



## Angriff der Mail-Bürokratie

[14.04.2004 17:57]

Viele große E-Mail-Server lassen sich für eine neuartige Art von Denial-of-Service-Angriffen missbrauchen, bei denen das Opfer mit Nachrichten über fehlgeschlagene Zustellungsversuche überflutet wird. Sie beruhen auf der Tatsache, dass viele Server auf eine Mail mit vielen ungültigen Adressen jeweils einzelne Fehlermeldungen versenden.

Eine Untersuchung von über 12000 zufällig ausgewählten Mail-Servern hat ergeben, dass sich circa 5 Prozent aller Mail-Server derart missbrauchen lässt. Diese Server akzeptieren alle Mails für ihren Domainnamen, haben keine erkennbare Obergrenze der Empfängeranzahl pro Mail und generieren pro ungültigen Empfänger eine Fehler-Mail inklusive Kopie des Originals mit allen Attachments. Bei größeren Organisationen sieht das Verhältnis noch schlechter aus. So lassen sich sehr viele Mailserver namhafter staatlicher Behörden im In- und Ausland sowie circa 30 Prozent der Fortune-500-Firmen für solche Attacken missbrauchen.

In einem Experiment wurde an 105 Server je eine Mail mit 1000 ungültigen Adressen und einem 10-KByte-Attachment verschickt. Das Gesamtvolumen des Versands betrug 3,6 MByte. Innerhalb weniger Stunden generierten diese Server über 80.000 Mails mit einem Gesamtvolumen von über 1,2 GByte. Die Absenderadresse der ursprünglichen Mail war gefälscht, die 80.000 Antworten hätten damit einen beliebigen Anwender treffen können.

In einem Artikel auf **heise Security**[1] beschreibt der Autor der Studie, Stefan Frei, die Ursachen des Problems und wie es sich beseitigen lässt:

- **Angriff via Mail -- Mail-Server als Verstärker für DoS-Angriffe**[2]

(ju[3]/c't)

### URL dieses Artikels:

<http://www.heise.de/security/news/meldung/46514>

### Links in diesem Artikel:

[1] <http://www.heise.de/security>

[2] <http://www.heise.de/security/artikel/46496>

[3] <mailto:ju@ct.heise.de>