

# Dokumentation des Spam Guardian für Plesk

## Inhalt dieser Dokumentation

- |   |                |
|---|----------------|
| <b>1. Kurzübersicht über die Funktionen</b>     | <b>Seite 2</b> |
| <b>2. Anmeldung &amp; Navigation</b>            | <b>Seite 3</b> |
| <b>3. Konfiguration</b>                         | <b>Seite 4</b> |
| <b>3.1 Navigation &amp; Übersicht</b>           |                |
| <b>3.2 Domainweite Konfiguration</b>            | <b>Seite 5</b> |
| <b>3.3 Konfiguration für einzelne Mailboxen</b> | <b>Seite 8</b> |
| <b>4. Training des Spamfilters</b>              | <b>Seite 9</b> |

## 1. Kurzübersicht über die Funktionen

Der 4PSA Spam Guardian Filter bietet Ihnen unter anderem die folgenden Features:

- Spamschutz für ganze Domains oder einzelne Mailboxen
- Automatischer, auf Bayes'schen Netzwerken basierender Lernprozess
- Spam-Einstellungen für den ganzen Server, pro Domain oder für einzelne Mailboxen
  - E-Mails mit einem Spamscore über X können mit benutzerdefinierten Tags versehen werden (typischerweise **\*\*\*SPAM\*\*\*** in der Betreffzeile)
  - E-Mails mit einem Spamscore über Y können automatisch gelöscht werden
  - Verschieben von Spam in einen IMAP-Ordner
  - Weiterleiten von Spam an eine andere Mailbox
  - Erkannte Spam-Mails können in Form eines E-Mail-Anhangs bereit gestellt werden
- Weitere Funktionen der AntiSpam-Erkennungsroutine:
  - Unterstützung für kollaboratives Spam-Filtering (Razor / Pyzor / DCC)
  - Automatisches Whitelisting
  - Lernfunktion mit definierbaren Grenzwerten
  - Prüffunktion für Kodierung und Sprache von Mails
- Umfangreiche Statistiken
  - Alle Statistiken werden auf Mailbox-, Domain- und Server-Ebene erstellt
  - Automatische Generierung von Graphen, basierend auf den Statistiken
  - Anzeige bearbeiteter, gelöschter und markierter E-Mails
  - Statistiken: bester Tag, schlimmster Tag, durchschnittliches Spam-Aufkommen etc.
  - Tägliche Statistiken können automatisch per E-Mail verschickt werden
- Individuell einstellbare Filter:
  - Whitelist – ermöglicht das Einrichten spezieller Mailadressen, die automatisch als vertrauenswürdig gelten
  - Blacklist – ermöglicht das Einrichten spezieller Mailadressen, die automatisch geblockt werden
  - Trusted Networks – ermöglicht das Einrichten spezieller Netzwerkadressen, die automatisch als vertrauenswürdig gelten
  - Im- und Export von Textdateien mit Blacklists, Whitelists und Trusted Networks möglich
- Legen Sie die Regeln für die Behandlung von Spam fest:
  - Filtern Sie nach Ausdrücken im Betreff, im Header oder im Inhalt der Mail

## 2. Anmeldung & Navigation

Um die Spamfilter-Einstellungen für eine ganze Domain zu konfigurieren, müssen Sie sich zunächst mit Ihrem Benutzerkonto in das Plesk-Interface einloggen.

Abbildung 1 – Plesk Login



Im linken Navigationsmenü unter dem Menüpunkt ‚Benutzerdefiniert‘ klicken Sie bitte auf die Verknüpfung ‚AntiSpam‘, um den Spam Guardian konfigurieren zu können.

