

## Benutzerhandbuch für SPAM-MAIL-BLOCKER

I.	Login .....	2
II.	Hauptmenü .....	3
1.	SPAM Modul – Your work .....	3
a)	Erkannte SPAM E-Mails.....	3
b)	Neue Absender bearbeiten .....	4
c)	Spam Postfach zurücksetzen.....	5
d)	Protokolldatei.....	5
2.	Eigene Regeln festlegen .....	6
a)	... für Absender.....	6
b)	... für Begriffe.....	7
c)	... für Header Felder .....	8
d)	Empfängeradressen umwandeln (nur bei Domainfilterung) .....	9
e)	Gültige Empfänger eintragen (nur bei Domainfilterung) .....	9
3.	Postfach Einstellungen .....	9
a)	Einstellungen.....	9
b)	Kennwort ändern .....	11
c)	externe Postfächer .....	11
4.	SPAM Modul Einstellungen .....	12
a)	Einstellungen.....	12
b)	Aufbewahrungszeiten.....	14
5.	Sonstiges .....	14
a)	Statistik.....	14
b)	Funktionsweise.....	14
c)	Rechner .....	14
III.	Benutzermenü.....	15
a)	Einstellungen.....	15
b)	Kennwort ändern .....	16
c)	Protokolldatei.....	16
d)	Ihr SPAM Postfach .....	17
e)	Spam Postfach zurücksetzen.....	18
f)	Erhaltene Mails zuordnen .....	18
g)	Statistik.....	19

## I. Login

Ihre E-Mail Administration

Geben Sie bitte folgende Informationen ein:

**Für ein einzelnes POP3 oder POP3 Sammelpostfach (auch Testaccount)**

POP3 Postfach

Kennwort

Login Daten als Cookie speichern

**Für eine Mail Adresse innerhalb einer komplett zu prüfenden Domain**

Email Name

Kennwort

Login Daten als Cookie speichern

**Login**

Haben Sie Administratorrechte, geben Sie im ersten Feld (POP3-Postfach) Ihr Postfach-Kürzel „pop00x-xx“ und im zweiten Feld Ihr Kennwort ein. Betätigen Sie den Login-Button, um sich anzumelden. Hierbei haben Sie auch die Möglichkeit Ihre Login Daten über ein „Cookie“ auf Ihrem PC zu speichern. Aktivieren Sie dazu „Login Daten als Cookie speichern“. **Verwenden Sie diese Funktion bitte nur, wenn Sie nur ein Postfach zur Filterung bestimmt haben.** Wenn Sie das nächste Mal auf die Administrationsseite gehen, werden Sie automatisch angemeldet. Falls Sie damit Probleme haben, löschen Sie einfach das entsprechende Cookie in Ihrem Internetbrowser.

Werden alle E-Mail Adressen einer Domain über uns gefiltert, und Sie wollen nur Ihre bzw. Ihre zugewiesenen E-Mail Adressen bearbeiten tragen Sie beim Benutzerkonto im dritten Feld (Email Name) Ihre E-Mailadresse, z.B. vorname.nachname@domain.de und im vierten Feld Ihr Kennwort ein. Betätigen Sie den Login-Button, um sich anzumelden. Weiter geht es dann beim Benutzermenü.

## II. Hauptmenü

### 1. SPAM Modul – Your work

The screenshot shows the 'easyWAN' administration interface. At the top left is the 'easyWAN' logo and a 'Logout' button. At the top right is a 'Neuigkeiten Update: 04.04.2008' link. Below the header is a welcome message: 'Willkommen easyWAN GmbH zur Administration Ihres POP3 Accounts: Cookies löschen'. The main content area is divided into several sections:

- SPAM Modul - Your work**:
  - Erkannte SPAM E-Mails**: Erkannte SPAM-E-Mails bearbeiten.
  - Neue Absender bearbeiten**: Neue Absender bearbeiten.
  - Spam Postfach zurücksetzen**: Hier werden alle erkannten SPAM E-Mails als unqualifiziert eingestuft.
  - Protokoll Datei**: Hier können Sie überprüfen, welches E-Mail wie verarbeitet wurde! Zuerst werden alle zugestellten E-Mails angezeigt.
- Eigene Regeln festlegen**:
  - ... für Absender**: ... hier definieren Sie wie Absender behandelt werden sollen.
  - ... für Begriffe**: ... hier definieren Sie wie Begriffe behandelt werden sollen.
  - ... für Header Felder**: ... hier definieren Sie wie E-Mails mit HEADER Informationen behandelt werden sollen.
- Postfach Einstellungen**:
  - Einstellungen**: Definieren Sie hier Ihre persönlichen Einstellungen, wie Weiterleitungen, E-Mail-Kopien und Abwesenheitsnachrichten.
  - Kennwort ändern**: Hier können Sie Ihr Kennwort neu definieren.
  - externe Postfächer**: Hier können Sie externe Postfächer mit IMAP und POP3 konfigurieren.
- SPAM Modul Einstellungen**:
  - Einstellungen**: Definieren Sie hier Ihre persönlichen Einstellungen.
  - Aufbewahrungszeiten**: Hier können Sie Ihre Aufbewahrungszeiten definieren.
- Sonstiges**:
  - Statistik**: ... beansprucht mehr Rechnerlast, wir bitten daher um ein wenig Geduld.
  - Funktionsweise**: eine Beschreibung wie dieser Filter funktioniert ...
  - Rechner**: Hier erfahren Sie was Sie mit dem SPAM-MAIL-BLOCKER sparen.
- Download**:
  - Auftragsformular**: als PDF.
  - allgemeine Geschäftsbedingungen**: die AGB's des technischen Betreibers.
  - Leistungsbeschreibungen**: die Leistungsbeschreibungen des technischen Betreibers.
  - Produktpräsentation**: des Herstellers als Powerpoint.

