Security & Firewalls: Was tun nach einem Einbruch

Problem:

Sowohl im ServerSupportForum als auch im rootforum ist immer wieder die Diskussion zu lesen: "Was tun nach erfolgreichem Einbruch oder Kompromitierung?"

Viele Hoster/Provider bestehen auf eine Neuinstallation des gesamten Servers.

Leider sagen die "erfahrenen Jungs" vom rootforum dies ebenfalls (siehe unten).

Diskussion um die Neuinstallation:

Es gibt viele Argumente...

Pro:

- Viele Server-Besitzer können eh nicht mit dem Server umgehen und die Probleme gar nicht erfassen.
- Bei einer Neuinstallation kann man direkt die aktuellen PHP-/CMS-Versionen installieren.
- Nur weil gewisse "Scanner" (z.B. rkhunter) sagen, daß ein System sauber ist, ist es das auch.

Kontra:

- Eine Neuinstallation kostet viel Zeit und Nerven.
- Meistens gehen dabei Daten verloren wie z.B. Emails, Passwörter, aktuelle Datenbank-Einträge.
- In der Regel wird ein Backup der Webs erstellt, der Server neu aufgesetzt und dann das Backup wieder eingespielt.

  Da die meisten Einbrüche über unsichere Scripte kommen, installiert man sich so seine Lücke direkt aufs Neue und der entsprechende Angreifer kann sie auch sofort wieder ausnutzen.

Fazit:

Bei einem solchen Einbruch sollte man auf jedenfall einen Fachmann hinzu ziehen.

Ein entsprechend erfahrener Administrator kann alle Ungereimtheiten entfernen und den gesamten Server absichern. Ein richtig guter Admin findet sogar die Lücke im System (sind meistens

PHP-Scripte) und kann diese flicken bzw. entschärfen.

Weiterhin kann man (schon lange vorher) entsprechende IDS (Intrusion-Detection-Systems) installieren. Hier spielen Snort und Tripwire eine entscheidende Rolle.

Weiterführende Links:

- rootforum.de: Vorgehensweise bei gecracktem Server
- rootforum.de: Warum sollte ich nach einem erfolgreichen Angriff mein Systems neu aufsetzen lassen?

Eindeutige ID: #1250
huschi
2007-08-10 18:23