Abbildung 2 – Menüleiste



### 3. Konfiguration

#### 3.1 Navigation & Übersicht

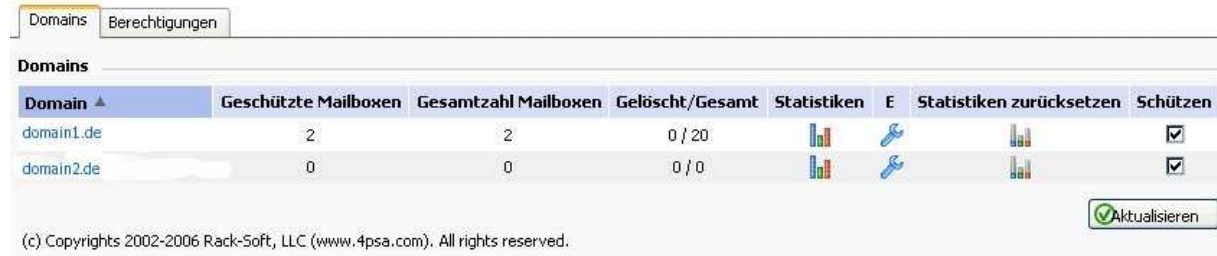
Der Menüpunkt ‚AntiSpam‘ ermöglicht Ihnen die folgenden Aktionen:

- Spamschutz für Domains und Mailboxen konfigurieren
- Anzeige von Statistiken für Domains und für einzelne Mailboxen
- Ändern der Einstellungen für Domains und Mailboxen

Auf der AntiSpam Übersichtsseite ist standardmäßig der Reiter ‚Domains‘ aktiv, welcher Sie per Klick auf die jeweilige Domain zur Verwaltungsseite für domainweite Einstellungen führt.

Abbildung 3 – Domainübersicht

Liste der Domains



Domain ▲	Geschützte Mailboxen	Gesamtzahl Mailboxen	Gelöscht/Gesamt	Statistiken	E	Statistiken zurücksetzen	Schützen
domain1.de	2	2	0 / 20				<input checked="" type="checkbox"/>
domain2.de	0	0	0 / 0				<input checked="" type="checkbox"/>




(c) Copyrights 2002-2006 Rack-Soft, LLC (www.4psa.com). All rights reserved.

In der Spalte ‚Domain‘ sehen Sie all Ihre Domains, die auf dem Server gehostet werden.

Nachfolgend werden Statistiken angezeigt (von links nach rechts):

- die Zahl der auf der Domain geschützten Mailboxen
- die Gesamtzahl der Mailboxen
- der Anteil der E-Mails, die wegen Spamverdachts nicht ausgeliefert wurden

Für jede Domain finden Sie drei Spalten mit folgenden Aktionsmöglichkeiten:

-  Anzeige der Statistiken für die jeweilige Domain
-  Einstellungen für die ausgewählte Domain ändern (E)
-  Zurücksetzen der Statistiken

Klicken Sie nun auf eine Domain, um eine Übersicht über alle Mailboxen unterhalb dieser Domain zu erhalten. Dabei ist zu beachten, dass die Mailboxen ohne den jeweiligen Domainnamen angezeigt werden (‚info@domain1.de‘ wird also z.B. schlicht zu ‚info‘).

Wenn das Häkchen in der Box ‚Gesamte Domain schützen‘ gesetzt ist, werden automatisch alle Mailboxen unterhalb der ausgewählten Domain vom Spamfilter bearbeitet. Wenn Sie diesen Haken entfernen, müssen Sie den Spamschutz für alle Mailboxen einzeln aktivieren und konfigurieren.

Abbildung 4 – Mailbox-Übersicht

Domains >  
Schutz für die Domain **domain1.de** Eine Ebene höher

Domains | Berechtigungen

---

**Domain-Schutz**

Gesamte Domain schützen  Aktualisieren

**Mailbox-Schutz**

Mailbox ▲	Gelöscht/Gesamt	Statistiken	E	Statistiken zurücksetzen	Schützen
info	0 / 20				<input checked="" type="checkbox"/>
test	-				<input checked="" type="checkbox"/>

Aktualisieren

(c) Copyrights 2002-2006 Rack-Soft, LLC (www.4psa.com). All rights reserved.

Auch in dieser Übersicht finden Sie die bereits vom vorigen Menüpunkt bekannten Einstellungsmöglichkeiten mit den dazugehörigen Symbolen – ‚Statistiken‘ ( ) für die Statistiken, ‚E‘ ( ) für die Einstellungen und ‚Statistiken zurücksetzen‘ ( ), um die Statistiken zurückzusetzen.

