

## **i:mail Filtereinstellungen**

Wichtiger Hinweis:

Um das i:mail-Webinterface richtig nutzen zu können, müssen Sie unbedingt Ihren PopUp-Blocker so einstellen, dass er für Ihr WebMail-Interface PopUps erlaubt, denn ansonsten können Sie nur einen Bruchteil der Funktionen des Mailservers nutzen.

### **Inhaltsverzeichnis**

#### **1. Einleitung**

#### **2. Einrichtung des Spamfilters**

##### **2.1 Grundlegendes**

##### **2.2 Wo finde ich die Spamfiltereinstellungen...**

###### **2.2.1 ...für eine domainweite Konfiguration?**

###### **2.2.2 ...für die Konfiguration einzelner Benutzer?**

##### **2.3 Hinzufügen neuer Filtereinstellungen**

##### **2.4 Verknüpfung von Filtern mit UND und ODER**

##### **2.5 Erläuterung der Spam-Level Angaben**

##### **2.6 Whitelisting mit Filterregeln**

## 1. Einleitung

In der heutigen Zeit sind sowohl Spam- als auch Virenmails ein sehr großes Ärgernis – sie belasten die Server, sie verstopfen Postfächer und kosten die Benutzer Nerven, in schlimmen Fällen sogar Geld.

Der Antivirenfilter ist serverweit einheitlich konfiguriert: alle E-Mails, die an Sie adressiert sind und dem Virenschanner zufolge ein Virus enthalten, werden von unseren Mailservern sofort automatisch gelöscht, noch bevor diese Ihr Mailpostfach erreichen. Falls Sie zusätzlich unseren integrierten Spamfilter nutzen möchten, hilft Ihnen die nachfolgende Dokumentation beim Einrichten Ihrer Filterregeln.

## 2. Einrichtung des Spamfilters

### 2.1 Grundlegendes

Bevor Sie beginnen, den Spamfilter zu konfigurieren, müssen Sie sich zunächst eine Frage stellen: „Will ich einen Filter für eine gesamte Domain erstellen, oder will ich lediglich ein einziges E-Mail-Konto filtern lassen?“

Die Beantwortung dieser Frage bestimmt Ihre weitere Vorgehensweise: wenn Sie sich entschieden haben, die Filter für ein **einzelnes** Mailkonto einzustellen, so loggen Sie sich bitte mit dem entsprechenden Benutzerkonto an Ihrem E-Mail-Webinterface ein, wenn Sie also z.B. den Account 'ich@IHREDOMAIN.de' konfigurieren möchten, so loggen Sie sich bitte mit diesem Konto ein.

Wenn Sie den Spamfilter gleich für **alle Mailkonten** unterhalb einer Domain einstellen möchten, so loggen Sie sich bitte als '[mailadmin@IHREDOMAIN.de](mailto:mailadmin@IHREDOMAIN.de)' am Webinterface ein.

Bitte bedenken Sie dabei, dass alle Änderungen an den Filtereinstellungen dann für **alle** Mailaccounts an Ihrer Domain gelten.

In folgender Tabelle noch einmal eine Übersicht, wie Sie sich einloggen sollten, um die Filter zu bearbeiten:

**Webinterface** <http://mail.IHREDOMAIN.de:8383>

**Benutzer** mailadmin@IHREDOMAIN.de Filterregeln gelten für gesamte Domain

**Benutzer** useraccount@IHREDOMAIN.de Filterregeln gelten für angemeldeten Mailaccount

### 2.2 Wo finde ich die Spamfiltereinstellungen...

#### 2.2.1 ...für eine domainweite Konfiguration?

Die Verarbeitungsregeln des Spamfilters finden Sie im Drop-Down-Menü '**Optionen und Stile...**' (auf der rechten oberen Seite des Webinterfaces) unter dem Unterpunkt ' -> 'Filter Domäne' (sofern Sie als mailadmin angemeldet sind)

