KATHOLISCHE UNIVERSITÄT EICHSTÄTT INGOLSTADT

UniversitätsRechenZentrum

Filtern von unverlangt zugesandten Werbe-EMails

1. Vorbemerkung

Mit dem DFN-MailSupport, an dessen Pilotierung sich die Kath. Universität Eichstätt-Ingolstadt (KU) seit Mitte Oktober 2011 beteiligt, wird ein zweistufiges Verfahren realisiert, das unerwünschte EMails entweder vom lokalen Mail-Server der KU fernhält oder soweit vorverarbeitet, dass sie durch entsprechende Filtermechanismen in geeignete EMail-Verzeichnisse der Nutzer einsortiert werden können. In der ersten Verfahrensstufe wird anhand zweier Kriterien eine Entscheidung über die Annahme von EMails gefällt:

- Existiert die angegebene EMail-Adresse des Empfängers tatsächlich als gültige EMail-Adresse auf dem Mail-Server der KU?
- Ist der Mail-Server des Versenders in einer der konsultierten Blacklists als bekannte SPAM-Schleuder eingetragen?

Nur wenn die Empfänger-Adresse gültig und der Versende-Server vertrauenswürdig ist, wird die EMail tatsächlich entgegengenommen, andernfalls wird die Annahme verweigert und der Absender darüber entsprechend verständigt.

Nach erfolgter Annahme wird jede EMail automatisch daraufhin untersucht, ob sie mit Schadsoftware (Viren oder sonstige Malware) behaftet ist oder ob es sich mit einer gewissen Wahrscheinlichkeit um SPAM handelt; das Ergebnis dieser Bewertung wird in zusätzlichen Kopfzeilen der EMail (EMail-Header) zur späteren Auswertung durch den lokalen Mail-Service der KU festgehalten. Die Details zum neuen Service DFN-MailSupport können in den DFN-Mitteilungen Ausgabe 80 vom Mai 2011, S. 10–13, `http://www.dfn.de/fileadmin/5Presse/DFNMitteilungen/DFN_Mitteilungen_80.pdf` und Ausgabe 81 vom November 2011, S. 8–11, (URL dann am Ende `..._81.pdf`) nachgelesen werden.

2. SPAM-Filterung

Neben diesen vorgeschalteten Verfahren des DFN-MailSupports wird auf dem Mail-Server der KU anschließend das auch bisher schon eingesetzte System **Sophos PureMessage** weiterhin verwendet, um mit Schadsoftware behaftete EMails endgültig zu verwerfen bzw. eine zusätzliche Bewertung der SPAM-Wahrscheinlichkeit – jetzt sozusagen als „zweite Meinung“ – vorzunehmen. Damit verfügen alle letztlich verbliebenen EMails über zusätzliche Kopfzeilen mit dem Hinweis `X-DFN-Spam-Level XX ... X` bzw. `X-Spam-Level XX ... X`, wobei die Anzahl der vergebenen `X` ein Maß für die SPAM-Wahrscheinlichkeit darstellen (allerdings mit unterschiedlicher Werteskala). Auch wenn diese zusätzlichen Kopfzeilen beim Öffnen einer EMail üblicherweise nicht angezeigt werden, sondern erst durch Einstellen der betreffenden Option im Mail-Client sichtbar gemacht werden [beim Mail-Client **Mozilla Thunderbird** beispielsweise durch *Ansicht* → *Kopfzeilen* → *Alle*], so kann doch jeder Nutzer auf der Grundlage dieser Kopfzeilen mit Hilfe eines Filters alle als hochgradig SPAM-verdächtig bewerteten EMails in einen gesonderten Ordner verschieben bzw. löschen lassen.

Dies geschieht am besten durch einen **serverseitigen Filter**, damit nicht auf jedem verwendeten Mail-Client gesondert Filtereinstellungen vorzunehmen sind.

