Viren- und Spamschutz beim Bürgernetz

Die Probleme bei E-Mail

Das Protokoll zum Versand von E-Mails – das „Simple Mail Transfer Protocol“, kurz: SMTP – enthält keine Authentifikation oder Echtheitsbestätigung, deswegen kann es leicht zum Versand von Viren und Werbung missbraucht werden. Aber leider gilt:

- Eine Änderung des Protokolls ist nicht einfach so möglich, ohne die Kompatibilität zu bestehenden Systemen (= Rest der Welt) zu verlieren.
- Mehr als jede dritte E-Mail bei uns ist unerwünscht. Tendenz steigend.
- Spammer passen sich an die Filter an.
- E-Mails sind „kritisch“ - es dürfen keinesfalls erwünschte E-Mails verloren gehen, ein Filter darf keine Fehler machen und wichtige E-Mails verschlucken.

Was prüft unser Mailserver

Um Spam und Missbrauch unseres Servers zu verhindern prüft unser Mailserver bestimmte Informationen:

- IP-Addresse des Absenders darf nicht auf einer „schwarzen Liste“ sein.
- Die Domain der Absenderaddresse muss existieren.
- Absenderaddressen – auch wenn diese nicht sehr aussagekräftig sind – werden gegen eine Filterliste geprüft (alle 2 Stunden aktualisiert).
- Empfängeraddressen müssen in unserem Zuständigkeitsbereich sein (also z.B. `@mucl.de`) oder der Absender muss sich vorher authentifiziert haben.

Effektiveres Nutzen

Mit folgenden Maßnahmen kann man E-Mail bei uns besser nutzen:

- Passwort-Authentifikation einschalten
- Vom Mailserver erkannten und markierten Spam („`SPAM:`“ im Betreff) in Ordner filtern – Siehe `http://service.drinsama.de/spam/`
- Zusätzlichen Spam-Filter verwenden (z.B. Mozilla Messenger ab 1.3 oder Apple Mail von OS X, der *individuell trainiert* wird und sich an die „persönlichen Mail-Mischung“ anpasst – und bei kontinuierlichem Training aktuell bleibt)
- Professionellen Virenschutz installieren und regelmäßig aktualisieren

Authentifizieren

Um sich am Mailserver zu authentifizieren – um so von einem beliebigen Provider aus E-Mails auch an nicht-mucl-Addressen versenden zu können – gibt es mehrere Möglichkeiten:

- Authentifikation mit Passwort einschalten („SMTP-AUTH“, meist muss dazu nur ein Häkchen im E-Mail-Programm gesetzt werden).
- Über das Bürgernetz einwählen (bekannte IP-Addresse).
- Erst Post abholen, dann versenden („SMTP-after-POP“, eher unzuverlässig).

Was nichts bringt:

Natürlich gibt es auch Maßnahmen, die nicht greifen:

- Antworten oder versuchen, sich abzumelden bei unseriösen Angeboten (bei Newslettern von seriösen Firmen ist das natürlich anders). Schlimmstenfalls bestätigt man so seine Addresse!
- Falsche „Benutzer nicht gefunden“ Mails verschicken (mailwasher) – der Absender ist praktisch immer falsch; die Addresslisten oft auf CD.
- Absenderaddressen „zuhause“ in Filterlisten aufnehmen – die selbe Addresse wird wahrscheinlich schon nicht mehr verwendet (oder ist die eines unschuldigen anderen Nutzers!).
- E-Mail-Addresse auf Webseiten verfälschen: die erwünschten Benutzer „leiden“ unter dieser Modifikation (für Firmen sowieso unmöglich - Teledienstgesetz).

Wichtige Addressen:

- Informationen zu unserem Werbefilter und der Konfiguration der Mailprogramme gibt es auf `http://service.drinsama.de/spam/`
- Informationen zu Kettenbriefen und anderen „Bitte weiterleiten“-Mails:
  (Bitte immer konsultieren, bevor man irgend so eine Mail weiterleitet!)
  `http://www.hoax-info.de/`
- Richtig Zitieren beim Antworten: `http://learn.to/quote`
- Fehler und Probleme von Outlook Express:
  `http://www.wschmidhuber.de/oeprob/`
- Mozilla auf Deutsch:
  `http://mozilla.kairo.at/`