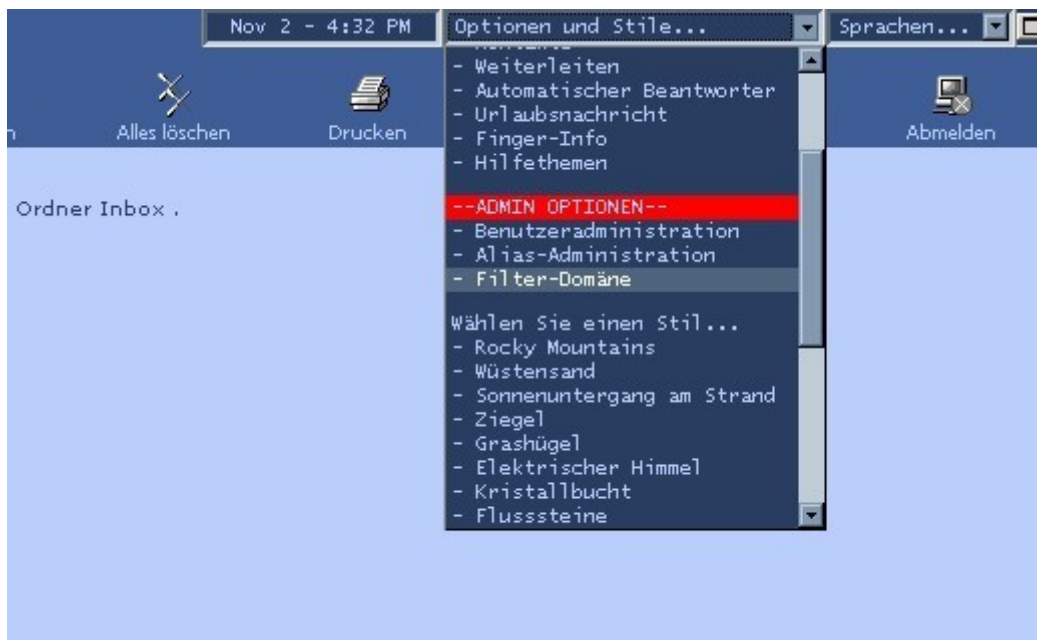
### 2.2.2 ...für die Konfiguration einzelner Benutzer?

Für die Einzelbenutzerkonfiguration konsultieren Sie bitte ebenfalls das Menü **'Optionen und Stile...'**.

Der entsprechende Unterpunkt lautet ' -> 'Filter' (nur, wenn Sie als einzelner User angemeldet sind).

