Protokoll-, Adressen-, Mail-Überprüfungen

- Protokoll-, Adressen-, Mail-Überprüfungen
- Empfänger-Validierung (User valid check)
- Abuse in diversen Varianten
- Nichtqualifizierte Header-Adressen
- HELO-String Überprüfung
- Pregreeting Protokollverletzung
- Ungültige Absender-MX Verweise

Empfänger-Validierung (User valid check)

Die Verwendung von TU Wien Mailadressen durch Spam-Mail-Versender hat zur Folge, dass durch nicht zustellbare Spam-Mails von allen Orten des Internets Mailerdaemon-Mails über die TU Wien hereinbrechen, ohne dass je ein TU Rechner an der eigentlichen Spam-Versendung beteiligt gewesen wäre.
Eine der möglichen Maßnahmen besteht derzeit darin, im Anlassfall die hier auftretenden Fantasie-Empfängeradressen (bestimmte oder nach einem gewissen Muster) unmittelbar am Bastionsrechner zu sperren. Normalerweise geschieht das in Absprache mit der EDV-verantwortlichen Person der betroffenen Subdomain. Im Extremfall können die Maßnahmen unmittelbar umgesetzt werden, wobei erst im Zuge dieses Schrittes die EDV-verantwortlichen Personen benachrichtigt werden.

Zusätzlich ist auf der Mailbastion eine **Empfänger-Validierung** (**User valid check**) implementiert, die im Anlassfall für gewisse Subdomains bzw. Hosts der tuwien.ac.at aktiviert wird. Das System basiert auf während des Mailempfangs durchgeführte SMTP-Abfragen beim Zielmailserver am TUNET, mit dem Zweck, die Gültigkeit der Empfängeradresse zu überprüfen (ohne dass tatsächlich noch der Mailtransport stattfindet).

Hinweise für Mail-Administratoren: Die Empfänger-Validierung ist in den Logfiles der Zielmailserver an folgenden Parametern erkennbar (was mitunter bei Unkenntnis Verwirrung hervorrufen könnte):

1. Der "HELO"-String lautet auf "user-check"
2. Die Absender-Adresse (Envelope-From, "MAIL FROM") lautet "<user-valid-test@tuwien.ac.at>"
3. Es wird immer nur genau ein Empfänger überprüft.

Dieses Verfahren erlaubt es bereits auf der Mailbastion, nicht existierende Empfänger oder vorläufig nicht erreichbare Server (in Wartung/ausgefallen) dem TU-externen Mailserver unmittelbar rückzumelden, sodass die Nachrichten nicht als Bounce-Mails die Mailqueue der Mailbastion durchlaufen müssen. Dies führt wiederum zu einer wesentlichen Entlastung der Mailbastion und einer effektiveren Weiterleitung.

Abuse in diversen Varianten

In Situationen, wo im umfangreichen Stil gefälschte bzw. nicht existende TU Wien Mailadressen als Empfänger aufscheinen, ist zur Vermeidung von übermäßigen Ressourcenbelastung (durch das zahlenmäßige Aufkommen, oder die Art der E-Mails, z.B. Mailbombs) eine vorübergehende Sperre des Absenders für die gesamt TU Wien vorgesehen. Die Sperren gehen dabei entweder von der Envelope- Adresse und/oder von der Mailserver-IP-Adresse aus.
Den aktuellen Status der Sperren erhält man aus Mailblockstatus. Dabei handelt es sich ausschließlich um Blockaden, die ausschließlich auf Reduzierung bzw. Vermeidung von Mailsystemressourcen vergenommen werden.

Nichtqualifizierte Header-Adressen

Nichtqualifizierte Header-Adressen des Absenders (From:-Zeile) werden für gewöhnlich von Mailservern, die die E-Mail

weiterleiten, korrigiert, d.h. es wird eine Qualifizierung vorgenommen, indem der volle Domainname des Mailservers ergänzt wird. Z.B. wird am Mailserver xyz.tuwien.ac.at

From: bad_spammer

zu

From: bad_spammer@xyz.tuwien.ac.at

Derartige zwar RFC-konforme, aber oftmals für die Empfänger irreführenden Manipulationen durch einen Mailserver kann man dadurch unterbinden, indem man die unqualifizierte Adresse durch eine entsprechende Pseudo-Qualifizierung markiert. Sofern eingesetzt, verwenden zentrale Server des ZID die Pseudo-Domain **FAKED-SENDER**. Damit wird

From: bad_spammer

zu

From: bad_spammer@FAKED-SENDER

umgeschrieben. Damit hat man die Möglichkeit, mit Hilfe von Mailfiltern derartige - typischerweise - Spam-Mails zu erkennen und entsprechend zu behandeln.

HELO-String Überprüfung

Mailserver, die sich bei der Übermittlung des SMTP HELO-Strings nicht an den RFC 2822 halten, werden permanent abgewiesen.
Typischerweise scheitern bei dieser Überprüfung sehr viele Spam-Quellen (aus Bot-Netzen operierende, zum SMTP-Proxies konvertierte "Zombie-PCs"), die oft nicht in der Lage sind, SMTP-konforme Mails in Umflauf zu bringen bzw. eher auf Geschwindigkeit als auf Einhaltung entsprechender RFCs getrimmt sind.

Dies betrifft allerdings nur E-Mails, die von außerhalb der TU Wien ankommen und über die Mailbastion bzw. die Incoming Mailrouter geleitet werden. Die Outgoing Mailrouter sind hier nicht so strikt, ebenso die Incoming Mailrouter, wenn eine E-Mail TU-internen Ursprungs ist.

Pregreeting Protokollverletzung

Bei der Protokollabwicklung eingehender SMTP-Verbindung, sollten absendende Server stets die Antworten des eingehenden Servers abwarten. Bei gewissen, Absenderadressbereichen des Internets wird eine künstlich verlängerte Antwortzeit (üblicherweise 5 Sekunden) hervorgerufen.
Ungeduldige Absender, wie typischerweise Spam-Quellen, deren Ziel es lediglich ist, möglichst schnell viele Spams in Umlauf zu bringen, scheitern hier, wenn sie in der Wartezeit ungefragt mit der SMTP-Konversation weiter machen (z.B. bereits die Absenderadresse "pre greeting" , also bevor der TU Mailserver seine Start- und Grußmeldung sendet, liefern).

Ungültige Absender-MX Verweise

Die Überprüfung des MX-Eintrages der Envelope-Absenderdomain kann auf nicht korrekte bzw. sinnvolle IP-Adressen verweisen. Typisch sind hier 127.0.0.1 (localhost) oder 192.168.x.x Adressen (private Adressen), weshalb somit an solche Absenderadressen etwaige Retourmails offensichtlich nicht mehr adressierbar sind. Derartige E-Mails werden gegebenenfalls permanent abgewiesen.