#### a) Erkannte SPAM E-Mails

Hier erhalten Sie Informationen darüber, welche E-Mails als SPAM erkannt wurden.

**Zeile rot hinterlegt** Diese Mail wurde vom Absender über das Challenge / Response Verfahren zugestellt. Das System hat Sie darüber informiert, dass Sie den Absender noch einstufen müssen.

**Zeile grün hinterlegt** Bei dieser E-Mail sind Absender und Empfänger gleich. Sie könnte seriös sein. Bitte qualifizieren Sie diese.

**Zeile violett hinterlegt** Diese E-Mail wurde gelöscht entweder wegen enthaltener verdächtiger Links oder weil der versendende Mailserver missbraucht wurde. Innerhalb der Speicherfrist können Sie sich eine solche E-Mail zustellen lassen.

**Zeile blau hinterlegt** Diese E-Mail wurde gelöscht auf Grund der Tatsache, dass sie an mehr als fünfzehn unbekannte Empfänger versandt wurde, sowie weil ihre MD5-Prüfsumme mit vielen anderen eintreffenden E-Mails identisch ist (Massenmail). Innerhalb der Speicherfrist können Sie sich eine solche E-Mail zustellen lassen.

Sie finden oberhalb der Liste eine Wahlmöglichkeit, mit der Sie die Anzahl der angezeigten E-Mails pro Seite variieren können. Standardmäßig sind

- 20 E-Mails pro Seite bei bis zu 1000 SPAM-E-Mails
- 50 E-Mails pro Seite bei über 1000 SPAM-E-Mails

eingestellt. Die Anzahl der Seiten finden Sie rechts daneben. Diese Seiten sind einzeln abrufbar. Je nach Einstellung der Menge (alle, 20, 50, 100, 200, 500) ergibt sich eine andere Anzahl der Seiten. Falls diese Einstellung verändert wird, wird der gespeicherte Wert auch beim nächsten Aufruf der Seite dargestellt. Die aktive Seite erscheint fett. Die Anzahl der Seiten verringert sich bei fortschreitendem Bearbeiten.

Bearbeitung:

Nach dem Anklicken von „Aktion durchführen“ können Sie auf der Bestätigungsseite oben „zum SPAM Postfach“ anklicken, um auf die nächste Seite zu gelangen. So verfahren Sie bis zur letzten Seite, können den Vorgang aber auch durch Klicken auf „Dieses Fenster schließen“ (auf der letzten Seite einzige Möglichkeit) beenden. Die restlichen SPAM-E-Mails bleiben im SPAM-Postfach, bis Sie diese durch erneutes Aufrufen bearbeiten.

Filterkriterien:

### Sortierung

Definieren Sie hier, ob Sie nach Datum (neueste oder älteste zuerst), nach Absender, nach Empfänger, nach Betreff (jeweils alphabetisch) oder nach Filterkriterium sortieren wollen.

### Filter

Hier ist automatisch „spam“ eingestellt, Sie können aber auch „alle E-Mails“ oder „gelöscht“ einstellen. E-Mails aus dem „gelöscht“-Ordner können bei Bedarf als vertrauenswürdig eingestuft und zugestellt werden.

### Finde

Geben Sie einen Begriff ein, der in Absender, Empfänger oder Betreff gesucht werden soll und betätigen Sie „Anfrage absenden“.

### Details anzeigen

Es wird angezeigt, durch welches Kriterium eine E-Mail qualifiziert wurde.

Um eine als Spam erkannte E-Mail trotzdem zuzustellen, wählen Sie den "Radio-Button" „vertrauen“. Dieser Absender wird dann in Ihre Vertrauensliste eingefügt und künftig nicht mehr auf Spam Inhalt überprüft.