### 3.2 Domainweite Konfiguration

Um nun den Spamfilter für Ihre gesamte Domain zu konfigurieren, öffnen Sie den Menüpunkt ‚AntiSpam‘ erneut, sodass Sie in die Übersicht über Ihre Domains gelangen.

Abbildung 3 – Domainübersicht

Liste der Domains

Domains | Berechtigungen

---

**Domains**

Domain ▲	Geschützte Mailboxen	Gesamtzahl Mailboxen	Gelöscht/Gesamt	Statistiken	E	Statistiken zurücksetzen	Schützen
domain1.de	2	2	0 / 20				<input checked="" type="checkbox"/>
domain2.de	0	0	0 / 0				<input checked="" type="checkbox"/>

Aktualisieren

(c) Copyrights 2002-2006 Rack-Soft, LLC (www.4psa.com). All rights reserved.

Nun klicken Sie bitte in der Zeile der gewünschten Domain auf das Icon , um das Menü für die Konfiguration der Filtereinstellungen der gewählten Domain zu erreichen (siehe Abbildung 5 auf Seite sieben).

*Folgende Einstellungen sind hier möglich:*

#### Spamfilter-Einstellungen für die Domain

- Domaineinstellungen zurücksetzen  
Wenn Sie die Einstellungen Ihres Spamfilters zurücksetzen möchten, wählen Sie diese Option und klicken Sie auf ‚Aktualisieren‘.
- Betreffzeile von Spam-E-Mail bearbeiten  
Wenn Sie diese Option aktivieren, werden erkannte Spam-Mails automatisch mit einem vorher definierten Begriff (Voreinstellung ist **\*\*\*SPAM\*\*\***) in der Betreffzeile markiert und können so leicht über Filterregeln in Mailclients oder dem WebMail-Interface aussortiert werden.

- Markierung des Betreffs für Spam-E-Mail

In dieser Zeile legen Sie fest, auf welche Art und Weise Spam-Mails in der Betreffzeile markiert werden sollen (Voreinstellung ist **\*\*\*SPAM\*\*\***).

- Spam als Anhang

Mit der Aktivierung dieser Funktion werden als Spam erkannte E-Mails automatisch in den Anhang einer neuen E-Mail gepackt und so als leere E-Mail mit Anhang ungefährlich verschickt.

- Einstellung zum Markieren von E-Mails

In der nebenstehenden Auswahlbox können Sie wählen, wie streng Ihr Spamfilter die E-Mails verarbeiten soll. Sie haben die Wahl zwischen fünf Abstufungen von ‚Sehr durchlässig‘ bis ‚Sehr streng‘. Wenn Sie ‚Benutzerdefinierter Wert‘ wählen, können Sie im Eingabefeld einen beliebigen Wert zwischen 0 und 1000 angeben, woraufhin alle E-Mails, die eine höhere Spamscore als die von Ihnen angegebene Zahl erhalten haben, gefiltert werden – je niedriger also die Zahl, desto mehr E-Mails werden vom Filter bearbeitet. Üblicherweise verwendet man hier Werte im Bereich zwischen 3 und 9.

- Einstellung zum Löschen von E-Mails

Wie beim vorherigen Punkt haben Sie auch hier die Wahl, wie streng dieser Filter Ihre E-Mails durchforsten soll – jedoch werden alle E-Mails, die vom Löschfilter gefiltert werden, automatisch vom Mailserver entfernt. Seien Sie daher vorsichtig mit diesen Einstellungen, sonst könnten auch erwünschte E-Mails verloren gehen.

Auch bei diesem Punkt können Sie wieder einen benutzerdefinierten Wert zwischen 0 und 1000 angeben, die Sortierung funktioniert analog zur Einstellung zum Markieren von E-Mails.

Wenn Sie verhindern möchten, dass Mails von diesem Filter gelöscht werden, können Sie in das Feld den Wert 1000 eingeben (dies ist auch die Standardeinstellung).

- Tägliche Statistik erzeugen

Wenn Sie diese Checkbox aktivieren, erzeugt der Spam Guardian eine tägliche Statistik für die ausgewählte Domain.

