TU Clausthal

Rundschreiben des Rechenzentrums

Erzstraße 51
D-38678 Clausthal-Zellerfeld
Tel.: 05323/72-2045

Alle Fakultäten und wissenschaftliche Einrichtungen
Zentrale Einrichtungen,
Präsidialbüro
Verwaltung
Personalrat
Gleichstellungsbüro

h i e r

05.07.2005

Spam-Bekämpfung via Greylisting

Sehr geehrte Damen und Herren,
das E-Mail-Aufkommen der TU Clausthal ist auch im vergangenen Jahr immer weiter gestiegen, Ursachen dafür sind neben Mail-Viren und –Würmern auch das vermehrte Aufkommen von Spam. Spam stellt etwa 90% aller an die TU Clausthal gesendeten E-Mails dar und ist damit eine sehr hohe Belastung für die Mail-Server und die Benutzer-Mailboxen der Hochschule. Das Rechenzentrum geht mit der zentralen Spam-Quarantäne durch das kommerzielle Produkt PureMessage von der Firma Sophos gegen das Spam-Aufkommen vor. Leider reicht das allein aber nicht mehr aus, um den Dienst E-Mail zuverlässig betreiben zu können. Immer wieder kommt es bei Spam-Attacken zu Staus auf den zentralen Mail-Gateways des Rechenzentrums, so dass E-Mails manchmal viele Stunden benötigen, bis sie beim Empfänger ankommen. Um solche Vorfälle zu verhindern, wollen wir weitere Schutzmaßnahmen gegen Spam ergreifen um den Dienst "E-Mail" weiterhin als zuverlässigen und schnellen Kommunikationsweg anzubieten.

Viele Hochschulen setzen neben einer Spam-Erkennungssoftware das Greylisting ein, mit dem der größte Teil des Spam schon vor der eigentlichen Spam-Erkennung und –Filterung heraus gefiltert wird. Greylisting nutzt die Eigenschaft der Spam-Versender aus, dass sie die E-Mails nach dem Motto "fire and forget" verschicken, das heißt der Versender von Spam macht sich keine Gedanken darüber, ob die Spams beim Empfänger angekommen sind oder nicht. Diese Tatsache lässt sich durch die Standards des SMTP-Protokolls, welches auf Mail-Servern zum Versenden und Empfangen von E-Mails eingesetzt wird, ausnutzen. Bei der Zustellung von E-Mails an die TU Clausthal werden den zentralen Mail-Gateways des RZ die folgenden drei Informationen mitgeteilt, bevor eine E-Mail angenommen wird:
* Absenderadresse der E-Mail
* Empfängeradresse der E-Mail

* IP-Adresse des Mail-Servers, der versucht eine E-Mail an die TU Clausthal zu senden.

Diese drei Informationen werden beim ersten Versuch der Zustellung einer E-Mail in einer Datenbank gespeichert, zusätzlich wird die Annahme der E-Mail zunächst verweigert. Spam wird in der Regel damit abgewehrt, da davon auszugehen ist, dass ein weiterer Zustellversuch nicht erfolgt. „Richtige E-Mails", die von sauber konfigurierten und damit RFC-konform arbeitenden Mail-Servern verschickt werden, erfolgt in der Regel nach 5 bis 60 Minuten ein zweiter Zustellversuch, da die Daten nun bekannt sind, wird die E-Mail angenommen und dem Empfänger zugestellt. Alle weiteren E-Mails von diesem Absender werden dann wieder ganz normal behandelt, also ohne Verzögerung ausgeliefert. Laut RFC 821 ist das einmalige Ablehnen einer E-Mail durchaus statthaft und somit legal!

Durch das Greylisting wird aber nicht nur Spam, sondern auch eine Vielzahl von Viren und Würmern abgeblockt, die sich per E-Mail verbreiten. So wehrt das Greylisting jene Viren und Würmer ab, die vom Virenscanner nicht gefunden werden können, weil es noch keine Virendefinitionen (Updates) für den Virenscanner gibt.

Das Greylisting wird am 11.07.2005 auf den zentralen Mail-Gateways des RZ aktiviert. Es betrifft nur E-Mails von externen Mail-Servern, E-Mails die innerhalb des Hochschulnetzes verschickt werden, sind vom Greylisting nicht betroffen. Das Greylisting wird inzwischen an vielen deutschen Hochschulen eingesetzt und wir gehen davon aus, dass damit auch an der TU Clausthal die Sicherheit und die Qualität des E-Mail-Dienstes weiter gesteigert wird. Bei Problemen, von denen Sie glauben, dass sie mit dem Greylisting zusammenhängen könnten, wenden Sie sich bitte umgehend an uns.

Mit freundlichen Grüßen,
gez. Frank Ebeling <ebeling@rz.tu-clausthal.de>
Oliver Koch <koch@rz.tu-clausthal.de>