

# Schutz vor Spam an der FH Nürnberg Greylisting

University of Applied Sciences



Franziska Städtler, Felizitas Heinebrodt

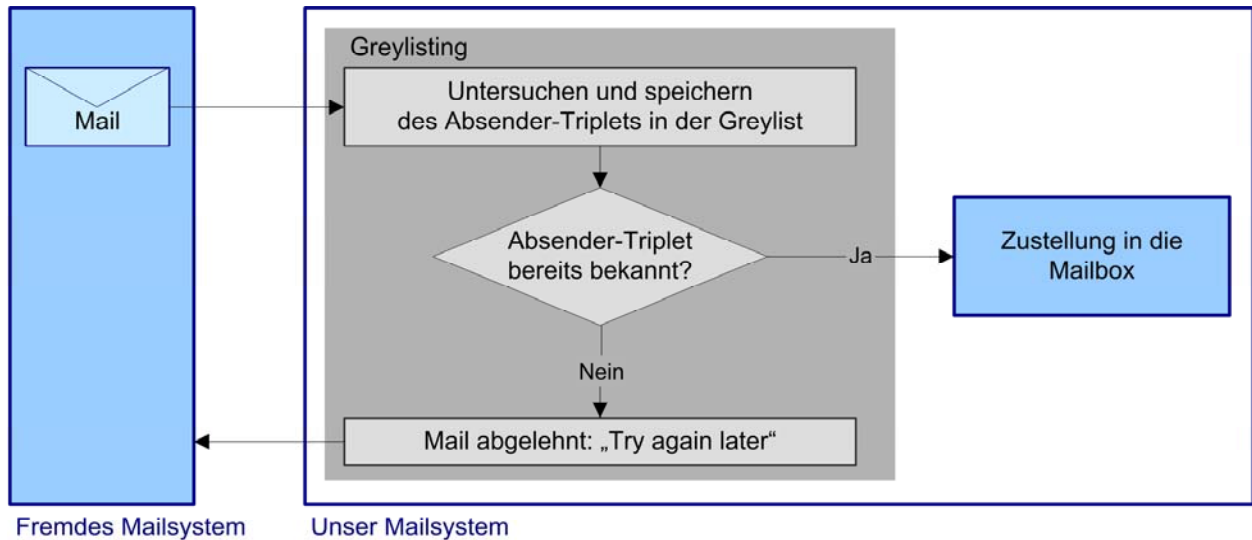
Georg-Simon-Ohm-Fachhochschule Nürnberg  
Rechenzentrum  
Kesslerplatz 12, 90489 Nürnberg

Version 1  
Juli 2005

Informationen des Rechenzentrums der Georg-Simon-Ohm-Fachhochschule Nürnberg



# Schutz vor Spam: Greylisting



Im Jahr 2004 waren bis zu 90% der Mails, die an der Fachhochschule eingingen, Spam, d.h. unverlangte Werbe-Mails. Zum Schutz vor Spam ist seit Juni 2005 im Mailsystem der Fachhochschule Greylisting im Einsatz.

## 1 Funktionsweise

Das Mailsystem führt Listen:  
 Auf einer **Whitelist** werden vertrauenswürdige Mailserver geführt. Mails von diesen Adressen werden zugestellt ohne die Spam-Filterung zu durchlaufen.  
 Eine **Blacklist**, d.h. eine Liste mit Email-Adressen, von denen nichts angenommen wird, gibt es an unserer Hochschule nicht.  
 Wenn eine Email eingeht von einem Absender, der nicht auf der Whitelist steht, dann wird diese Adresse auf die **Greylist** gesetzt. Diese Greylist ist die zentrale Komponente unseres Spam-Schutzes, der deswegen Greylisting genannt wird.

*Anmerkung: Bei Mails innerhalb der Hochschule kommt Greylisting nicht zum Einsatz.*

### 1.1 Greylisting

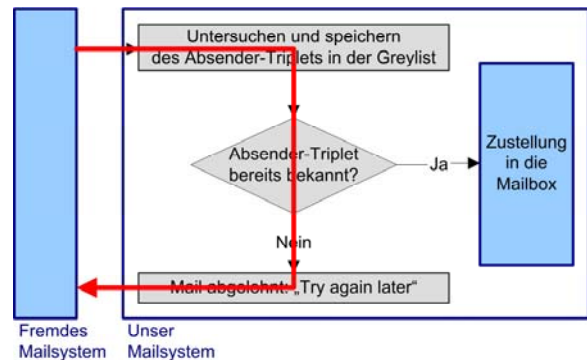
Bei jeder Mail, die an der Hochschule eingeht und deren Absender nicht in der Whitelist steht, wird das so genannte Absender-Triplet festgestellt:

- die IP-Adresse des Mailservers, von dem die Mail abgeschickt wurde
- die Absenderadresse
- die Empfängeradresse

Das Mailsystem merkt sich das Triplet in der Greylist und kann so jede Mail eindeutig identifizieren.

#### 1. Zustellversuch:

Greylisting arbeitet nach folgender Grundregel: „Wenn ich das Triplet einer eingehenden Mail noch nie gesehen habe, dann verweigere ich die Zustellung und sage dem Mailserver, von dem die Mail kam, er soll es später noch mal versuchen.“



Die Mail wird nicht angenommen.

*Dieses Verhalten ist standardkonform. Der Standard fordert, dass Mailsysteme den Zustellungsversuch nach einiger Zeit wiederholen.*

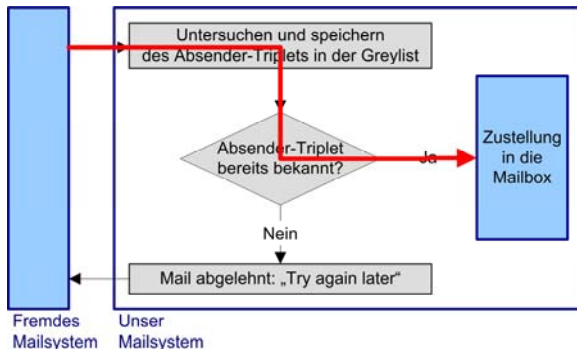
#### Reaktion des fremden Mailsystems:

Ein anständiger, korrekt konfigurierter Mailserver steckt daraufhin die Mail in eine Warteschlange und versucht es automatisch später ( je nach Konfiguration zwischen 30 und 60 Minuten) noch einmal, die Mail an unser Mailsystem zu schicken. Der Absender merkt davon nichts.

Unseriöse Mailserver (Spammer) verfügen üblicherweise über keine Warteschlangenverarbeitung. Deswegen können sie den Zustellversuch nicht wiederholen. Ihre Spam-Mail wird nicht zugestellt.

## 2. Zustellversuch:

Kommt die Mail das zweite Mal, ist ihr Triplet bekannt (weil es bereits in der Greylist steht) und die Mail wird an die angegebene Adresse zugestellt.



## 1.2 Auto-Whitelisting

Beim ersten Zustellversuch wird die Mail zurück zum Absender geschickt mit dem Hinweis „Try again later“. Ihr Triplet wird in die Greylist eingetragen.

Kommt die Mail zum zweiten Mal, wird sie zugestellt. Ihr Triplet wird dann für 24 Stunden in eine so genannte Auto-Whitelist eingetragen, sodass alle folgenden Mails mit dem Triplet (d.h. mit der selben Absender- und Empfängeradresse) ohne Verzögerung durchgehen.

Dabei verlängert sich die Zeit, die die Triplets in der Auto-Whitelist bleiben bei jeder weiteren Zustellung auf wieder 24 Stunden.

## 2 Vorteile

Greylisting hat gegenüber der bisherigen Spam-Filterung den Vorteil, dass keine Mails mehr verloren gehen können.

Schlimmstenfalls - wenn der Mailserver des Absenders nicht standardkonform konfiguriert ist und die wiederholte Zustellung nicht kann - bekommt der Absender die Meldung, dass die Mail nicht zugestellt werden konnte.

## 3 Nachteile

Es kommt zu einer Verzögerung im Mailverkehr, da beim ersten Zustellversuch die Mail nicht angenommen, sondern zurückgeschickt wird. Die Dauer der Verzögerung hängt davon ab, wie lange der Mailserver des Absenders mit der Wiederholung des Zustellversuchs wartet.

Allerdings kommt es durch das Auto-Whitelisting nur bei der ersten Mail eines Absenders innerhalb von 24 Stunden zu der genannten Verzögerung.

## 4 Referenzen

Viele Mailbetreiber schützen sich mittlerweile durch Greylisting vor der Spam-Flut.

### Hochschulen:

Uni Bayreuth, Uni/FH Würzburg, FH Augsburg, RWTH Aachen, IU Bremen, Uni Freiburg, TU Chemnitz, HDM Stuttgart, FHT Esslingen, Uni Köln, Leibniz Rechenzentrum München, Tusur.ru

### Institutionen:

Auswärtiges Amt (auswaertiges-amt.de), Bundeszentrale für politische Bildung (bpb.de), Bundesanstalt für Landwirtschaft und Ernährung (ble.de), Das Portal des Bundes (bund.de), Tomsk.gov.ru

### Firmen:

Epson, ASQF, msg Systeme GmbH, Javamagazin, Commerzbank, Ev. Landeskirche Baden, Datev, JCIDesign, Framatome-ANP, Maxalution, CoreOptics, meer.net, zaz.com.br, liu.se

## 5 Was Sie tun können

Um bereits im Vorfeld zu verhindern, dass Sie Spam bekommen: Seien Sie sparsam mit der Verbreitung Ihrer Email-Adresse. Füllen Sie nicht jedes Formular aus, das Sie im Internet finden!

Wenn doch eine Mail in Ihrer Mailbox landet, löschen Sie die Mail umgehend. Öffnen Sie auf keinen Fall an die Mail angehängte Dateien. Hier handelt es sich meist um Viren. Und beantworten Sie solche Mails nicht – auch dann nicht, wenn Ihnen angeblich angeboten wird, Ihre Adresse würde dann vom Verteiler gestrichen! Die meisten Spammer nutzen Ihre Antwort zur Verifizierung Ihrer Adresse („Jipieh, die Adresse gibt es wirklich! Da schicke ich gleich noch mehr Werbung hin.“).

Spam ist eine billige Möglichkeit, Werbung zu verschicken und lohnt sich für den Spammer bereits bei einer Antwort auf 10.000 E-Mails. Sorgen Sie dafür, dass es sich trotzdem nicht lohnt: Kaufen Sie nichts aufgrund einer Spam-Mail!