Falls Sie nichts verändern und auf "Aktion durchführen" klicken, wird alle anderen E-Mails als "zu löschen" in Ihre Liste eingefügt. In Zukunft werden alle gleichlautenden E-Mails gelöscht.

Mit der **Lupe**  können Sie sich jede E-Mail anzeigen lassen.

### b) Neue Absender bearbeiten

Betätigen Sie den jeweiligen „Radio-Button“ der Rubriken „in Zukunft vertrauen“, „spam“, „löschen“ oder „nichts“ (keine Kategorie) und klicken Sie „Aktion durchführen“, um die eingegangenen E-Mails zu qualifizieren. Wenn Sie das Häkchen in einem Feld in der Überschriftenzeile anklicken, werden alle angezeigten E-Mails nach dieser Kategorie qualifiziert.

vertrauen	= der Absender wird in Ihre Liste der vertrauenswürdigen Absender eingetragen.
spam	= der Absender wird beim nächsten Mal in den Spamordner verschoben.
löschen	= der Absender wird für die Zukunft als zu löschender Absender eingetragen.
nichts	= der Absender wird beim nächsten Mal behandelt, als hätte er noch nie eine E-Mail an den Empfänger geschrieben. Es findet keine Qualifizierung statt.

## c) Spam Postfach zurücksetzen

### Spam Postfach zurücksetzen

[Hilfe](#)

Hier werden alle bisher erkannten SPAM E-Mails als unqualifiziert eingestuft. Diese E-Mails können aber nachwievor auch in der Protokolldatei eingesehen werden.

[zurück zur Auswahl](#)

aktuelles Datum in der Datenbank: 2008-05-06 07:01:08

neues Datum: 2008-05-06 14:07:34

Sollten Sie einmal keine Zeit oder Gelegenheit für die Durchsicht der erkannten Spam-E-Mails haben, benutzen Sie den Button „Spam Postfach zurücksetzen“. Alle darin befindlichen E-Mails werden nach „Aktion durchführen“ daraufhin nicht qualifiziert und bei erneutem Eintreffen als noch unbekannt behandelt. Für die Dauer der Aufbewahrungszeit befinden sie sich jedoch weiterhin in der Protokolldatei.

Damit wird die Gefahr ausgeschlossen, bei der Durchsicht des SPAM-Postfachs versehentlich eventuell doch seriöse E-Mails zu übersehen und zu löschen. Das kann besonders in der Situation eine Hilfe sein, wenn Sie einige Tage keine Gelegenheit hatten, das SPAM-Postfach zu leeren, und sich dadurch eine große Menge E-Mails darin angesammelt hat, Sie aber sich nicht der Mühe unterziehen möchten, dieses zu bearbeiten.

Angezeigt wird das Datum der letzten Bearbeitung sowie das Datum der aktuellen Sitzung.

## d) Protokolldatei

Hier erhalten Sie Informationen darüber, wer Ihnen wann eine E-Mail gesendet hat. So lange das System die gesuchte E-Mail im Speicher hält, können Sie sich diese zustellen lassen, auch wenn sie als SPAM erkannt oder gelöscht wurde.

- **Startdatum**  
Definieren Sie hier, an welchem Datum (24 Stunden) oder von welchem Datum an gesucht werden soll. Dabei können Sie den Zeitraum für den **Monat** und das **Jahr** bestimmen. Standardmäßig ist das aktuelle Datum eingestellt.
- **Finde**  
Geben Sie einen Begriff ein, der in Absender, Empfänger und Betreff gesucht wird.
- **Details anzeigen**  
Es wird angezeigt, durch welches Kriterium eine E-Mail qualifiziert wurde.

Dabei können Sie in folgenden Unterordnern suchen:

- **Alle Mails**  
Es werden alle E-Mails angezeigt, die im angegebenen Zeitraum empfangen wurden.
- **zugestellt (standardmäßige Einstellung)**  
Es werden nur die zugestellten E-Mails angezeigt, die von Absendern empfangen wurden, die von Ihnen noch nicht qualifiziert wurden. In diesen E-Mails wurden keine SPAM Kriterien gefunden.
- **gelöscht**  
Es werden nur die E-Mails angezeigt, die durch das System gelöscht wurden, die also eindeutige SPAM-Kriterien erfüllen.
- **spam**  
Es werden nur die E-Mails angezeigt, die nach SPAM Regeln erkannt wurden und für den Benutzer im SPAM-Postfach zur Qualifizierung vorgehalten werden.
- **vertrauenswürdig**  
Es werden nur die E-Mails angezeigt, die Ihnen als vertrauenswürdig zugestellt wurden.

Haben Sie alle Felder definiert, klicken Sie auf "**Anfrage absenden**".