### 2.3 Hinzufügen neuer Filtereinstellungen

#### Ansicht für Administratoren

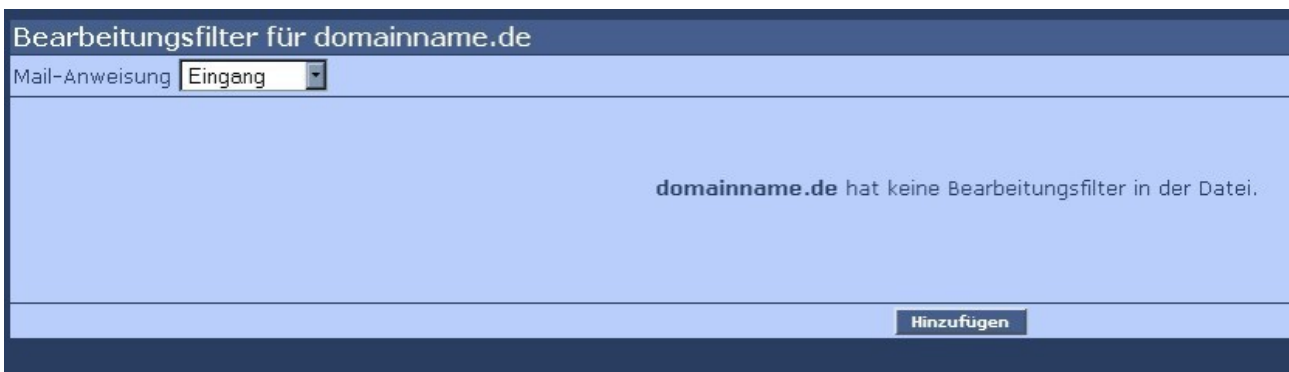


### Ansicht für Benutzer

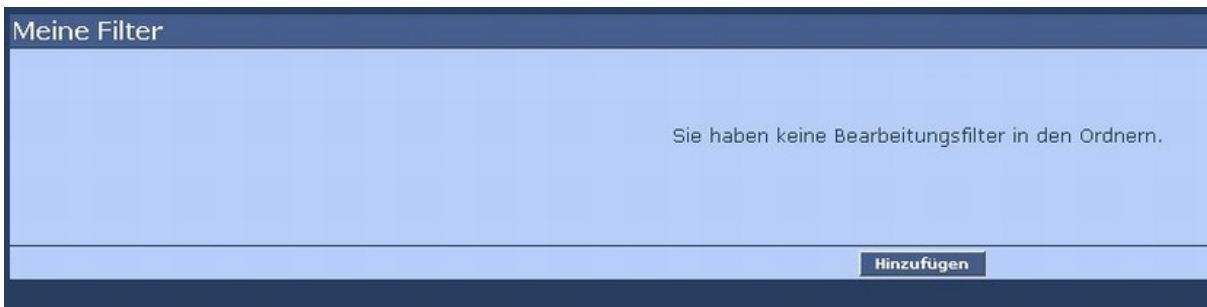


Um nun eine neue Regel zu definieren, klicken Sie bitte zunächst auf 'Hinzufügen'!

### Ansicht für Administratoren



### Ansicht für Benutzer



### Wir empfehlen Ihnen die folgende Konfigurationsweise:

Um nicht für jeden E-Mail-Account immer wieder die gleichen Regeln konfigurieren zu müssen, gibt es die oben bereits erwähnte Möglichkeit, diese mit dem administrativen E-Mail-Account domainweit festzulegen. Diese Regel gilt dann – wie in Punkt 1 beschrieben - für alle E-

Mailadressen, die Sie unterhalb Ihrer Domain eingerichtet haben.

Eingangsregelung bearbeiten für domainname.de

1. Wählen Sie das FELD aus, nach dem Sie suchen wollen.
2. Geben Sie einen Suchstring in das untere Feld ein. Aktivieren Sie das Auswahlfeld, damit der Suchtext von einer externen Datei kommen kann. Das Listenfeld zeigt eine Liste aller existierenden Regelungsdateien an. Klicken Sie auf 'Aktualisieren', um den Inhalt der ausgewählten Regelungsdatei zu erhalten. Die maximale Grenze eines direkten Suchstrings (nicht von einer externen Datei) ist 255. Suchstrings die länger als 255 Zeichen sind, werden nach dem 255. Zeichen abgetrennt.
3. Geben Sie eine Mailbox oder eine E-Mail-Adresse in das Textfeld ein. Eingehende Mails werden zu dieser Mailbox oder E-Mail-Adresse geleitet, wenn diese Regelung in Kraft ist. Wird nichts in das Textfeld eingetragen, wird die herausgefilterte Nachricht in einer Mailbox mit dem Namen 'neu' platziert.

Feld auswählen  
[Dropdown]  Beinhaltet  beinhaltet nicht

Phrase  
[Textfeld]

Groß-/Kleinschreibung passt zusammen  
 String aus Datei suchen: [Dropdown]

[Bedingung aktualisieren] [Bedingung hinzufügen]

Regelungen  
[Liste mit Up/Down Pfeilen und Checkmarken]

[UND einfügen] [ODER einfügen] [Entfernen]

Filter-Aktion: [Dropdown: Verschieben Sie die Nachricht in diese Mailbox:]  
Bestimmungsort: [Textfeld]

[Abbrechen] [Beenden]

Wählen Sie nun, um einen Filter zu erstellen, bitte als Feld "Header" und wählen Sie die Option "Beinhaltet" aus.

