Sicherheit

Mein Server verschickt Spam, was kann ich dagegen machen?

1. Der Server ist gehackt – in diesem Fall hat der Versender Zugriff auf Ihren Server und kann die E-Mails direkt oder über ein Skript versenden lassen. Feststellen können Sie dieses ggf. über Tools wie **Chkrootkit**. Die einzige Möglichkeit wirklich sicher zu gehen das der Hacker kein Zugriff mehr auf Ihrem Server hat ist diesen Neu zu installieren. Zuvor sollten Sie die Passwörter zu Ihren Mail-Accounts ändern.
2. Der Mailserver arbeitet als offener Relay – in diesem Fall nimmt der Mailserver jede E-Mail ohne Authentifizierung an und versendet sie weiter. Da unsere Grundkonfiguration so angelegt ist das immer eine Authentifizierung benötigt wird, deutet dieses ebenfalls darauf hin, dass der Server gehackt worden ist oder das Sie die Konfiguration des Mailservers entsprechend geändert haben. Diese Sicherheitslücke lässt sich z.B über folgende Seite testen: http://www.mailradar.com/openrelay/
3. Der Versender verwendet Cross Site Skripting – in diesem Fall verwendet der Angreifer eine fehlerhaft programmierte Webseite / CMS auf Ihrem Server, über die er ein Skript ausführen kann. Cross Site Skripting ist über eine Verbindung der Logdateien des Mailservers und Webservers zu erkennen. In diesem Fall muss eine E-Mail vom Benutzer wwwrun bzw. www-data versandt worden sein und zur selben Zeit in der log Datei des Webservers ein Aufruf einer Webseite erfolgt sein. Über die Auswertung dieses Aufrufs kann sowohl das betreffende Skript auf dem Server als auch das nachgeladene Skript des Angreifers Identifiziert und die IP des aufrufenden Servers ermittelt werden.
   Weitergehende Informationen zum Cross Site Skripting http://de.wikipedia.org/wiki/XSS.
   Allgemeine Informationen zur Serversicherheit http://www.bsi.de.

Eindeutige ID: #1163
Verfasser: Wolfram Heinen
Letzte Änderung: 2021-04-01 06:25