Kategorien:




**Zeile rot hinterlegt** Diese Mail wurde vom Absender über das Challenge / Response Verfahren zugestellt. Das System hat Sie darüber informiert, dass Sie den Absender noch einstufen müssen.



**Zeile grün hinterlegt** Bei dieser E-Mail sind Absender und Empfänger gleich. Sie könnte vertrauenswürdig sein. Bitte qualifizieren Sie diese.

**Zeile violett hinterlegt** Diese E-Mail wurde gelöscht entweder wegen enthaltener verdächtiger Links oder weil der versendende Mailserver missbraucht wurde. Innerhalb der Speicherfrist können Sie sich eine solche E-Mail zustellen lassen.

**Zeile blau hinterlegt** Diese E-Mail wurde gelöscht auf Grund der Tatsache, dass sie an mehr als fünfzehn unbekannte Empfänger versandt wurde, sowie weil ihre MD5-Prüfsumme mit vielen anderen eintreffenden E-Mails identisch ist (Massenmail). Innerhalb der Speicherfrist können Sie sich eine solche E-Mail zustellen lassen.

Symbole:

-  E-Mail erneut zustellen  
Hier wird Ihnen die E-Mail erneut zugestellt.
-  E-Mail anzeigen  
Hier erhalten Sie ein neues Fenster, in dem die komplette E-Mail in Ihrem ursprünglichen Format angezeigt wird.
-  Absender vertrauen  
Wenn Sie hier klicken, wird dieser Absender als vertrauenswürdig gekennzeichnet. Falls der Absender bereits als zu löschender Absender eingetragen ist, muss dieser zuerst in den Absender-Regeln (2.a) manuell gelöscht werden.

Eine bereits gelöschte E-Mail, die Sie sich zustellen lassen wollen, muss zuerst als vertrauenswürdig qualifiziert werden  , anschließend wählen Sie „E-Mail erneut zustellen“  . Der Absender dieser E-Mail kann künftig ungefiltert E-Mails an Ihr Postfach schicken.

Falls sich noch andere E-Mails des Absenders in der Protokolldatei befinden, werden Ihnen diese automatisch angezeigt. Sie können sie sich ebenfalls zustellen lassen.

## 2. Eigene Regeln festlegen

### a) ... für Absender

#### Absender importieren/exportieren

**Absender importieren / exportieren** [Hilfe](#)

Wählen Sie die Datei:

**Absender** [Hilfe](#)

Anzeige der Anfangsbuchstaben:  [\[Domains anzeigen\]](#) [\[Adressen über Postausgangsserver eingestuft\]](#)

[zurück zur Auswahl](#)

Anzahl aller Datensätze: 27066

Regel entfernen an von	was ist zu tun	Wann / TimeStamp
Neuer Absender	<input type="text"/>	spam
Neuer Absender	<input type="text"/>	spam
Neuer Absender	<input type="text"/>	spam
Neuer Absender	<input type="text"/>	spam
Neuer Absender	<input type="text"/>	spam

### Datei importieren

Übernehmen von eigenen Adressdateien in die Liste der vertrauenswürdigen Absender:

1. Speichern Sie die E-Mail-Adressdatei aus Ihrem Mailprogramm (Outlook, Firefox, etc.) in eine beliebige Datei im Format .csv oder .txt.
2. Wählen Sie den Namen der Datei über „Durchsuchen...“ und klicken Sie anschließend "Datei importieren."

In den nachfolgenden Schritten werden alle E-Mailadressen, die sich in der von Ihnen gewählten Datei befinden, als vertrauenswürdig eingestuft.

### Datei exportieren

Um die Suche nach bestimmten Absenderadressen im SPAM-Postfach für den Administrator zu erleichtern, bietet das System hier eine Exportfunktion. In dieser alphabetisch geordneten Liste werden alle jemals eingestuft Adressen gespeichert. Klicken Sie mit der **rechten Maustaste** auf den Link „Download“ und speichern Sie die erstellte Datei.

„Absender suchen“ Tragen Sie in dem freien Feld eine Absenderadresse ein, die Sie z.B. neu qualifizieren wollen.

„Anzeige der Anfangsbuchstaben“ Setzen Sie das Häkchen in das vorgesehene Feld, bestätigen Sie Ihre Wahl durch die Return-Taste und erhalten Sie eine alphabetische Liste aller Anfangszeichen, über die Sie bestimmte Absender suchen und bearbeiten können.

„Domains anzeigen“ Es werden alle komplett eingestuft Domains angezeigt.

„Adressen über Postausgangsserver eingestuft“ Es erscheint eine Liste all der E-Mail-Adressen, an die Sie selber schon E-Mails geschickt haben, und die dadurch als vertrauenswürdig eingestuft wurden.

