

# Sichere Konfiguration von Mailclients

Günter Lau | Computer- und Medienservice, Systemsoftware und Kommunikation | laug@cms.hu-berlin.de

## Sicher bei der Nutzung

Sicherheit beginnt mit dem Wissen um die Unsicherheiten. Beim Medium E-Mail gehen nahezu alle beschreibenden Werte auf direkte Angaben und Einträge des Nutzers zurück. Damit sind die meisten Parameter der Kopfzeilen mit großer Vorsicht anzusehen. Nicht nur im Briefinhalt kann gelogen werden, auch mit dem „Umschlag“ wird geschwindelt. Es kann ja fast alles gefälscht sein. Seien Sie sich dieser Gefahr bewusst. Einen beträchtlichen Teil des Mailverkehrs nimmt die „unerwünschte“ Mail (Junk oder Spam) ein. Um sich die E-Mail-Bearbeitung nicht unnötig schwer zu machen, nutzen Sie die angebotenen Möglichkeiten, hier eine Vor-

persönliche Bewertung hin zu trainieren. Moderne Clients, wie Mozilla, Thunderbird und Opera, bieten hier Verfahren an, mit denen das Mailtool lernt, was Sie als Spam ansehen.

Der Prüfvorgang, wie er von den Posteingangsservern vorgenommen wird und dem die ankommende Mail unterworfen wird, liefert als Ergebnis zusätzliche Kopfzeilen (headerlines), die durch Filter ausgewertet werden können. Diese (zusätzlichen) auszuwertenden Zeilen heißen X-Spam-Level und X-Spam-Flag. Eine E-Mail wird als spamverdächtig gekennzeichnet, indem in der X-Spam-Level-Zeile eine Folge von neun \*-Zeichen eingesetzt wird und in der X-Spam-Flag-Zeile ein YES eingetragen wird.

```
(8.13.8/8.13.8) with ESMTP id m4TA1SGO023312 for <cortezka@cms.hu-berlin.de> Thu, 29 May 2008 12:01:29 +0200 (CEST)
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result: AvX/AFAbPkg+tzqO/2dsb2JhbAAMBgEBiA0TgT9lgTKBHkShR+IAIES
X-Spam-Level: *****
X-IronPort-AV: E=Sophos;i="4.27,561,1204498800"; d="scan'208,217";a="9465021"
X-Spam-Flag: YES
Received: from unknown (HELO [62.183.58.142]) ([62.183.58.142]) by ir2.cms.hu-berlin.de with ESMTP; 29 May 2008 12:01:22 +0200
```

Abb. 1: Diese Kopfzeilen werden hinzugefügt, wenn die zentrale Prüfung diese Mail als Spam einstuft.

sortierung vorzunehmen, um die Spreu vom Weizen zu trennen. Wenn Ihnen dann noch klar ist, dass diese Trennung nicht absolut sein kann, aber an einer Verbesserung der Trefferwahrscheinlichkeit ständig gearbeitet wird, haben Sie das rechte Bewusstsein für den Umgang mit SPAM. Zwei einander ergänzende Verfahren können hier genutzt werden. Das Reagieren auf die Spam-Bewertung, die durch unsere Posteingangsserver vorgenommen wird, gewissermaßen die allgemeine, zentrale Kontrolle, und die Möglichkeit, Ihren Mailclient auf Ihre eigene,

Bei der Filterdefinition im Mailclient muss die benutzte Zeile, also X-Spam-Level bzw. X-Spam-Flag, da sie nicht zum Standard gehört, hinzugefügt werden. Ein Filter besteht aus zwei Teilen, einer Bedingung und der Beschreibung einer Aktion, die erfolgen soll, wenn diese Bedingung erfüllt ist. In einem Filter unter Thunderbird könnte als Bedingung gestellt werden, dass die X-Spam-Flag-Zeile die Zeichenkette „YES“ enthält, und die damit verbundene Aktion einen Transport dieser E-Mail in den Junk-Folder verlangt.