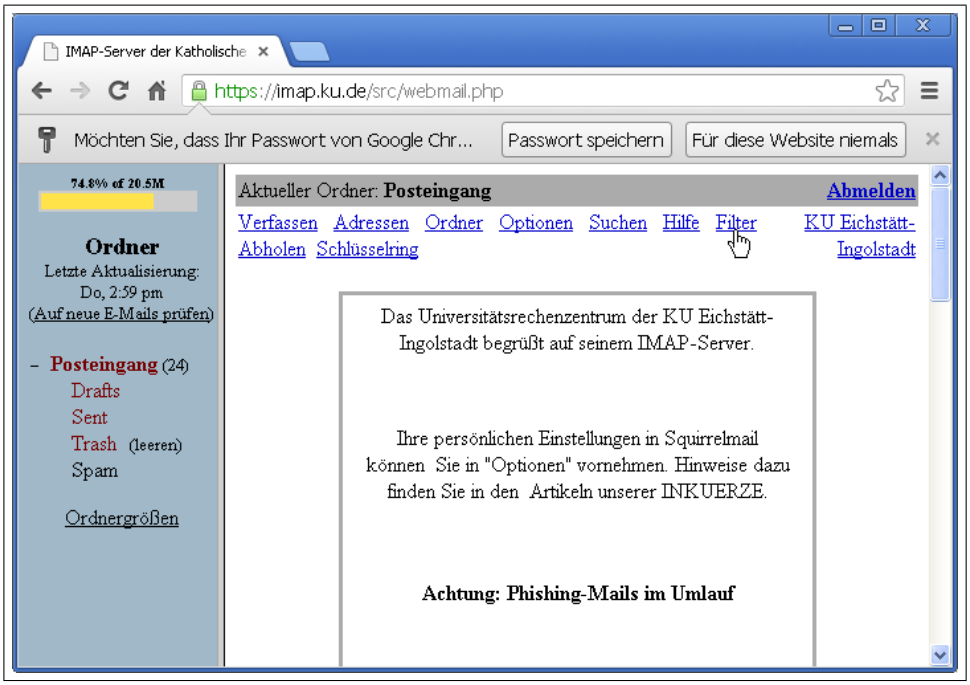
3. Filterregeln

Auf der Grundlage umfangreicher Tests möchte ich für die Filterregeln folgende persönlichen Empfehlungen geben:

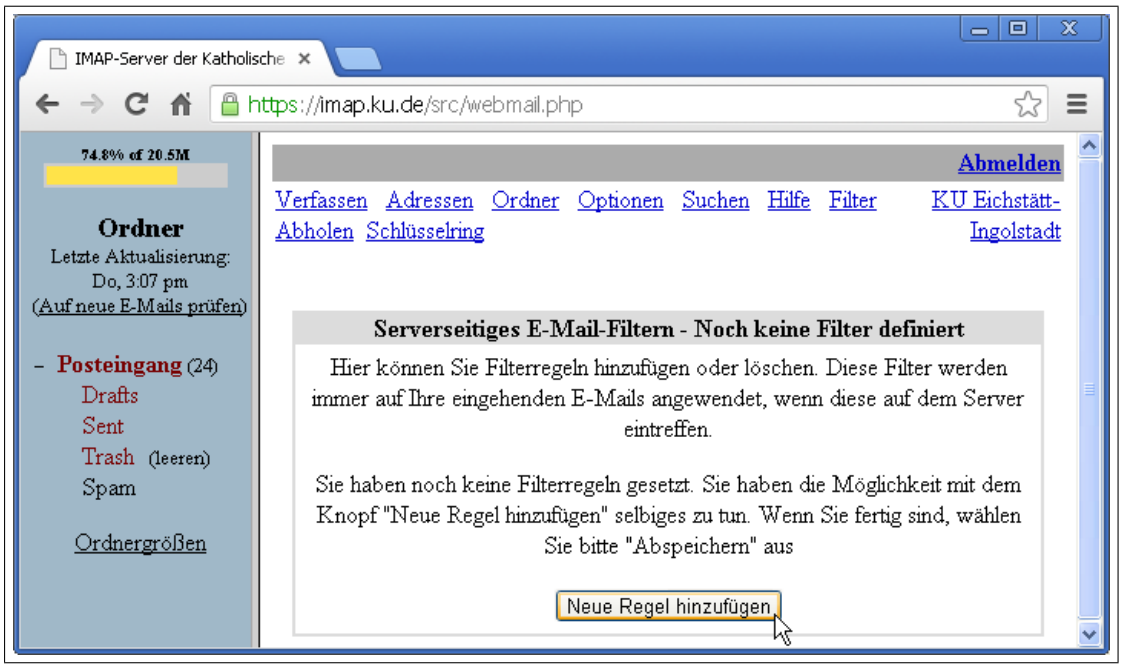
- Verschieben Sie hochgradig SPAM-verdächtige EMails in einen gesonderten Ordner `Spam`;
- Starten Sie dazu mit den Schwellenwerten `X-Spam-Level XXX` (drei `X`) und `X-DFN-Spam-Level XXXXXXXX` (acht `X`).

