Sicherheit

Woran erkenne ich das mein Server gehackt / kompromitiert wurde?

Diese Frage ist sehr schwierig zu beantworten ist. Im Extremfall erkennt man das gar nicht oder nur mit speziellen Analysetools.

Ungewöhnliches Verhalten Ihres Servers kann ein Anzeichen sein, muss es aber nicht. So kann ein erhöhtes aufkommen als unzustellbar zurückgesendeter E-Mails ein Indiz dafür sein, dass Ihr Server für den Versand vom Spam E-Mails missbraucht wird. Das selbe Phänomen tritt aber auf, wenn jemand die Adresse des Servers als Absenderadresse verwendet um einer Existenzprüfung der Absenderdomäne zu überlisten. In letzterem Fall hat Ihr Server mit dem Versand nichts zu tun, erhält aber alle als nicht zustellbar zurückgesendeten E-Mails.

Ein sicheres Zeichen dafür, dass ein Unbefugter sich auf Ihrem Server zu schaffen gemacht hat, ist immer das Verschwinden von Log Dateien oder die Veränderung von Daten.

Wenn Sie den Verdacht haben, dass ein Eindringling sich an Ihrem System zu schaffen gemacht hat, hilft meist die Überprüfung der Log Dateien oder die Verwendung eines Testprogramms. Diese Programme suchen meistens nach so genannten Rootkits Nähere Informationen hierzu finden Sie unter http://de.wikipedia.org/wiki/Rootkit.

Als Überprüfungstools haben sich für Windows Blacklight (zu beziehen unter: http://www.f-secure.com/blacklight) und unter Linux checkrootkit (zu beziehen über: http://www.chkrootkit.org) bewährt.

Eine gut geführte Liste aktueller Sicherheitslücken finden Sie unter http://www.securityfocus.com/ unter dem Punkt Bugtraq. Sofern Sie allgemeine Informationen über Computersicherheit wünschen empfiehlt sich das BSI Grundschutzhandbuch das Sie kostenfrei unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html herunterladen können.

Eindeutige ID: #1164
Verfasser: Wolfram Heinen
Letzte Änderung: 2021-04-01 06:28