Web-Server: Über meinen Server werden Spam's verschickt!

Problem:

Die Symptome sind immer die Selben: langsam füllt sich die Mailqueue, der eigene Mailversand wird immer langsamer, wenn man seine root-Mails ließt, erhält man massenweiße Bounces von Mails, die man nie verschickt hat.

Erklärung:

Ein Spammer nutzt den Server zum Spamversand.

Meistens steckt ein auf dem Server eingeschleustes (PHP-)Script oder ein vorhandenes, lückenhaftes Mailscript dahinter.

Was ist zu tun?

...ist meißt die erste Frage. Die Antwort klingt erstmal leicht:

1. Mailserver abschalten.

2. Fehlerhaftes Script finden und entfernen.

3. Spammails aus der Queue entfernen.

Lösung zu 2.):

Da i.d.R. ein CGI-/PHP-Script dahinter steckt (egal ob eingeschleust oder ein Vorhandenes ausgenutzt) gibt es 2 mir sinnvolle/bekannte Möglichkeiten:

1. Möglichkeit:

Wir suchen im maillog nach dem Beginn einer solchen Spam-Welle und vergleichen die Zeiteinträge in den (vielen vielen) `access_log`-Dateien nach passenden Einträgen.

2. Möglichkeit:

Wir gestallten die `mail`-Routine so um, daß aus den verschickten Mails das Script erkennbar wird.

Wir erstellen einen `sendmail-wrapper` welches erstens einen extra Header in die Email schreibt und zweitens ein Logfile in `/tmp/` erstellt.

```
#!/bin/sh
TODAY=`date -Iseconds`
echo $TODAY sendmail-wrapper called $USER from $PWD ››/tmp/mail.send
(echo X-Additional-Header: $(dirname $PWD);cat) | /usr/lib/sendmail-real "$@"
```

Anmerkung: Im Header setzten wir ganz bewust einen `dirname` ein weil sonst evtl. interne Geheimnisse aus geplaudert werden könnten.)

Danach muß der Wrapper noch in die Abarbeitung eingeführt werden:

```
chmod +x sendmail-wrapper
mv /usr/lib/sendmail /usr/lib/sendmail-real
mv sendmail-wrapper /usr/lib/sendmail
```

Was tun, wenn sich nix tut?

Ob es funktioniert ist leicht mit einem kleine PHP-Script, welches ein Email verschickt zu überprüfen. Falls das Logfile nicht geschrieben wird, einfach mal prüfen, ob PHP überhaupt Sendmail nutzt und welcher `sendmail_path` in `phpinfo()` angezeigt wird. Ggf. kommen auch andere Pfade in Frage. Dann handelt man damit einfach analog zu oben.

Warum reicht das?

a) Weil die meisten Installationen von PHP oder CGI-Scripten `sendmail` nutzten.

b) Weil auch bei ausgeschalteten Mailserver das Logfile geschrieben wird.

Wie mach ich das Rückgängig?

einfach die `sendmail-real` wieder statt den Wrapper einsetzen:

```
mv /usr/lib/sendmail-real /usr/lib/sendmail
```

Was kann man noch tun?

Grundsätzlich sollte man hin und wieder mal testen, ob man nicht einen offenen Relay-Server unterhält.

Eindeutige ID: #1215
huschi

Web-Server: Über meinen Server werden Spam's verschickt!

2007-08-12 11:01