### **Whitelist-Einstellungen für die Domain**

In der Whitelist können Sie E-Mail-Adressen angeben, von denen Sie auf jeden Fall E-Mails erhalten wollen – alle E-Mails von Mailadressen auf der Whitelist werden vom Spamfilter mit einem Spamscore von -100 versehen.

Bei der Angabe der Mailadressen können Sie auch die Wildcards \* (für eine Zeichenfolge) und ? (für ein einzelnes Zeichen) setzen, um mit einem Eintrag mehrere Mailadressen abzudecken.

Mit der Option ‚Aus Datei importieren‘ können Sie eine Textdatei mit E-Mail-Adressen für die Whitelist von Ihrem Computer hoch laden und importieren. Außerdem können Sie einmal getroffene Whitelist-Einstellungen genauso in eine Datei auf Ihrem Computer exportieren.

### **Blacklist-Einstellungen für die Domain**

Den gegenteiligen Effekt zur Whitelist bietet Ihnen die Blacklist. Alle E-Mail-Adressen, die sich auf Ihrer schwarzen Liste wieder finden, werden vom Mailserver akzeptiert und mit einem entsprechend hohen Spamscore versehen, aber nicht gelöscht oder abgelehnt - die E-Mails müssen danach noch auf ihren Spamscore hin herausgefiltert werden.

Wie bei der Konfiguration der Whitelist können Sie auch hier Wildcards verwenden sowie Listen importieren und exportieren.

### **Vertrauenswürdige Netzwerke für die Domain**

Vertrauenswürdige Netzwerke sind Netze, die von Ihnen ausgewählt werden und die – wie die White List – vom Spamfilter entsprechend markiert werden.

Auch hier können Sie die Listen aus einer Datei importieren sowie eine bereits erstellte Liste auf Ihrem Computer speichern.

Auf der folgenden Seite dieser Dokumentation finden Sie eine Abbildung zur Illustration der eben erläuterten Filterfunktionen.

## Abbildung 5 – Domainweite Einstellungen

[Domains >](#)

### Domain-Einstellungen für domain1.de

 [Eine Ebene höher](#)

**Domains** | **Berechtigungen**

---

#### Spam Engine-Einstellungen für die Domain

Domaineinstellungen zurücksetzen  Ja, ich stimme zu

Betreffzeile von Spam-E-Mail bearbeiten  für Nachrichten, die markiert aber nicht gelöscht werden sollen.

Markierung des Betreffs für Spam-E-Mail

Spam als Anhang

Einstellung zum Markieren von E-Mails  Benutzerdefinierter Wert  (zwischen 0 und 1000)

Einstellung zum Löschen von E-Mails  Benutzerdefinierter Wert  (zwischen 0 und 1000)

Tägliche Statistik erzeugen

---

#### Whitelist-Einstellungen für die Domain

E-Mail Adresse (\* und ? erlaubt)

Aus Datei importieren

E-Mail von dieser Adresse nie als SPAM markieren

### 3.3 Konfiguration für einzelne Mailboxen

Wenn Sie spezielle Filter-Einstellungen für einzelne Mailboxen treffen möchten, so müssen Sie zunächst in der Übersicht der Domains auf eine Ihrer Domains klicken, um eine Liste der bislang konfigurierten Mailboxen zu erhalten.

Abbildung 4 – Mailbox-Übersicht

Domains > **Schutz für die Domain domain1.de** [Eine Ebene höher](#)

Domains | Berechtigungen

**Domain-Schutz**


Gesamte Domain schützen  [Aktualisieren](#)

**Mailbox-Schutz**

Mailbox ▲	Gelöscht/Gesamt	Statistiken	E	Statistiken zurücksetzen	Schützen
info	0 / 20				<input checked="" type="checkbox"/>
test	-				<input checked="" type="checkbox"/>

[Aktualisieren](#)

(c) Copyrights 2002-2006 Rack-Soft, LLC (www.4psa.com). All rights reserved.

Nun klicken Sie bitte in der Zeile der gewünschten Mailbox auf das Schraubenschlüssel-Symbol , um das Menü für die Konfiguration der Filtereinstellungen der gewählten Mailbox zu erreichen.

