Security & Firewalls: Woran erkennt man einen erfolgreichen Einbruch (Hack)?

Frage:

Woran erkennt man denn einen Einbruch?

Meistens ist es ja zuspät, weil der Provider bereits den Server gesperrt hat.

Antwort:

Es sind meist einfache Spuren:

- Sehr viele unerklärliche Einträge im Maillog.
- Cron-Einträge von Programmen, die Du nie installiert hast.
- Software die im `/tmp/`, `/var/tmp/` oder `.phptemp/` installiert ist.
- Ansteigender Traffic.

Ein besonderer Augenmerk ist meist auf alle Aktivitäten und Dateien von User `www`|`wwwrun`|`www-data` zu richten, da die meisten Einbrüche per Cross-Site-Scripting (XSS) in schlecht gesicherten Web-/PHP-Anwendungen stattfinden.

Prevention:

Programme wie `logwatch` und `rkhunter` bringen zwar keine Verbesserung der Sicherheit, lassen aber rechtzeitige Aufschlüsse über Versuche zu.

Traffic-Auswertung per IAM z.B. helfen ebenfalls: Traffic über einzelne Ports messen

Ansonsten hilft ein ständiges Updaten aller Software-Pakete (`apt-get`, `up2date` oder `yum`) und vorallem ein anständig abgesichertes PHP.

Eindeutige ID: #1174
huschi
2006-06-13 20:42