

## Spam-Flut

# Wirksamer Schutz vor elektronischer Belästigung

Jeder, der per E-Mail kommuniziert, kennt das Problem: Auf jede erwünschte Nachricht kommen mit Sicherheit drei bis vier Spam-Mails. Statistiken zufolge werden täglich bis zu 180 Milliarden davon verschickt. Das entspricht etwa 86 Prozent des gesamten globalen E-Mail-Volumens.

**D**och die Zahlen sagen noch mehr aus: Im Umkehrschluss ergibt sich, dass maximal 14 Prozent aller E-Mails erwünscht sind; bei einer detaillierten Betrachtung sinkt dieser Anteil sogar auf bis zu 1,6 Prozent der ankommenden E-Mails. Mittlerweile bietet daher jeder *Provider* einen gewissen Grundschutz vor *Spam*. Fast alle arbeiten dazu mit einer so genannten Text-Muster-Erkennung, bei der anhand bestimmter Kriterien in einer E-Mail die Wahrscheinlichkeit ermittelt wird, mit der diese als *Spam* einzustufen ist. Nicht nur die dazu benötigte enorme Rechenzeit gestaltet dieses jedoch schwierig. Die *Provider* sind dazu verpflichtet, jede zunächst angenommene E-Mail an den Empfänger zuzustellen. Das bedeutet: auch für als *Spam* erkannte E-Mails muss eine Zustellung erfolgen. Daher empfiehlt es sich, bereits vor der Annahme einer E-Mail zu prüfen, ob es sich um *Spam* handelt.

## Methode Blacklisting

Um das zu ermöglichen, sind jedoch andere Bewertungskriterien heranzuziehen, da zu diesem Zeitpunkt der Inhalt der E-Mail nicht

bekannt ist. Viele *Provider* nutzen zusätzlich *Blacklisting* als eine Maßnahme gegen *Spam*. Hierfür werden durch *Spam*-Versand auffällig gewordene IP-Adressen in global verfügbare Liste aufgenommen, die jeder *Provider* zur Beurteilung von ankommenden E-Mails zu Rate ziehen kann. Wesentlicher Nachteil dabei ist allerdings, dass einige Zeit vergeht, bis eine durch *Spam*-Versand auffällig gewordene IP-Adresse auf einer *Blacklist* erscheint. Durch die Kombination von verschiedenen *Blacklists* lassen sich etwa 75 Prozent der *Spam*-Mails vor der Annahme ablehnen. Dazu kommt: fast 36 Prozent der IP-Adressen versenden nur bis zu 30 Minuten lang *Spam*. Meist ist diese Zeit zu kurz, um rechtzeitig einen *Blacklist*-Eintrag für diese IP-Adresse zu generieren.

## Methode Spam-Score

Für einen besseren *Spam*-Schutz besteht die Möglichkeit, sich bei eingehenden E-Mails für jede IP-Adresse, die eine E-Mail zugestellt hat, den *Spam-Score*, also die Wahrscheinlichkeit, mit der eine E-Mail als *Spam* einzustufen ist, zu merken. Wird ein bestimmter Schwellenwert

mehrfach überschritten, ist die IP-Adresse für einen kurzen Zeitraum gesperrt. Fällt die IP-Adresse nach dieser Sperre erneut negativ auf, verlängert sich die Sperrdauer mit der Anzahl der Verstöße, wobei die maximale Sperrdauer 24 Stunden niemals überschreitet. Positive Bewertungen einer IP-Adresse haben zur Folge, dass eine einmalige Überschreitung des Schwellenwertes nicht gleich zu einer Sperrung führt.

## Methode externer Service

Selber eine Anti-*Spam*-Lösung zu implementieren, ist in der Regel mit großem Aufwand verbunden. Die größere Herausforderung besteht jedoch darin, diese Lösung permanent zu pflegen und weiterzuentwickeln. Einige Hersteller bieten Anti-*Spam*-Lösungen als sogenannte *Appliances* an – *Hardware*-Lösungen, die vor die Mail-Systeme gestellt werden. Diese Lösungen bieten starre und lediglich durch *Updates* aktualisierbare Mechanismen gegen *Spam*. Dienstleister, die eine Anti-*Spam*-Lösung als Service anbieten, können einen besseren Schutz vor *Spam* gewährleisten. Durch die Masse an E-Mails, beziehungsweise an *Spam*, die täglich bei ihnen verarbeitet wird, ist eine wesentlich höhere Erkennungsrate zu erzielen. Zudem erfolgt eine permanente Überwachung der Anti-*Spam*-Maßnahmen, um diese stets den aktuellen Gegebenheiten anzupassen. Es ist somit ratsam, bei der Wahl des Internet-*Providers* auf die angebotenen Anti-*Spam*-Dienstleistungen zu achten. ▲

Der Autor Sebastian Ganschow ist als Network & System Engineer bei der Dr. Bülow & Masiak GmbH tätig.

Dr. Bülow & Masiak GmbH  
Professional Network Solutions  
Victoriastraße 119, 45770 Marl  
Tel.: 02365/41 46 0  
info@buelow-masiak.de  
s.ganschow@buelow-masiak.de  
www.buelow-masiak.de



Sebastian Ganschow, B.Sc., bei der Überwachung von Kundenservern und der Systemdiagnose