Natürlich müssen Sie nicht ausschließlich nach den Markierungen im E-Mail-Header filtern, jedoch ist unsere automatische Spamlevel-Erkennung auf eine Filterung im E-Mail-Header ausgelegt. Das heißt, dass jede E-Mail unseren Spam-Vorfilter durchläuft und anhand von verschiedenen Blacklists eine entsprechende Markierung in ihrem Header erhält, die dann vom Spamfilter in i:mail abgefragt wird.

Wenn Sie nun z.B. alle E-Mails herausfiltern und automatisch löschen möchten, die im Betreff den Begriff 'Käsespätzle' stehen haben, so muss Ihr Filter folgendermaßen aussehen:

Regelung bearbeiten

1. Feld auswählen
2. Geben Sie einen Suchstring in das untere Feld ein. Aktivieren Sie das Auswahlfeld, damit der Suchtext von einer externen Datei kommen kann. Das Listenfeld zeigt eine Liste aller existierenden Regelungsdateien an. Klicken Sie auf 'Aktualisieren', um den Inhalt der ausgewählten Regelungsdatei zu erhalten. Die maximale Grenze eines direkten Suchstrings (nicht von einer externen Datei) ist 255. Suchstrings die länger als 255 Zeichen sind, werden nach dem 255. Zeichen abgetrennt.
3. Geben Sie eine Mailbox oder eine E-Mail-Adresse in das Textfeld ein. Eingehende Mails werden zu dieser Mailbox oder E-Mail-Adresse geleitet, wenn diese Regelung in Kraft ist. Wird nichts in das Textfeld eingetragen, wird die herausgefilterte Nachricht in einer Mailbox mit dem Namen 'neu' platziert.

Feld auswählen  
[Dropdown]  Beinhaltet  beinhaltet nicht

Phrase  
[Textfeld]

Groß-/Kleinschreibung passt zusammen  
 String aus Datei suchen: [Dropdown]

[Bedingung aktualisieren] [Bedingung hinzufügen]

Regelungen  
[Liste mit Up/Down Pfeilen und Checkmarken]

[UND einfügen] [ODER einfügen] [Entfernen]

Filter-Aktion: [Dropdown: Verschieben Sie die Nachricht in diese Mailbox:]  
Bestimmungsort: [Textfeld]

[Abbrechen] [Beenden]

Dabei können Sie zudem bestimmen, ob bei den Begriffen Groß- und Kleinschreibung Beachtung finden soll (Standard: aus).

Groß-/Kleinschreibung passt zusammen  
 String aus Datei suchen

**Im Einzelnen haben Sie nun folgende Filter-Aktionen zur Auswahl:**

<b>Filter-Aktion:</b>	Die Nachricht löschen
<b>Bestimmungsort:</b>	Verschieben Sie die Nachricht in diese Mailbox: Mit Kopie senden an: Leiten Sie die Nachricht weiter an: Zurückschicken Die Nachricht löschen

**'Verschieben Sie die Nachricht in diese Mailbox:'** bewirkt, unter Angabe einer Ziel-Mailbox, dass alle E-Mails, die vom Filter als Spam markiert werden, in die von Ihnen definierte Mailbox verschoben werden. Dabei muss sich die Ziel-Mailbox auf demselben Server befinden.

**'Mit Kopie senden an:'** empfiehlt sich weniger für eine Spamfilter-Einstellung, denn diese Funktion bewirkt, dass eine vom Filter erkannte Spam-Mail mit einer Kopie an eine von Ihnen definierte Mailadresse geschickt wird.

**'Leiten Sie die Nachricht weiter an:'** sorgt dafür, dass die E-Mail, ohne dass eine Kopie in Ihrem Postfach zurückbleibt, an eine andere Mailadresse weitergeleitet wird, die sich auch auf einem anderen Mailserver befinden kann.

**'Zurückschicken'** sorgt dafür, dass die E-Mail 'gebounce' wird und die E-Mail mit dem Vermerk 'undeliverable to user' an den Versender der E-Mail geschickt wird. Dies kann allerdings auch als eine Form des Spam angesehen werden, denn durch die Benutzung dieser Option wird jede Spam-E-Mail erneut verschickt, diesmal nicht in Ihr Mailkonto, sondern von Ihrem Mailkonto auf ein anderes.

**'Die Nachricht löschen'** ist die eindeutigste Option: hier wird die E-Mail, sobald der Filter greift, vom Server gelöscht; nichts bleibt zurück.

In den Bestimmungsort tragen Sie die gewünschte Mailbox beziehungsweise den gewünschten Empfänger ein; wird nichts in das Textfeld 'Bestimmungsort' eingetragen, wird die heraus gefilterte Nachricht automatisch in einer Mailbox mit der Bezeichnung 'new' platziert.

Es besteht ebenfalls die Möglichkeit, einen Anhang der E-Mail zu blocken bzw. direkt zu löschen:

Im am obigen Bild veranschaulichten Beispiel wird jede E-Mail, die als Anhang eine .exe-Datei enthält, sofort verarbeitet.

Dies ist besonders sinnvoll zum Schutz gegen Viren oder Würmer.

Sie können natürlich jede beliebige Dateierdung, z.B. also

name=".\*\.com"

name=".\*\.bat"

name=".\*\.pif"

name=".\*\.scr"

name=".\*\.reg"

verwenden.

## 2.4 Verknüpfung von Filtern mit UND und ODER

Sie können mehrere Filter bequem mit einem logischen UND sowie einem logischen ODER verknüpfen und somit zwei Fliegen mit einer Klappe schlagen. Zudem können Sie somit sehr spezifische Filtereinstellungen erstellen.

Filterbeispiel



In unserem obigen Beispiel werden nun also alle E-Mails vom Filter betroffen, deren Betreff das Wort Schnee enthält und deren Text gleichzeitig NICHT das Wort Sonne im Mailtext oder das Wort Regen im Betreff beinhaltet. Sie können die Begriffe und Verbindungen mit Hilfe der Pfeiltasten rechts von dem abgebildeten Kasten nach oben und unten bewegen.

Mit AND stellen Sie also eine Bedingung her, die auf jeden Fall erfüllt sein muss, mit OR stellen Sie eine gleichrangige Beziehung zweier Begriffe her.

## 2.5 Erläuterung der Spam-Level Angaben

Wenn Sie nun von unserem automatischen Spamfilter profitieren möchten und keine eigenen Filtereinstellungen vornehmen möchten, müssen Sie lediglich die vier Spamlevel-Begriffe so einsetzen, wie Sie es benötigen.

Das heißt, Sie erstellen beispielsweise eine Regel, die folgendermaßen aussieht:

Meine Filter			
Feld	Filter	Wert	Verschieben nach
Header	Beinhaltet	LEVEL30	Verschieben Sie die Nachricht in diese Mailbox junk
			<input type="button" value="Alles löschen"/> <input type="button" value="Hinzufügen"/>

Diese Regel bewirkt nun, dass alle E-Mails, die von unserem Spamfilter mit LEVEL30 markiert worden sind, automatisch in die Mailbox 'junk' verschoben werden.

Dabei sind unsere Spamlevel so gewählt, dass sie eine ordentliche Abstufung darstellen und somit flexibel eingesetzt werden können; entscheidend ist, dass die Filtereinstellungen immer auf das Feld 'Header' angewendet werden, da sonst die automatische Filterung nicht greifen kann.

## **Bedeutung der unterschiedlichen Spam-Level**

### **Unterstützte Spam-Level sind:**

**LEVEL10**

**LEVEL20**

**LEVEL30**

**LEVEL40**

Dabei ist zu beachten, dass beim Einsatz von Spamlevel 10 bedeutend mehr E-Mails herausgefiltert werden, als dies bei LEVEL40 der Fall sein wird. Besonders der Einsatz von LEVEL20 und LEVEL10 kann demzufolge dazu führen, dass auch gewünschte E-Mails Sie plötzlich nicht mehr erreichen können. Daher ist beim Einsatz dieser Filterstufen Vorsicht geboten!

### **LEVEL40**

Bei dieser E-Mail handelt es sich mit großer Wahrscheinlichkeit um eine Spam-Mail.

Sie erhalten die Möglichkeit, diese E-Mail in Ihren Spam-Ordner (Hinweis: i:mail bezeichnet Ordner auch als Mailboxen, daher bedeutet der Begriff ‚Spam-Mailbox‘ dasselbe wie ‚Spam-Ordner‘) zu verschieben oder die Mail direkt vom Mailserver bouncen (d.h. abprallen) zu lassen - diese Entscheidung liegt jedoch allein in Ihrer Hand und kann natürlich jederzeit über die Filtereinstellungen verändert werden.

*Begriff LEVEL40 --> Aktion: 'Zurückschicken'* (nur möglich, wenn Sie sich als „mailadmin“ oder „root“ eingeloggt haben) oder 'verschiebe zu Mailbox „Spam“'

### **LEVEL30**

Der Mailserver des Versenders steht auf mehreren Blacklists oder der Versender existiert nicht.

*Begriff LEVEL30 ---> Aktion: 'verschiebe zu Mailbox "Spam"'*

Diese Regel hat den Vorteil, dass Sie regelmäßig Ihre E-Mails, die in diese Mailbox geleitet werden, überprüfen und ggf. Ihre Filterregeln anpassen können.

### **LEVEL20**

Mails, die unter LEVEL20 fallen, sind oft kein Spam, da auch Newsletter etc. leicht vom Server als LEVEL20 deklariert werden können.

Daher empfiehlt sich für Spamlevel 20 ein Filter wie dieser:

*Begriff LEVEL20 --> Aktion: 'verschiebe zu Mailbox "Junk"'*

Sie sollten bei Benutzung von LEVEL20 auf jeden Fall regelmäßig die Mailbox 'Junk' auf gewollte E-Mails untersuchen und ggfs. die Filtereinstellungen anpassen.

## **LEVEL10**

LEVEL10 ist die schärfste Spamlevel-Einstellung; hier wird sozusagen jede E-Mail, die auch nur ansatzweise verdächtig erscheint, vom Server markiert.

Ein Einsatz von LEVEL10 empfiehlt sich daher nur dann, wenn Sie an einem bestimmten Mailkonto nur sehr wenig bis gar keine E-Mail empfangen möchten; Filter, die LEVEL10 benutzen, sollten Sie nur unter den äußersten Umständen auf Ihre gesamte Domain anwenden.

Wenn Sie aber ein Mailkonto einrichten möchten, das wirklich nur vertrauenswürdige E-Mail erhält, die eventuell noch auf Ihrer persönlichen Whitelist steht, kann der Spamlevel 10 durchaus nützlich sein.

**Sie können** Ihren also Spamfilter je nach Bedarf verschärfen, um einem erhöhtem Aufkommen von Spam entgegen zu wirken.

Bitte beachten Sie dabei aber, dass aufgrund eines zu scharf eingestellten Spamfilters auch von Ihnen erwünschte E-Mails aussortiert werden könnten - wenn Sie also Ihr Postfach sprichwörtlich 'zunageln', so kann Ihnen natürlich der Postbote auch keine Post mehr zustellen.

## **2.6 Whitelisting mit Filterregeln**

Im Bereich der Spam-Filterung gibt es nur eine Sache, die noch tückischer als Spam-E-Mails selbst sind: E-Mails, die fälschlicherweise vom Spamfilter als Spam deklariert werden und ungelesen im Nirvana verschwinden. Besonders ärgerlich ist dieses, 'false positives' genannte Phänomen im Zusammenhang mit Bestellungen oder generell bei der Korrespondenz mit Geschäftspartnern und solchen Personen, auf deren E-Mails Sie angewiesen sind.

Grundsätzlich unterstützt i:mail zunächst keine Whitelist, auf die Sie alle Mailserver und Domains eintragen könnten, von denen Sie auf jeden Fall E-Mail erhalten möchten, ohne, dass der Spamfilter diese vorher aussortiert.

Allerdings ist es dennoch möglich, ein effektives Whitelisting auf Ihrem i:mail Mailaccount einzurichten – mit Hilfe entsprechender Filterregeln.

Kurz gesagt weisen Sie in einer solchen Filterregel den Mailserver an, Mails von bestimmten Absendern auf jeden Fall in Ihren Posteingang zuzustellen.

Wie Sie Filterregeln definieren, wurde Ihnen bereits im Rahmen dieser Dokumentation aufgezeigt. Bei einer Filterregel, die dafür sorgen soll, dass Sie E-Mail von bestimmten Absendern oder mit bestimmten Betreffzeilen auf jeden Fall erhalten, können Sie prinzipiell ähnlich vorgehen wie etwa beim Einrichten einer Regel, die Spam aussortiert.

## Folgende Punkte sind für ein Whitelisting entscheidend:

- wenn Sie die Regel für Ihre gesamte Domain konfigurieren möchten, loggen Sie sich mit dem Benutzer ‚mailadmin‘ in das Web-Interface ein, wenn Sie die Regel lediglich für einen einzelnen Benutzer konfigurieren möchten

- erstellen Sie nun eine Regel folgendem Beispielschema:

**Feld:** Von **beinhaltet**  
**Phrase:** @ihredomain.de  
**Filter-Aktion:** Verschieben Sie die Nachricht in diese Mailbox:  
**Bestimmungsort:** main

- die obige Beispielregel würde nun dafür sorgen, dass alle E-Mails, deren Absender die Phrase ‚@ihredomain.de‘ enthalten, automatisch in Ihren Posteingang zustellen
- intern verwaltet i:mail den Posteingang über die Mailbox mit der Bezeichnung ‚main‘, nicht, wie man vermuten könnte, über die Bezeichnung ‚Inbox‘ – wenn Sie also als Bestimmungsort ‚Inbox‘ angeben, so wird ein neuer Mailbox-Ordner namens ‚Inbox‘ erstellt, in den die E-Mails zugestellt werden – diesen Ordner sehen Sie nicht, wenn Sie etwa mit einem Mailclient wie Outlook per POP3 Ihre E-Mails abrufen
- Sie können die obige Beispielregel selbstverständlich nach Belieben verändern und an Ihre Bedürfnisse anpassen

## Einige weitere Hinweise:

Damit eine solche Filterregel auch greift, müssen Sie sicherstellen, dass die Regel abgearbeitet wird, **bevor** Sie Spam aussortieren lassen – das heißt, falls Sie bereits Filterregelungen zur Spam-Bekämpfung eingerichtet haben, müssen Sie Ihre Whitelist-Regel nun in der Abfolge der Filterregeln nach oben verschieben, damit die Whitelist-Regel vor der Spamfilter-Regel verarbeitet wird.

Nun müssen Sie lediglich noch eine mögliche Fehlerquelle beachten: wenn Sie z.B. domainweite Filterregeln eingerichtet haben (mit dem mailadmin-Benutzer) und nun eine Whitelist-Regel für einen einzelnen Mailbenutzer (etwa [info@ihredomain.de](mailto:info@ihredomain.de)) erstellen, so greifen die domainweiten Filterregeln stets, bevor die Filterregeln der einzelnen Benutzer abgearbeitet werden.

Das heißt effektiv, dass Sie eine solche Whitelist-Regel entweder ebenfalls domainweit erstellen müssen, oder aber Ihre Spamfilter-Regeln für jeden einzelnen Benutzer einrichten, damit Sie überblicken können, in welcher Abfolge Ihre Regeln verarbeitet werden.