KASPERSKY lab

Auszug Whitepaper „Sicherheit für Blogs und PHP“

SCHUTZ FÜR PHP

PHP-Seiten sind bei Unternehmen beliebt, aber auch leicht angreifbar

Nicht jedes Unternehmen setzt zwingend auf ein komplettes Content Management System, einige entscheiden sich lieber für ein PHP-basiertes System, um die eigene Webseite zu betreiben oder Dienste zur Verfügung zu stellen. Das hat zunächst den Vorteil, dass man gegen Attacken auf verwundbare Blogging-Plugins geschützt ist. Allerdings ist auch PHP keineswegs eine uneinnehmbare Festung für Angreifer, im Gegenteil. Seit 2000 listet CVE Details [1] über 340 gefundene Schwachstellen und mindestens 41 Exploits auf.
Attacken auf PHP finden daher ebenso statt, wie Angriffe auf Blog-Systeme. Das liegt auch daran, dass man bei einer erfolgreichen Attacke auf PHP umfassende Rechte auf dem Zielsystem erhält, da PHP den Unterbau für interaktive Seiten und Systeme liefert. Wer also eine erfolgreiche Attacke entwickelt, kann diese für zahlreiche Webseiten und -Dienste nutzen.

Entsprechend müssen auch PHP-basierte Anwendungen gegen bösartige Besuche geschützt werden. Die wichtigste Regel ist auch hier die Aktualisierung von Komponenten. Egal ob PHP oder unterstützende Programme wie etwa ImageMagick: Sobald neue Versionen erhältlich sind, sollten die Verantwortlichen diese schnellstmöglich in Update-Pläne aufnehmen, um bekannte Schwachstellen zu schließen und die eigene Angriffsfläche zu minimieren.

Schritt Nummer 2 ist das Härten der PHP-Installation. Ähnlich wie bei Wordpress gibt es zahlreiche Anleitungen und Ressourcen zum Thema PHP Hardening. Einen ersten Ansatz liefert dafür die offizielle Dokumentation [2], zahlreiche andere Ressourcen im Web sind nur eine einfache Suchanfrage entfernt.

Quellen:

[1] http://www.cvedetails.com/product/128/PHP-PHP.html?vendor_id=74
[2] http://www.php.net/manual/de/security.php

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.