versäumte Sicherheitsupdates. Gleiches gilt auch für Joomla! sowie alle anderen CMS- und Shopsysteme.

Für den Fall, dass Ihr WordPress gehackt wurde, finden Sie hier eine Zusammenstellung der wichtigsten Schritte mitsamt einiger Tipps.

Schritt 1: Website deaktivieren - Backups herunterladen

Um weitere Schäden zu vermeiden, sollte die Webseite zuallererst offline genommen werden. Zwei bewährte Möglichkeiten:

- .htaccess Passwortschutz (example.org/xssen.php)
- Umbenennung/Umleitung des Basisverzeichnisses (Wartungsseite einrichten)

Im Anschluss laden Sie Sicherungen von allen relevanten Daten herunter. Neben des Dateisystems und der Datenbank gehören auch die Logdateien des Servers für die unbedingt notwendige Analyse des Hackerangriffs dazu. Diese befinden sich entweder im /logs Verzeichnis auf dem Webspace oder sind über das Control Panel des Webhosters abrufbar.

Schritt 2: Einbruch analysieren - Sicherheitslücke finden

Für die Malware Analyse ist es wichtig, dass die Zeitstempel der heruntergeladenen Dateien erhalten bleiben (Option im FTP Programm). Damit kein Virus-Alarm die Übertragung stört, deaktivieren Sie temporär den lokalen Virenschutz.

Potenzielle Schaddateien finden Sie wie folgt:

- Kürzlich veränderte Dateien inspizieren
- *Malware Logs des Hosters durchgehen*
- *Lokaler Scan der Daten mit guter Anti-Virus-Software*
- WordPress Root Verzeichnis prüfen
    - Halten Sie Ausschau nach Dateinamen != .htaccess, index.php, wp-*.php, xmlrpc.php (Standardmäßig liegen 15 PHP Dateien im WP Hauptverzeichnis

Von jedem Schadcode Fund den Timestamp (Datei Änderungszeitpunkt) notieren.
Achtung! Dieser kann durchaus auch verfälscht sein - unauffällig dem der übrigen Dateien im jew. Verzeichnis

entsprechen. Auch die Timestamps der Verzeichnisse sollten beachtet werden.
Basierend darauf:

- Analyse der Webserver Access Logs
    - Auffällige POST Einträge
    - Typische Angriffsmuster

Ein hilfreiches Tool für das Herauspicken der POST Requests und weitere Tipps zur Auswertung finden Sie hier.

Schritt 3a: Backup wiederherstellen

Wenn sich der Zeitpunkt der Kompromittierung anhand der Logdateien zweifellos feststellen lässt und ein Backup vorliegt, bietet sich die Wiederherstellung und anschließende Aktualisierung und Absicherung dessen an.

Schritt 3b: Dateisystem bereinigen (WP + Plugins neu installieren)

Damit ausgeschlossen werden kann, dass sich weiterhin Malware in den Core und wp-content Verzeichnissen befindet, ist die Neuinstallation des WordPress Kerns und aller Plugins nötig.

1. Alle Systemdateien von WordPress ersetzen, dafür wp-admin/ und wp-includes/ komplett löschen.
2. Alle Plugins durch saubere Versionen ersetzen, dafür alle Ordner in wp-content/plugins/ löschen, gleiches gilt für das Theme.
3. Alle PHP-Dateien in wp-content/uploads/ suchen/löschen.

Auch bezahlte Premium Plugins müssen mit einem frischen Installationspaket direkt aus der Quelle neu installiert werden - nehmen Sie hier nicht einfach die Version aus dem Backup. Schon eine einzelne übersehene Schaddatei reicht aus, dass die WordPress Installtion darüber erneut gehackt werden könnte.

Schritt 4: Passwörter ändern

Die Änderung sämtlicher Passwörter versteht sich von selbst - FTP, MySQL (Datenbank), WordPress Accounts usw.
Dabei sollten Sie es vorziehen starke Passwörter zu verwenden mit Groß-/Kleinbuchstaben, Zahlen und für maximale Sicherheit zusätzlich Sonderzeichen.

Um zu vermeiden, dass Ihr WordPress erneut gehackt wird, müssen regelmäßig Updates durchgeführt werden. Nur so lässt sich das größtmögliche Maß an Sicherheit erhalten.

Symptome einer gehackten Website

Häufig wird gefragt, was Angreifer mit der Kompromittierung einer Webseite bezwecken wollen. Das Hauptziel ist es vorerst, den Web-Account durch das Hinterlegen von Webshells kontrollieren zu können und über versteckte Backdoors jederzeit erneut Zugriff erlangen zu können - auch wenn

Teile der Schaddateien bereits gelöscht worden sind. Der Angreifer hat dadurch freie Hand und die vollständige Kontrolle mit faktisch unbegrenzten Möglichkeiten.
Im Wesentlichen kann es auf kurz oder lang zu folgenden Symptomen kommen.

Umleitungen & Pop-ups

Beim Klick auf ein Google Suchergebnis öffnet sich nicht die eigentliche Seite, sondern man wird auf eine ganz andere Domain mit meist eher unseriösem Inhalt umgeleitet. Eine Umleitung oder Popups können auch erst nach dem Einstieg, zufällig während der Navigation über die gehackte Website ausgelöst werden. Manchmal kommt es abhängig vom Referrer & User-Agent nur sporadisch zu dieser Weiterleitung.

Spam Versand

Der Klassiker - Hacker platzieren ein Spam-Script gut versteckt auf dem Webspace und nutzen dies für den massenhaften Versand von Spam Mails. Die Folge können Blacklist Einträge sein, bspw. in der spamhaus.org Datenbank, die den E-Mail Verkehr stören. Glücklicherweise erkennen die meisten Webhoster den Versand von Massenmails, sodass dem im Idealfall schnell ein Riegel vorgeschoben wird.

Black-Hat SEO

Es werden haufenweise Links innerhalb des Contents mit hart umkämpften Keywords platziert (typisch sind z.B. Pharma Hacks) oder die Inhalte werden inkl. der Meta Description vollständig ausgetauscht. Je länger dieser Zustand andauert, desto erheblicher werden die Einbußen im SEO Ranking.

Verteilung von Viren & Malware

Insbesondere in diesem Fall muss die betreffende Seite sofort abgeschaltet werden. Die Auslieferung eines Virus kann weitreichende Folgen haben. Vom Ransomware Virus hat wohl jeder schon mal gehört. Dass die Seitenbesucher sich Schadsoftware einfangen, sollte unbedingt vermieden werden.