„Regel entfernen“ Setzen Sie hier ein Häkchen, wird der entsprechende Absender aus der „vertrauenswürdig“-Liste entfernt, nachdem Sie am Ende der Liste „ändern“ geklickt haben.

### b) ... für Begriffe

[zurück zur Auswahl](#)

	Begriff suchen				
	Wort/Wörter und	Wort/Wörter und	Wort/Wörter und	Wort/Wörter	was ist zu tun
Neuer Begriff	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	spam <input type="button" value="v"/>
Neuer Begriff	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	spam <input type="button" value="v"/>
Neuer Begriff	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	spam <input type="button" value="v"/>
Neuer Begriff	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	spam <input type="button" value="v"/>
Neuer Begriff	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	spam <input type="button" value="v"/>
<input type="button" value="ändern"/>					

Schlüsselbegriffe können als zu löschen, als SPAM oder auch als vertrauenswürdig eingestuft werden. Das Spamfilter-System untersucht die eingehenden E-Mails inklusive Anhänge oder Webseiten-Inhalte (enthaltene Links) auf die eingestellten Begriffe. Auch hier können Sie mithilfe des Suchfensters einzelne Begriffe suchen.

### Bearbeitung:

Wortkombinationen von bis zu vier Begriffen sind möglich:

Eine Buchstabenkombination mit sechs oder weniger Zeichen, die in allen Fällen, also auch z.B. „hot“ in „Paprikaschote“ oder „hotel“, erkannt werden soll, muss im ersten Feld mit einem Leerzeichen davor eingetragen werden! (z.B. „ hot“)

Eine Buchstabenkombination, die nur dann erkannt werden soll, wenn sie von zwei Leerzeichen umgeben ist, muss im ersten Feld ohne Leerzeichen davor eingetragen werden! (z.B. „hot“ ohne Leerzeichen)

Wenn die Klassifizierung aufgehoben werden soll, setzen Sie ein Häkchen vor der betreffenden Zeile. Entscheiden Sie im Auswahlfenster am Ende jeder Zeile, wie der oder die Begriffe klassifiziert werden sollen. Bestätigen Sie Ihre Eingabe mit dem Button „ändern“.

**Wichtig:** Bedenken Sie bei der Klassifizierung von Begriffen oder Buchstabenkombinationen genau, ob diese in jedem Fall nur einer Kategorie (löschen, SPAM, vertrauenswürdig) zuzuordnen sind! Keinesfalls sollten Sie Begriffe wie HTML, Outlook, Microsoft, www, SMTP, POP3 oder andere im Internet gebräuchliche Kürzel oder Warenzeichen einer Klassifizierung unterziehen!

c) ... für Header Felder

Im Header-Feld sind alle Informationen enthalten, die im Zusammenhang mit dem Transport einer E-Mail vom Absender bis zum Empfänger auftreten.

[zurück](#)

	Header Feld	Inhalt	wie behandeln
Neuer Header	<input type="text"/>	<input type="text"/>	spam
Neuer Header	<input type="text"/>	<input type="text"/>	spam
Neuer Header	<input type="text"/>	<input type="text"/>	spam
Neuer Header	<input type="text"/>	<input type="text"/>	spam
Neuer Header	<input type="text"/>	<input type="text"/>	spam

Nutzen Sie diese Option, um Newsletter als vertrauenswürdig einzustufen. Dies ist z.B. dann wichtig, wenn diese von nicht-existierenden oder wechselnden Postfächern versendet werden, die ansonsten vom Spamfilter aussortiert werden würden.

1.) **Beispiel für einen Newsletter:**

- From bounce\_wlw@inxserver.de Thu Jun 5 11:11:13 2008  
Return-Path: <bounce\_wlw@inxserver.de>  
Received: from viruswall-5 (viruswall.easywan.net [195.234.152.5])  
by smtp1.easywan.net (8.12.2/8.12.2/SuSE Linux 0.6) with SMTP id  
m559BBex012468  
for <k.peither@easywan.net>; Thu, 5 Jun 2008 11:11:11 +0200  
Received: From inxmx2.inxserver.de ([213.144.20.3]) by viruswall-5 (WebShield  
SMTP v4.5 MR1a);  
id 1212657057609; Thu, 5 Jun 2008 11:10:57 +0200  
Received: from s101.inxserver.de (s101.inxserver.de [213.144.20.5])  
by mail.inxserver.de (Postfix) with ESMTP id 2AF9A20000F  
for <k.peither@easywan.net>; Thu, 5 Jun 2008 11:10:36 +0200 (CEST)  
Date: Thu, 5 Jun 2008 11:05:35 +0200 (CEST)  
From: Wer liefert was? GmbH <newsletter@wlw.de>  
**Reply-To: Wer liefert was? GmbH <newsletter@wlw.de>**  
To: k.peither@easywan.net  
Message-ID:  
<INX.112db57ac2ddd6c006a56b096e9.85b.1276af.1fe0.11a57f9549f2a.bounce\_  
wlw@inxserver.de>  
Subject: =?ISO-8859-1?Q?Newsletter\_Juni\_-\_Website-Usabili?=  
=?ISO-8859-1?Q?ty\_-\_Nutzen\_Sie\_die\_M=F6glichkeiten?=  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary="-----\_Part\_981829\_24711046.1212657041060"  
X-Mailer: Inxmail EE 3.6, build 080306

Tragen Sie zur Qualifizierung in „Header Feld“ den Namen der Zeile, also z.B. Reply-To (wichtig: **ohne** Doppelpunkt), und in „Inhalt“ den dazu gehörigen Text: Wer liefert was? GmbH <newsletter@wlw.de> ein (In unserem Beispiel fett gedruckt). Wählen Sie dann die Kategorie „vertrauenswürdig“ und klicken auf „ändern“, um die Qualifizierung abzuschließen.



## 2.) Löschen von Begriffen, die in der Betreffzeile enthalten sind

- From MAILER-DAEMON@smtp1.easywan.net Fri Jun 6 11:49:48 2008  
Return-Path: <MAILER-DAEMON@smtp1.easywan.net>  
Received: from viruswall-6 (viruswall.easywan.net [195.234.152.5])  
by smtp1.easywan.net (8.12.2/8.12.2/SuSE Linux 0.6) with SMTP id  
m569nlwN009568  
for <k.peither@easywan.net>; Fri, 6 Jun 2008 11:49:47 +0200  
Received: From 201008133060.user.veloxzone.com.br ([201.8.133.60]) by  
viruswall-6 (WebShield SMTP v4.5 MR1a);  
id 1212745841953; Fri, 6 Jun 2008 11:50:41 +0200  
Received: from [201.8.133.60] (port=  
helo=201008133060.user.veloxzone.com.br)  
by viruswall.easywan.net with esmtp  
id --  
for k.peither@easywan.net; Fri, 06 Jun 2008 06:49:35 --300  
Message-ID: <4849082F.5060701@easywan.net>  
Date: Fri, 06 Jun 2008 06:49:35 --300  
From: "Ellen" <>  
User-Agent: Thunderbird 2.0.0.9 (Windows/20071031)  
MIME-Version: 1.0  
To: "Juliette" <k.peither@easywan.net>  
**Subject: Street casino**  
Content-Type: text/html; charset=ISO-8859-1  
Content-Transfer-Encoding: 7bit

Tragen Sie zur Qualifizierung in „Header Feld“ den Namen der Zeile, also z.B. Subject (wichtig: **ohne** Doppelpunkt), und in „Inhalt“ den dazu gehörigen Text: Street casino oder - falls Sie alle E-Mails, in denen das Wort „casino“ im Betreff auftaucht - %casino% ein. Wählen Sie dann die Kategorie („wie behandeln“) und klicken auf „ändern“, um die Qualifizierung abzuschließen.

Wenn Sie diese Option nutzen, beachten Sie bitte, dass das Filterkriterium nur für die Betreffzeile aktiviert ist, nicht für den Absender oder den Inhalt (Text, Bilder, Links, Anhänge etc.)

d) Empfängeradressen umwandeln (nur bei Domainfilterung)

e) Gültige Empfänger eintragen (nur bei Domainfilterung)

Hier können Sie als Administrator gültige E-Mail-Adressen für eine E-Mail-Adresse innerhalb einer komplett gefilterten Domain festlegen.

## 3. Postfach Einstellungen

a) Einstellungen

### Postfacheinstellungen.

Diese werden 15 Minuten nach der nächsten vollen Stunde (z.B. 13:15 Uhr) aktiv.

[zurück zur Auswahl](#)

#### E-Mail Weiterleitung

[Hilfe](#)

Zieladresse:

wan.net m.peither@intern.easywan.net

#### E-Mail-Kopie

[Hilfe](#)

Zieladresse:

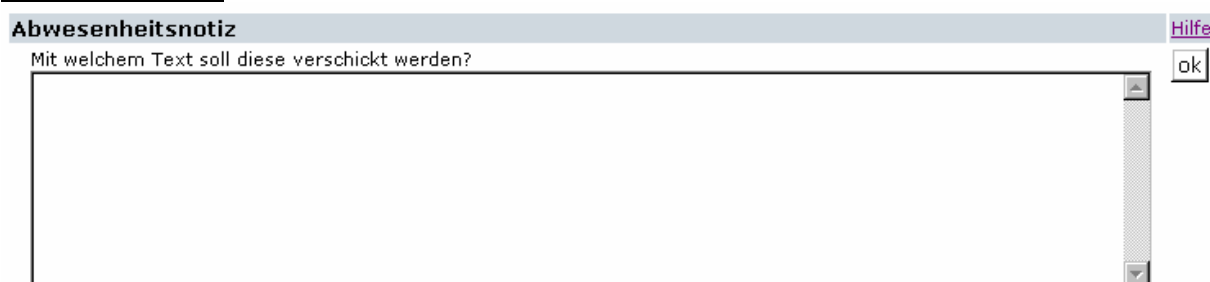
### E-Mail Weiterleitung

Tragen Sie unter „Zieladresse“ die Mailadresse ein, an die Ihre E-Mails weitergeleitet werden sollen. Betätigen Sie den „ok“-Button, um die Einstellung zu aktivieren - achten Sie auf korrekte Schreibweise, da der Absender eine Unzustellbarkeitsnachricht erhält, wenn die angegebene Adresse fehlerhaft ist. Falls mehrere Adressen definiert werden sollen, trennen Sie diese bitte mit einem Leerzeichen.

### E-Mail-Kopie

Tragen Sie unter „Zieladresse“ die Mailadresse ein, an die eine zusätzliche Kopie der eingehenden E-Mails erstellt werden soll. Betätigen Sie den „ok“-Button, um die Einstellung zu aktivieren – achten Sie auf korrekte Schreibweise, da der Absender eine Unzustellbarkeitsnachricht erhält, wenn die angegebene Adresse fehlerhaft ist. Falls mehrere Adressen definiert werden sollen, trennen Sie diese bitte mit einem Leerzeichen.

### Abwesenheitsnotiz



Tragen Sie hier den Text ein, der als Abwesenheitsnotiz versendet werden soll. Dabei erhält jeder Absender nur **eine Notiz**, unabhängig von der Anzahl der E-Mails, die er Ihnen sendet. Sobald Sie einen Text in das Feld eingetrag haben und die eingegeben Werte abspeichern, wird diese Funktion aktiviert.

Um diese wieder zu deaktivieren, markieren Sie das komplette Feld mit <STRG-A> und löschen den kompletten Text. Klicken Sie danach auf "ok" und die Abwesenheitsnotiz ist wieder deaktiviert.

Alle 15 Minuten nach einer vollen Stunde werden die neuen Einstellungen vom System aktualisiert und sind von diesem Zeitpunkt an gültig.

## b) Kennwort ändern

### Kennwort ändern.

Diese Änderung wird erst ab der nächsten vollen Stunde um viertel nach (z.B. 13:15 Uhr) aktiv. Ändern Sie z.B. Ihr Kennwort um 11:23 Uhr, wird dieses tatsächlich erst um 12:15 Uhr geändert. Um sich auf in dieser WebInterface Seite um 11:40 einloggen zu können, brauchen Sie aber bereits Ihr neues Kennwort.

[zurück zur Auswahl](#)

Neues Kennwort

Neues Kennwort wiederholen

Geben Sie Ihr neues Kennwort in das erste Feld ein, bestätigen Sie dieses im zweiten Feld und betätigen Sie „abspeichern“.

Alle 15 Minuten nach einer vollen Stunde werden die neuen Einstellungen vom System aktualisiert und sind von diesem Zeitpunkt an gültig.

Ändern Sie z.B. Ihr Kennwort um 11:32 Uhr, wird dieses tatsächlich erst um 12:15 Uhr geändert. Um sich auf diesem Webinterface auf der Startseite um 11:40 Uhr erneut einloggen zu können, benötigen Sie jedoch bereits das neue Kennwort.

## c) externe Postfächer

Diese Seite benötigen Sie, wenn Sie ein einzelnes Postfach eines Diensteanbieters von SPAM MAIL BLOCKER filtern lassen wollen.

Diensteanbieter	externer POP3 Server	POP3 User	POP3 Kennwort	Abrufintervall	Abrufprotokoll
AOL.com	imap.de.aol.com	Benutzer	0123djd78	15 Min.	IMAP
GMX.DE	pop.gmx.de	Vorname.Nachname@gmx.de	0123djd78	5 Min.	POP3
T-ONLINE	popmail.t-online.de	Vor.Name@t-online.de	0123djd78	5 Min.	POP3
WEB.DE	pop3.web.de	Vorname.Nachname	0123djd78	15 Min.	POP3
YAHOO.DE	pop.mail.yahoo.de	Vorname_Nachname	0123djd78	5 Min.	POP3
HOTMAIL.COM *)	pop3hot.com	Vorname_Nachname@hotmail.com	0123djd78	5 Min.	POP3

Entfernen

externer POP3 Server	POP3 User	POP3 Kennwort	Abrufintervall	Abrufprotokoll
<input type="text"/>	<input type="text"/>	<input type="text"/>	alle 15 Min. ▾	POP3 ▾
<input type="text"/>	<input type="text"/>	<input type="text"/>	alle 15 Min. ▾	POP3 ▾

1.) Suchen Sie Ihren E-Mail-Diensteanbieter in unserer Beispielliste und schreiben Sie den Namen des zuständigen POP3 Servers in das erste Feld.