Die entsprechenden Filterregeln werden auf dem IMAP-Mail-Server der KU mit Hilfe des WebMailers **SquirrelMail** folgendermaßen eingestellt: Gehen Sie in Ihrem Browser auf die Webseite `mail.ku.de`, melden sich dort mit Ihrer Nutzerkennung (Name:) und Ihrem Passwort (Password:) beim WebMailer an

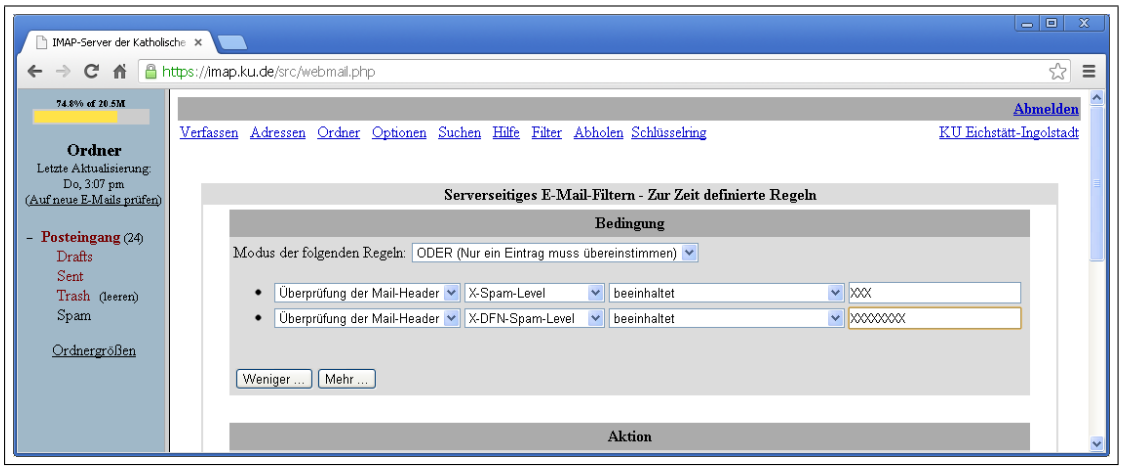
und wählen anschließend die Option *Filter*



Klicken sie anschließend im Fenster *Serverseitiges E-Mail-Filtern* auf die Schaltfläche *Neue Regel hinzufügen*