*Das Medium E-Mail ist vielfältigen Störungen ausgesetzt. Dazu zählen z. B. die Datenflut durch unerwünschte Werbemails und Versuche, mittels gefälschter Anfragen und untergeschobener URLs persönliche Daten „abzufischen“ oder den Datenverkehr „mitzuhören“.*

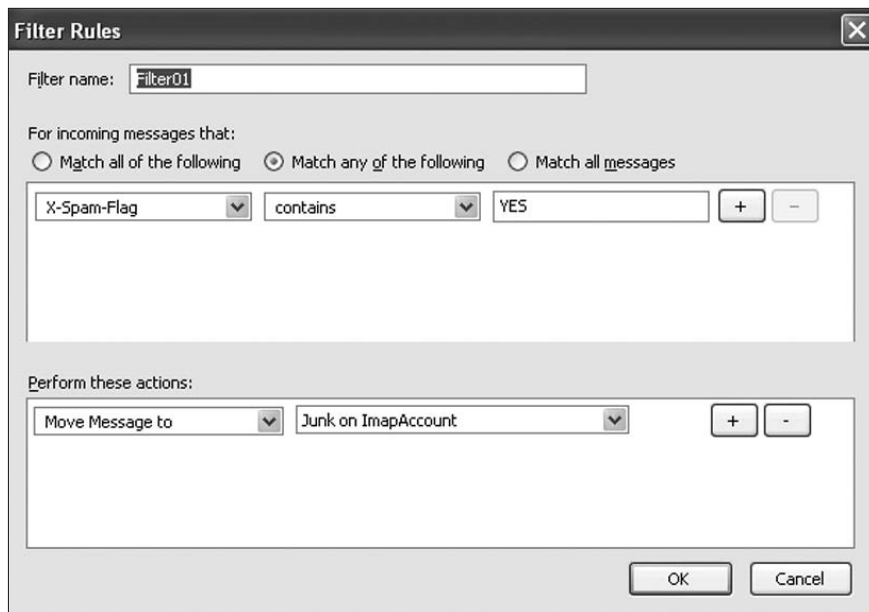


Abb. 2: Filter überträgt automatisch Mails, bei denen X-Spam-Flag auf YES gesetzt ist, in den Junk-Folder.



Abb. 3: Diese Zertifikate der Telekom, des DFN-Vereins und der HU sollten vorhanden sein oder über „Import“ bereitgestellt werden (Beispiel: Thunderbird).

Bedingung:

X-Spam-Flag contains YES

Aktion:

Move Message to Junk on ImapAccount.

Auf Ihre persönlichen Belange hin trainieren Sie Ihren Client, indem Sie die automatisch vorgenommene Bewertung, ob Ihr Client diese E-Mail für „Junk-Mail“ hält oder nicht, durch Anklicken umschalten. In der Anzeige von einzelnen E-Mails oder von Foldern gibt es hier ein gesondertes Feld bzw. eine Spalte.

## Sicher in den Verbindungen

In der Verbindung zwischen Server und Client wird der Client gewissermaßen Ihr Stellvertreter. Er soll ja Ihre Daten lesen und anzeigen können, speziell Ihre Mailbox und Ihre zentralen Verzeichnisse. Dazu nutzt er Ihren Account und es bedarf dafür auch Ihres Passwortes. Beide Zeichenketten müssen also über das Netz geschickt werden. Dabei besteht die Gefahr des unerlaubten „Abhörens“. Daher sollten Maßnahmen ergriffen werden, die dafür sorgen, dass diese Zeichenketten nicht im Klartext ausgetauscht werden. Das Stichwort dazu heißt: „Sichere Verbindung“. Hier handeln die beteiligten Rechner miteinander ein Verschlüsselungsverfahren aus. Dadurch können Account und Passwort nicht mitgelesen werden. Aktivieren Sie also bei der Definition Ihrer Posteingangs- und Postausgangsserver die Verfahren für eine „Sichere Verbindung“.