Folgende Einstellungen sind hier möglich:

Abbildung 6 – Einstellungen für Mailboxen (Auszug)

Domains > [livestats.ipv6now.de](#) > **Mailbox-Einstellungen für info@domain1.de** [Eine Ebene höher](#)

Domains | Berechtigungen

**Spam Engine-Einstellungen für die Mailbox**

Mailboxeinstellungen zurücksetzen  Ja, ich stimme zu

Betreffzeile von Spam-E-Mail bearbeiten  für Nachrichten, die markiert aber nicht gelöscht werden sollen.

Markierung des Betreffs für Spam-E-Mail

Spam als Anhang

Spam-Weiterleitung aktivieren

Spam an die folgende Adresse weiterleiten  @livestats.ipv6now.de

Spam in einen IMAP-Ordner verschieben

IMAP-Ordner zum Speichern der Spam-E-Mails

Einstellung zum Markieren von E-Mails  Benutzerdefinierter Wert  (zwischen 0 und 1000)

Einstellung zum Löschen von E-Mails  Benutzerdefinierter Wert  (zwischen 0 und 1000)

Tägliche Statistik erzeugen

[Aktualisieren](#)

Der größte Teil der Einstellungen ist identisch zu denen aus der domainweiten Konfiguration bekannten. Wenn Sie eine Referenz hierfür benötigen, konsultieren Sie bitte den Punkt 3.2 dieser Dokumentation.

Im Folgenden werden lediglich die Einstellungen angesprochen, die sich von jenen für die domainweite Konfiguration unterscheiden.

### Spam-Weiterleitung

Die Optionen ‚Spam-Weiterleitung aktivieren‘ und ‚Spam an die folgende Adresse weiterleiten‘ legen fest, ob und wie Spam-Mails automatisch an eine andere Mailbox weitergeleitet werden sollen. Dabei ist zu beachten, dass Sie diese Weiterleitung nur für Mailboxen auf derselben Domain nutzen können. Es empfiehlt sich daher bei Nutzung dieser Funktion, eine separate Mailbox ‚Junk‘ zu erstellen, auf die Sie Ihre Spam-Mails dann weiterleiten können, um sie gegebenenfalls auf fälschlich als Spam markierte Mails überprüfen zu können.

### Spam in einen IMAP-Ordner verschieben

Wenn Sie Ihren Spam eine zeitlang archivieren möchten, können Sie die erkannten Spam-Mails automatisch in einen IMAP-Ordner verschieben lassen. Den Namen des betreffenden Ordners können Sie unter ‚IMAP-Ordner zum Speichern der Spam-E-Mails‘ in das nebenstehende Textfeld eintragen.

*Beachten Sie bitte, dass sich auch alle E-Mail-Benutzer mit Angabe Ihrer Mailadresse sowie Ihres Kennworts am Plesk Interface anmelden können, um die Einstellungen Ihrer Mailbox zu bearbeiten.*

