Auszug Whitepaper „Sicherheit für Blogs und PHP“

GEGENMASSNAHMEN NACH ATTACKEN

Checkliste Erste Hilfe nach Attacken auf Blogsysteme

Egal ob Massenattacke, Defacement oder gezielter Angriff, das sollten Sie nach einem Angriff auf Blogsysteme beachten:

Das Erste-Hilfe-Set nach einer Attacke: Computer scannen, Blog reinigen, Passwort ändern und Backup nutzen

- Ruhe bewahren und keineswegs überstürzte Aktionen starten.
- Den betroffenen Server offline nehmen und vorübergehend durch eine statische HTML-Seite ersetzen.
- Falls Sie Anzeige erstatten wollen: Einen Experten für Forensik hinzuziehen, um Beweise zu sichern.
- Alle lokalen Systeme mit einem Virenscanner überprüfen [1].
- Den Blog reinigen: Versuchen Sie, alle infizierten Elemente des Blogs zu finden und nutzen Sie dazu die Support-Seiten des Bloganbieters. Ziehen Sie gegebenenfalls einen Experten hinzu. Für Wordpress gibt es dazu ein ausführliches FAQ [2].
- Sämtlicher Passwörter ändern [3], um die Zugänge zu Webinterface, FTP- und Datenbankserver zu schützen.
- Falls aktuelles Backup vorhanden: Inhalte des Webspace und der Datenbank löschen, Blog komplett neu aufsetzen und letztes Backup einspielen. Beachten Sie dazu die Hinweise des Bloganbieters [4].

Falls Sie nicht über ein aktuelles Backup verfügen, sichern Sie stattdessen am besten alle Daten auf einem lokalen System. Auch Opfer einer Defacement-Attacke können unter Umständen die wichtigsten Daten wiederherstellen. Suchen Sie entsprechende Anleitungen im Internet und geben Sie die Wörter „Gegenmaßnahmen“, „Clean“ oder „Help“ sowie die Nachricht oder den Namen der Angreifer als Suchbegriffe ein.

[1] http://www.kaspersky.com/de/home_user
[2] http://codex.wordpress.org/FAQ_My_site_was_hacked
[3] http://www.kaspersky.com/de/news?id=207566607
[4] http://codex.wordpress.org/Restoring_Your_Database_From_Backup

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.