

Mail-Server: Greylisting: Vor- und Nachteile

Was ist Greylisting?

Greylisting (oder auch manchmal "Graylisting") ist ein Zwischending zwischen Black- und Whitelisting.

Während Blacklists eingesetzt werden um Emails vollständig zu blocken und Whitelists um Emails (ungeprüft) durch zu lassen, bildet Greylisting die Mitte:

Der erste Kontakt wird geblockt und erst der Zweite kommt rein.

Um die Funktion und den sinnvollen Einsatz zu verstehen braucht es einiges an Kenntnis:

Fragen und Antworten:

Wie funktioniert Greylisting?

Greylisting merkt sich ein Trippel aus den Eingangsdaten:

1. IP-Adresse des einliefernden Mail-Servers
2. Sender-Email-Adresse
3. Empfänger-Email-Adresse

Beim ersten Kontakt merkt sich Greylisting dieses Trippel aber meldet dem einliefernden Mailserver einen [Temporary not available](#). Jeder richtige Mailserver erkennt diesen Fehlercode und versucht es nach einiger Zeit noch einmal.

Sobald dieser Server es nochmal versucht, erscheint dieses Trippel ein zweites Mal im Greylisting. Dadurch weiß die Software nun, daß es sich hierbei um einen realen Mailserver handelt. Meistens wird dieses Trippel dann auch für einige Zeit (z.B. 1 Monat) auf eine Whitelist gesetzt, so daß der weiterer Emailverkehr nicht behindert wird.

Warum funktioniert Greylisting?

Greylisting blockt deshalb so viele Spam-Emails, weil viele Spam-Programme einfach nur die Daten raushauen ohne auf Fehlermeldungen Rücksicht zu nehmen. Insbesondere versuchen Sie es nur in seltenen Fällen ein zweites Mal mit dem selben Trippel. Denn Spam-Versand ist inzwischen in vielen Ländern eine Straftat. D.h. der Spammer muß sich ständig verstecken und wechselt daher regelmäßig die IP und nutzt überwiegend gefaked/zufällige Absender-Adressen.

Daher ist diese Methode deutlich effektiver und auch Ressourcen sparender als z.B. ein SpamAssassin und/oder RBL-Blocking.

Mail-Server: Greylisting: Vor- und Nachteile

Welche Software steckt hinter Greylisting?

Da Greylisting direkt in den SMTP-Server eingreifen muß ist dies meist nur über Umwege zu erreichen:

- Bei Postfix wird dies über [Postgrey](#) erreicht.
- Für Sendmail gibt es einen Greylist-Milter.
- Und bei Qmail muß man es selber [einkompilieren](#).

Welche Nachteile hat Greylisting?

Der größte Nachteil ist der Zeitverzug beim "Erstkontakt". Dies trifft vor allem neue Geschäftsbeziehungen im Business-Bereich.

Viele Internet-Nutzer denken auch immer gleich, daß dann wichtige Emails nicht mehr durchkommen.

Dies ist definitiv nicht der Fall!

Denn die wichtigen (und eben auch realen) Emails werden immer über Email-Server verschickt. Dieser versucht grundsätzlich die Email über einen längeren Zeitraum zu verschicken.

Manche unbedarfte Benutzer haben Angst, daß deren Kontakte die Email ein zweites Mal schicken müssen.

Nein, das übernimmt der Email-Server!

Für Webhoster und Server-Admin's ist hier häufig Überzeugungsarbeit zu leisten. Ein paar Argumente:

- "Alle Emails kommen an. Nur die Erste braucht geringfügig länger."
- "Es betrifft nur den Erstkontakt!"
- "Ihre Kontakt-/Bestell-Formulare auf der Website sind davon nicht betroffen."
- "Ihre verschickten Emails sind davon nicht betroffen!"
- "Lesen Sie den Artikel bei Wikipedia!"
- "Dafür sparen Sie sich locker 100 Spams am Tag."

Mail-Server: Greylisting: Vor- und Nachteile

Überzeugen kann häufig auch eine kurze Statistik oder die Installation des Plesk-Greylist-Control-Panel.

Warum kommen immer noch Spam-Mails an?

Hier ist der Einzelfall zu unterscheiden:

Meistens sind es Emails, die über einen realen Email-Server kommen. Dies kann verschiedene Gründe haben. Aber meistens den, daß dieser Server nicht mehr 100%ig unter der Kontrolle des Administrators steht.

Zum Anderen gibt es den Mechanismus der MX-Server. D.h. zu einer Domain kann man mehrere Email-Server definieren. Wenn dann nur auf einem Greylisting läuft, wird der nächste genommen der diese Email evtl. direkt annimmt.

Weitere Links:

- [Plesk/Qmail: Spamprotection mit Greylisting](#)
- [Debian/Postfix: Greylisting mit Postgrey](#)
- [SuSE/Postfix: Greylisting mit Postgrey](#)
- [Plesk & Qmail: Greylisting mit spamdyke](#)
- Artikel bei Wikipedia: [Greylisting](#)
- Finde alle Artikel zum Thema "[Greylisting](#)".

Eindeutige ID: #1272

huschi

2007-11-13 12:38