## 4. Training des Spamfilters

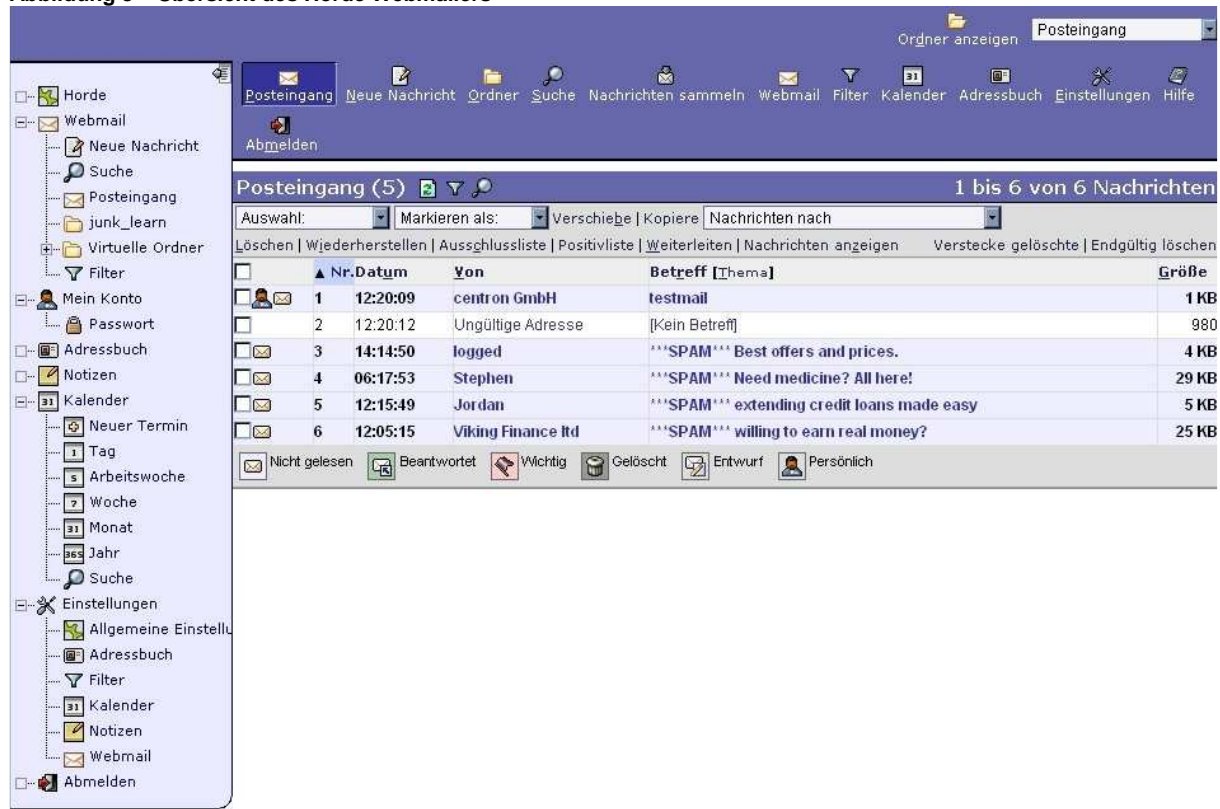
Die Trainingsfunktion Ihres Spamfilters können Sie am einfachsten über das Horde WebMail-Interface konfigurieren und einsetzen. Loggen Sie sich hierfür bitte mit Ihren E-Mail-Zugangsdaten über die Adresse ein, die wir Ihnen in unserer E-Mail mit Ihren Zugangsdaten haben zukommen lassen (Bsp.: webmail.domain1.de).

Abbildung 7 – Das Horde WebMail-Interface



Wenn Sie sich dort erfolgreich angemeldet haben, müssen Sie zunächst die beiden benötigten Ordner für den lernfähigen Spamfilter erstellen, um den Filter danach trainieren zu können. Dies können Sie in der WebMail-Übersicht in Ihrem Posteingang erledigen, klicken Sie also bitte in der linken Navigationsleiste einfach auf den Punkt ‚Webmail‘, um das entsprechende Menü zu öffnen.

Abbildung 8 – Übersicht des Horde Webmailers



Klicken Sie in dieser Übersicht bitte auf den Punkt ‚Ordner‘ in der Menüleiste am oberen Rand der Seite, oberhalb Ihres Posteingangs.

Abbildung 9 - Ordneransicht

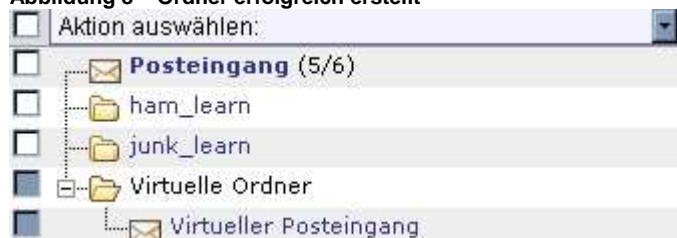


In der Ordneransicht können Sie nun die beiden benötigten Ordner per Klick auf ‚Aktion auswählen:‘ → ‚Ordner erstellen‘ einrichten.

