



Was bedeutet „Backscatter“ und warum ist das so gefährlich?

Backscatter beschreibt die Eigenschaft eines Mailserver, bei eingehenden E-Mails den Absender zu überprüfen. Dies geschieht dadurch, dass der Mailserver versucht, eine E-Mail ohne Absenderangabe an die Absenderadresse der eingehenden E-Mail zu senden. Wird die leere E-Mail angenommen, gilt die Adresse als erfolgreich geprüft. Die empfangenden Mailserver versuchen durch diese Technik, sinnlose Absenderangaben zu filtern.

Für echte E-Mails ist diese Vorgehensweise prinzipiell kein großes Problem.

Allerdings öffnet eine solche Verhaltensweise der Mailserver eine große **Sicherheitslücke**, die sog. **DOS-Angriffe** ermöglicht und in der Vergangenheit auch mehrfach zu Abstürzen in Rechenzentren geführt hat.

Hierbei werden unzählige (teilweise mehrere Millionen) E-Mails mit einer bestimmten Absenderangabe gezielt an Mailserver verschickt, die für **Backscatter** bekannt sind.

Beispielhaft verwenden wir hier die E-Mail-Adresse Test@Spam-Sperre.de.

Nehmen wir an, ein Hacker hat nun ein **Botnetz** aufgebaut und veranlasst 100.000 Computer dazu, jeweils 1.000 E-Mails mit der Absenderadresse

Test@Spam-Sperre.de an backscatternde Mailserver zu verschicken.

Diese versuchen nun alle, die eingehenden E-Mails zu prüfen und senden pro E-Mail eine Anfrage an den Mailserver hinter Spam-Sperre.de.

100.000 Computer x 1.000 Mails = 100.000.000 Anfragen

Was passiert? Der Mailserver der Domain Spam-Sperre.de wird mit der Flut der (nahezu zeitgleichen) Anfragen überfordert sein und seinen **Dienst verweigern**.

Aufgrund der Tatsache, dass nicht zustellbare E-Mails 7 Tage lang gespeichert werden und während dieser Zeit im 5-Minuten-Takt ein erneuter Zustellversuch unternommen wird, fällt der angegriffene Mailserver **mindestens für eine Woche aus**.

Ein solcher Angriff ist technisch absolut kein Problem und der Administrator der Domain Spam-Sperre.de kann letztendlich nichts gegen die Flut der Anfragen unternehmen.

Spam-Sperre.de erkennt Anfragen, die durch Backscattern entstehen und unterbindet diese Technik, da sie zum einen **missbräuchlich** ist und zum anderen eine **Sicherheitslücke** entstehen lässt, deren Ausmaß sich nicht abschätzen lässt.

Wenn auch Sie Ihr Unternehmen gegen solche Angriffe absichern möchten, lautet unsere Empfehlung:

