Greylisting

Das Rechenzentrum setzt auf den zentralen Mail-Gateways, die für den gesamten Mail-Verkehr der TU Clausthal zuständig sind, das sogenannte Greylisting zur Abwehr von Spam ein.

Was ist Greylisting?

Das Greylisting ist eine weitere Abwehrmaßnahme gegen Spam. Das Greylisting nutzt aus, dass bei gewöhnlichem Spam nur einmal versucht wird, die Spam E-Mails an einen Mail-Server zu schicken. Grundlage für das Greylisting ist hierbei, dass einem Mail-Server die folgenden drei Informationen bekannt sind, bevor er eine E-Mail annimmt:

- Absenderadresse der E-Mail
- Empfängeradresse der E-Mail
- IP-Adresse des Mail-Servers

Diese Informationen werden nun beim ersten Zustellversuch einer E-Mail in einer Datenbank gespeichert und die Annahme der E-Mail wird dann zunächst erst einmal verweigert. Dies ist im Rahmen des SMTP-Protokolls (RFC 821) möglich und bedeutet nichts anderes, als dass die Annahme der E-Mail vorrübergehend nicht möglich ist und dass es zu einem späteren Zeitpunkt noch einmal versucht werden soll. Ein richtig konfigurierter Mail-Server unternimmt dann nach einer gewissen Zeit einen zweiten Zustellversuch, bei dem die E-Mail dann auf Grund der in der Datenbank gespeicherten Daten auch angenommen wird.

Gültigkeit von Datenbank-Einträgen beim Greylisting:

Die in der Datenbank gespeicherten Triplets aus Empfänger- und Absenderadresse sowie IP-Adresse des versendenden Mail-Servers werden für zunächst zwei Tage in der Datenbank behalten, kommt in dieser Zeit ein zweiter Zustellversuch vor, so wird die Gültigkeit des Datenbank-Eintrags auf 35 Tage verlängert. Bei jeder neuen Zustellung wird die Gültigkeit eines Triplets wiederum auf 35 Tage verlängert.

Warum Greylisting?

Durch das Greylisting wird Spam sehr zuverlässig abgeblockt und auch Würmer und Trojaner können mittels Greylisting erfolgreich bekämpft werden. So werden per Greylisting beispielsweise jene Viren abgeblockt, für die es noch keine Virendefinitionen für den Viren-Scanner gibt. Beim Greylisting gehen keine E-Mails verloren!

Der einzige Nachteil des Greylistings liegt in der einmaligen Verzögerung beim Empfangen von E-Mails. Des Weiteren kann man die Dauer bis zum zweiten Zustellversuch nicht beeinflussen, erfahrungsgemäß liegt diese Zeit aber zwischen 5 Minuten und einer Stunde.