Dabei sollten Sie nun einen Ordner mit dem Namen ‚junk\_learn‘ und einen weiteren Ordner mit dem Namen ‚ham\_learn‘ erstellen.

Der Ordner ‚junk\_learn‘ ist dabei für Spam-Mails gedacht, die vom Filter noch nicht erkannt und markiert wurden, während der Ordner ‚ham\_learn‘ für E-Mails konzipiert ist, die Sie auf jeden Fall empfangen wollten oder die fälschlicherweise als Spam markiert worden sind.

Abbildung 8 – Ordner erfolgreich erstellt



Nachdem die beiden Trainings-Ordner erstellt worden sind (beachten Sie dabei bitte, sich exakt an die obige Schreibweise zu halten, denn sonst werden die Ordner von unserem automatischen Skript nicht überprüft), können Sie sich wieder in Ihren Posteingang begeben und in diesem dann mit dem Training des Filters beginnen.

Abbildung 9 – Posteingang

Nr.	Datum	Von	Betreff [Thema]	Größe
1	12:20:09	centron GmbH	testmail	1 KB
2	12:20:12	Ungültige Adresse	[Kein Betreff]	980
3	14:14:50	logged	***SPAM*** Best offers and prices.	4 KB
4	06:17:53	Stephen	***SPAM*** Need medicine? All here!	29 KB
5	12:15:49	Jordan	***SPAM*** extending credit loans made easy	5 KB
6	12:05:15	Viking Finance ltd	***SPAM*** willing to earn real money?	25 KB

Sie sehen, dass in unserem obigen Beispiel bereits einige E-Mails mit **\*\*\*SPAM\*\*\*** in der Betreffszeile vom Filter als Spam markiert worden sind. Sie können die Markierung wie in Punkt 3.2 beschrieben natürlich auch jederzeit ändern, wenn Sie dies wünschen.

### Spam...

... der nicht als solcher erkannt wurde, sollten Sie nun markieren und über die Funktionsleiste des Webmailers in den Ordner ‚junk\_learn‘ **verschieben**. Klicken Sie hierzu zunächst auf die Box ‚Nachrichten nach‘, wählen Sie dort den Ordner ‚junk\_learn‘ aus und klicken Sie dann auf ‚Verschiebe‘ links von der Box.

### Ham...

... ist eine E-Mail, wenn sie auf jeden Fall erwünscht ist. Solche E-Mails sollten Sie **nicht** in den Ordner ‚ham\_learn‘ **verschieben**, sondern vielmehr eine **Kopie** in diesem Ordner **erstellen** – auch dies ist über die Funktionsleiste Ihres Webmailers möglich, mit Hilfe der Funktion ‚Kopiere‘.

Es kann selbstverständlich auch vorkommen, dass eine E-Mail zu Unrecht als Spam markiert wird. In einem solchen Fall können Sie, um dies zukünftig zu vermeiden, eine Kopie dieser E-Mail im Ordner ‚ham\_learn‘ ablegen, um dem Filter für die Zukunft beizubringen, solche E-Mails nicht mehr als Spam zu behandeln.

Danach sollten sich im Ordner ‚junk\_learn‘ also alle nicht automatisch erkannten Spam-Mails befinden, im Ordner ‚ham\_learn‘ Kopien von erwünschten E-Mails.

Diese beiden Ordner werden in jeder Nacht automatisch per Skript überprüft, die Ergebnisse ausgewertet und in den lernfähigen Spamfilter implementiert. Nachdem dies durchgeführt wurde, werden die Inhalte der Ordner ‚junk\_learn‘ und ‚ham\_learn‘ automatisch gelöscht – aus diesem Grund sollten Sie auch niemals erwünschte E-Mails in den Ordner ‚ham\_learn‘ verschieben, sondern wie oben beschrieben eine Kopie in diesem Ordner erstellen.

### Hinweis:

Die Ordner ‚junk\_learn‘ und ‚ham\_learn‘ können als IMAP-Ordner selbstverständlich in allen gängigen E-Mail-Clients wie etwa Microsoft Outlook oder Mozilla Thunderbird abonniert und so auch ohne das WebMail-Interface zum Training des Spamfilters genutzt werden.