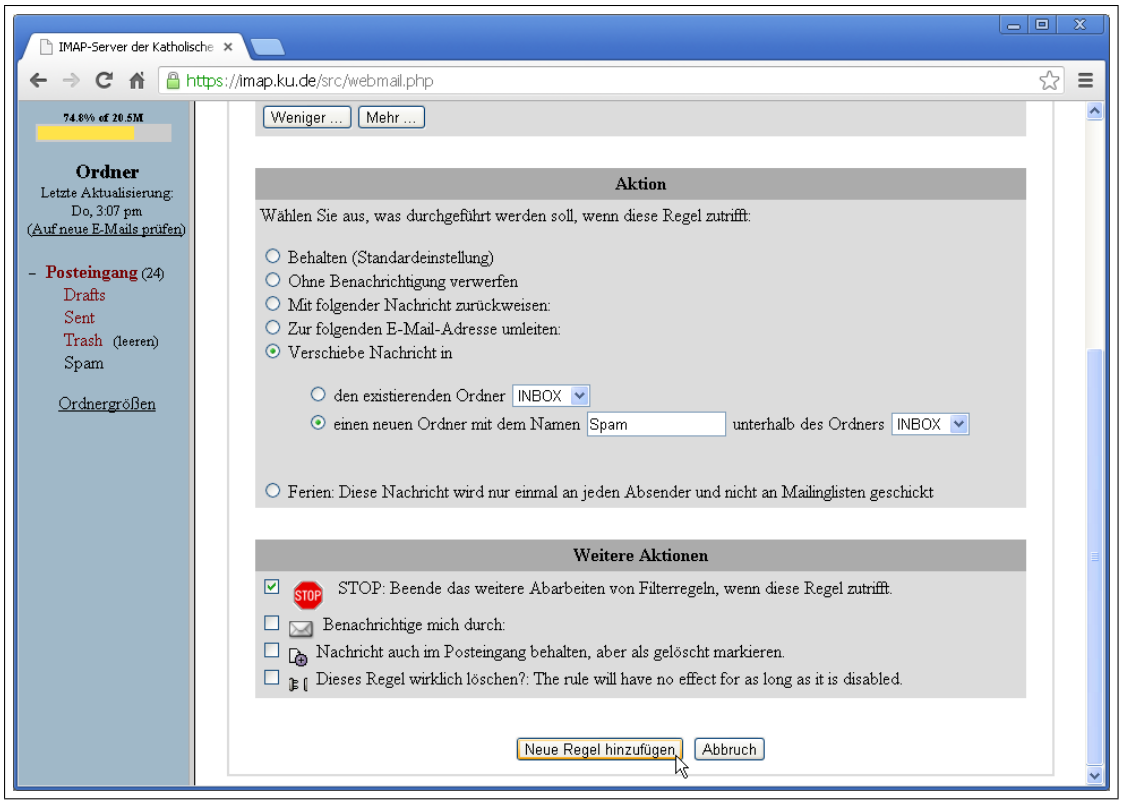


und reduzieren Sie durch Klicken auf die Schaltfläche *Weniger ...* die Anzahl der Regelzeilen auf zwei. Wählen Sie als *Modus der folgenden Regeln:* die Option `ODER (Nur ein Eintrag muss übereinstimmen)`, wählen in der ersten Regelzeile als Mail-Header statt `An: oder CC` die Option `X-Spam-Level` aus und tragen in das rechte Feld `XXX` ein. Entsprechend wählen Sie in der zweiten Regelzeile als Mail-Header statt `An: oder CC` die Option `X-DFN-Spam-Level` aus und tragen in das rechte Feld `XXXXXXXX` ein.



Als zugehörige Aktion wählen Sie im unteren Fensterbereich die Option *Verschiebe Nachricht in* mit der Zusatzoption *einen neuen Ordner mit dem Namen* `Spam` *unterhalb des Ordners* `INBOX` aus. [Wenn der Ordner `Spam` bereits existiert, weil Sie ihn bereits bei einer früheren Filterdefinition erzeugt haben, wählen Sie natürlich als Zusatzoption *in den existierenden Ordner* `Spam`.]

Ein Haken bei der Zusatzaktion *STOP: Beende das weitere Abarbeiten von Filterregeln, wenn diese Regel zutrifft* vervollständigt schließlich den Eintrag. Ein abschließendes Klicken auf *Neue Regel hinzufügen* beendet die Definition der SPAM-Filterregeln.



Mit Hilfe dieser Filterregeln werden nun SPAM-verdächtige Mails automatisch in den Ordner `Spam` verschoben. Schauen Sie deshalb regelmäßig in Ihrem Ordner `Spam` nach, ob sich nicht gelegentlich auch mal eine Mail dorthin verirrt hat, die Sie persönlich nicht als SPAM einstufen würden (sogenannte False Positives) und die Sie deshalb in einen anderen Ordner verschieben müssen, bevor Sie alle Mails im Ordner `Spam` löschen. Sollte dies häufiger passieren oder sollten noch zuviele SPAMs in Ihrem Eingangsordner verbleiben, müssten Sie die Filterregeln in der einen oder anderen Richtung gegebenenfalls nachjustieren.

Dr. W.A. Slaby Stand: Dezember 2012