## Ganz sicher im Mailverkehr mit ausgewählten Partnern

Da die meisten Angaben im Mail-Umschlag direkt durch den Nutzer gesetzt werden, können all diese Angaben auch falsch sein und missbräuchlich verwendet werden. Es ist deshalb mit einem zusätzlichen Aufwand verbunden, wenn man seinem Mailpartner zeigen und verbindlich nachweisen möchte, diese Mail stammt wirklich von mir, die übermittelten Daten wurden (unterwegs) nicht verändert und sie konnten auch nicht von Dritten gelesen werden. Dies sind die Ziele, die man erreichen möchte: Authentizität, Integrität und Vertraulichkeit. Hilfsmittel, diese Ziele zu erreichen, stellen Zertifizierungsinstanzen zur Verfügung. Sie stellen Ausweise (Zertifikate) aus, deren Echtheit in Kombination mit Verschlüsselungsverfahren nachgewiesen bzw. überprüft werden kann. Die Zertifikate und eine Anleitung, wie diese in den Mailclient zu installieren sind, werden auf den WWW-Seiten des CMS bereitgestellt (Homepage des CMS → A bis Z → XYZ → Zertifikat). Die benötigten Zertifikate

(Deutsche Telekom Root CA 2, DFN-PKI-Global, HU-CA) sind in ein beliebiges Verzeichnis auf dem Rechner, der als Mailclient dient, abzuspeichern. Aus diesem Verzeichnis sind die Zertifikate dann in den Mailclient zu importieren. Das geschieht beispielsweise für den Thunderbird-Mailclient über die Kette: Tools → Account Settings... → Security → View Certificates → Authorities → Import oder Tools → Options → Advanced → Certificates → View Certificates → Authorities → Import.

„View Certificates“ zeigt die bisher akzeptierten Zertifizierungsinstanzen und bietet über den Button „Import“ die Möglichkeit, zusätzliche Zertifikate zu installieren.

Zum Importieren neuer Zertifikate werden diese nacheinander ausgewählt und geöffnet. Mit dem Bestätigen des Vertrauens in die Zertifikate können diese dann zur Identifizierung von Servern und Nutzern eingesetzt werden.

Zum Schutz von Inhalten einer E-Mail stehen zwei Verfahren zur Verfügung: „Signieren“ und „Verschlüsseln“. (Bitte „Signieren“ und „Signatur“ nicht gleichsetzen oder verwechseln. Signatur ist ein lesbarer Textabschnitt, der automatisch an den Textkörper gehangen wird.) Signieren bedeutet: Über dem Zertifikat und dem Mailtext wird eine Art gemeinsame „Quersumme“ (Hash-Code) gebildet. Dieser Wert wird mit dem geheimen Schlüssel des Absenders verschlüsselt und an die E-Mail gehangen. Der Empfänger kann jetzt unter Nutzung des öffentlichen Schlüssels zwei Eigenschaften nachweisen:

Die E-Mail stammt tatsächlich vom richtigen Absender und die E-Mail ist im Originalzustand. Der eigentliche Text der E-Mail bleibt von diesem Sicherheitsfeature unberührt. Er bleibt also auch dann lesbar, wenn der Empfänger nicht über die Möglichkeiten verfügt, sich von der Echtheit zu überzeugen. Signieren könnte man eine E-Mail also immer einsetzen sollte man es aber nur da, wo es tatsächlich geboten ist.

Kommt es wirklich auf Geheimhaltung an, so muss verschlüsselt werden. Zum Verschlüsseln muss man im Besitz des Zertifikats des Empfängers sein. Damit wird die E-Mail verschlüsselt.

Diese Verschlüsselung kann nur mit dem geheimen Schlüssel des Empfängers wieder lesbar gemacht werden. Dadurch bleibt der Inhalt dieser Mail Dritten verborgen. Dieses Verfahren gewährleistet also die Vertraulichkeit. Es bedarf aber, mindestens in der Richtung vom Empfänger zum Sender, der Übermittlung des Zertifikats. Und es kann nur mit Hilfe eines Chipkartenlesers tatsächlich auch gelesen werden. Es ist also auch nur zwischen Partnern sinnvoll, die Absprache über eine Verschlüsselung getroffen und die nötigen Zertifikate untereinander ausgetauscht haben.

Die Funktionen „Signieren“ und „Verschlüsseln“ werden zwar von den Mailclients bereitgestellt, sie können aber nur genutzt werden, wenn man im Besitz der richtigen Zertifikate ist und ein Lesegerät für die Smartcard verfügbar ist.