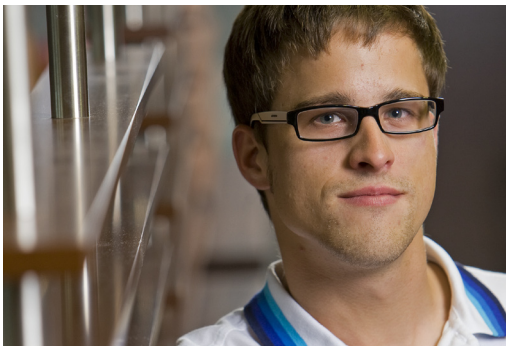
Auszug Whitepaper „Sicherheit für Blogs und PHP“

SCHUTZ UND VORSORGE



KASPERSKY-EXPERTE CHRISTIAN FUNK EMPFIEHLT: SCHUTZ DURCH VORSORGE

Blogs schützt man am besten präventiv

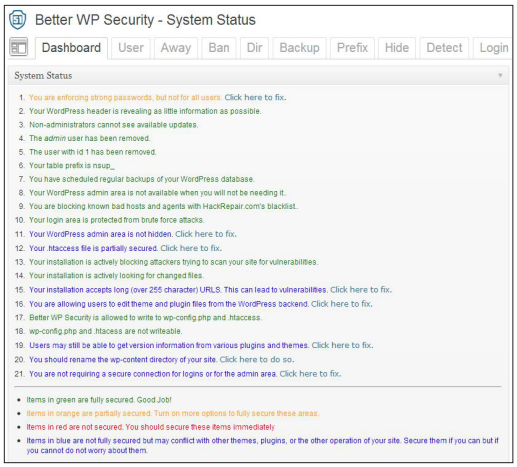
Wie kann ich am besten verhindern, dass mein Blog gehackt wird? Mit präventiven Maßnahmen, empfiehlt Christian Funk, Virenexperte bei Kaspersky Lab. Denn besser als Aufräumen nach der Attacke ist das Verhindern der Attacke an sich. Tatsächlich kann man mit ein paar einfachen Regeln die Angriffsfläche auf den eigenen Blog deutlich verringern und vor allem Massenattacken und Defacements wirkungsvoll verhindern.

Die wichtigste Regel lautet: Updates. Egal ob es sich um eine neue Version des Blogsystems, eines Plugins oder eines Themes handelt, sobald die Macher eine Aktualisierung zur Verfügung stellen, sollte diese schnellstmöglich installiert werden. Der Grund dafür ist oben beschrieben: Spätestens wenn eine behobene Schwachstelle dokumentiert wurde, werden Angreifer diese in ihre Programme integrieren. Allerdings sollte man sich hier nicht in Sicherheit wiegen: Selbst bevor Schwachstellen offiziell bekannt werden, können diese den Kriminellen bereits bekannt sein.

Der nächste Schritt ist das Abhärten der Web-Applikation. Hinter diesem Begriff verstecken sich bewährte Mittel und Wege, um die eigene Angriffsfläche weiter zu verringern. Für Wordpress haben die Macher eine umfangreiche Dokumentation [1] zusammengestellt, für alle anderen Systeme gibt es ähnliche Anleitungen. Im Zweifel hilft eine Suche nach „Systemname + Hardening“.

Folgende Punkte gelten für die meisten Systeme:

- Verbergen Sie die Versionsnummer: So haben Angreifer eine deutlich kleinere Chance, mit automatisierten Skripten herauszufinden, ob Ihr System veraltet ist.
- Ignorieren Sie den Standard-Admin-Nutzer: Dieser ist meist sehr gut dokumentiert, entsprechend einfach können ihn Kriminelle abfragen. Besser ist es, den eigentlichen Admin-Account nach der Installation einzumotten oder zu deaktivieren und einen dedizierten, neuen Account anzulegen.
- Nutzen Sie die verfügbaren Rechtestufen: Nicht jeder Nutzer benötigt einen Vollzugriff. Selbst wenn Sie Ihren Blog alleine führen, sollten Sie bei alltäglichen Aufgaben einen Account mit möglichst wenig Rechten verwenden. Denn Vollzugriff benötigen Sie eigentlich nur für Updates des Systems.
- Achten Sie auf Berechtigungen: Oftmals müssen nicht alle Daten auf dem Webserver von jedermann les- und schreibbar sein. Beschäftigen Sie sich mit den notwendigen Berechtigungen und passen Sie diese für Ihre Installation an.
- Je weniger Plugins, desto besser: Jedes Plugin öffnet potenziell einen neuen Weg in Ihr System. Achten Sie darauf, möglichst wenige Erweiterungen zu installieren. Unnötige Erweiterungen sollten Sie zumindest deaktivieren, idealerweise sogar löschen.
- Updates, Updates, Updates: Installieren Sie Aktualisierungen, sobald diese verfügbar sind. Achten Sie zudem darauf, dass alle verwendeten Plugins und Themes aktiv weiterentwickelt werden – nichts ist schlimmer, als auf veraltete Software zu setzen.
- Nutzen Sie Sicherheits-Plugins: Eine Ausnahme von der „möglichst wenig Erweiterungen“-Regel stellen Sicherheits-Plugins dar. Diese können oftmals viele der Best-Practices automatisch durchführen und den eigenen Blog gegen Angreifer schützen (siehe Bilder unten).
- Backups: Nutzen Sie die Funktionen Ihres Systems, um in regelmäßigen Abständen Sicherungen anlegen zu lassen. Dadurch können Sie im Falle einer Attacke Ihr System schneller wieder zum Laufen bringen.



Erweiterungen wie Better Security für WordPress integrieren eine ganze Reihe von Best-Practice-Ansätzen für die Sicherung der Website.

Einmal eingerichtet blockieren Sicherheitserweiterungen fehlerhafte Zugriffe automatisch.

Quelle:

[1] http://codex.wordpress.org/Hardening_WordPress

Dieser Text ist Teil des Kaspersky-Whitepapers „Sicherheit für Blogs und PHP - Wordpress und Co. vor Hackern schützen“. Das Whitepaper ist unter http://www.kaspersky.com/de/downloads/pdf/kaspersky_whitepaper_blogs_und_security_final.pdf abrufbar oder kann bei kaspersky@essentialmedia.de per E-Mail angefragt werden.