2.) In das zweite Feld schreiben Sie bitte die vollständige E-Mail-Adresse, die gefiltert werden soll.

3.) In das dritte Feld schreiben Sie dann noch das Kennwort Ihres POP3 Kontos.

4.) Wählen Sie bei „Abrufintervall“ 5 oder 15 Minuten. Bitte ändern Sie „Abrufprotokoll“ nur nach Rücksprache mit uns!

5.) Betätigen Sie den „ok“-Button, um die Einstellung zu aktivieren.

Der SPAM MAIL BLOCKER holt nun Ihre Post von diesem POP3 Postfach ab und überprüft diese nach Ihren Filterkriterien.

## 4. SPAM Modul Einstellungen

### a) Einstellungen

#### Spam Modul aktivieren

Um die Filterung zu aktivieren, muss zunächst der Radiobutton in der ersten Rubrik auf „ja“ gesetzt werden. Alle u. a. Regeln werden über die Radiobuttons „ja“ und „nein“ aktiviert bzw. deaktiviert.

#### Standard Spam Regeln aktivieren

Es werden Schlüsselwörter wie Viagra in den verschiedensten Ausprägungen wie z.B. Vi@gra, Viagra, etc., die im Betreff und im eigentlichen E-Mail vorkommen, abhängig vom Textinhalt (beschränkt auf einen Absatz), erkannt und als SPAM aussortiert.

#### Automatische Berichte

Hier bestimmen Sie, wann und wie oft Ihnen Berichte automatisch per Mail zugestellt werden. In diesen finden Sie z.B. wie viele Emails als SPAM identifiziert wurden oder welche Absender noch zu qualifizieren sind.

Bei Aktivierung können Sie zwischen „täglich“ (Montag bis Freitag) und „wöchentlich“ (jeden Montag) wählen.

#### Virenerkennung

Diese Regel ist nur dann verfügbar, falls die komplette Domain oder Ihr "Schattenpostfach" auf Viren überprüft wird. Falls ein Virus erkannt wird, wird dieser in das Spam Postfach verschoben oder gelöscht, je nach Einstellung unter "was soll mit diesen geschehen". Hierbei werden auch Absender überprüft, die als vertrauenswürdig definiert wurden. Wenn Ihnen bereits vertrauenswürdige Absender einen Virus senden, hat dies keinen Einfluss auf das Regelwerk.

Zusätzlich generiert der SPAM-MAIL-BLOCKER eine E-Mail an den zuständigen Provider (absendende IP-Adresse laut RIPE <http://www.ripe.net>) indem wir ihm mitteilen, dass der PC mit der für ihn zuständigen IP-Adresse einen Virus versendet hat.

Bei „was soll mit den erkannten passieren?“ – wählen Sie zwischen „gelöscht“, damit die betroffene E-Mail komplett gelöscht wird und „spam“, wenn die – von unserem System gereinigte - E-Mail in den Spamordner verschoben werden soll.

**Diese Option tritt nur in Kraft, wenn Sie das Virenerkennungs-Paket bestellt haben.**

#### Erkennung von nicht identifizierbaren Absendern

Der SPAM-MAIL-BLOCKER überprüft mittels des SMTP Protokolls und ggf. einer Kontroll E-Mail ob der Versender einer E-Mail überhaupt existiert. Es hat keinen Sinn, eine E-Mail von einem nicht existierenden Absenders zu empfangen, da Sie darauf auch nicht antworten können. Die vom System versandte E-Mail ist standardisiert (s. „Hilfe“), kann aber in dem dazugehörigen Feld vom Benutzer individuell gestaltet werden. Zur Aktivierung des eigenen Textes klicken Sie bitte unten auf der Seite auf „abspeichern“.

#### Benachrichtigung über SPAM Erkennung an den Absender

Falls eine eingehende E-Mail als SPAM erkannt wurde, wird mit dieser Option eine Antwort-E-Mail an den Absender erzeugt, worin dieser informiert wird, dass seine E-Mail in das SPAM-Postfach verschoben und nicht an den Adressaten zugestellt wurde. Der Absender hat dann die Möglichkeit, mit Hilfe eines Links, Ihnen die E-Mail korrekt zuzustellen. Wenn Sie keinen eigenen Text verfassen möchten, verwendet dieser Automatismus einen Standardtext, welchen Sie in der „Hilfe“ finden.

#### Welche Informationen werden in die E-Mail eingetragen, wenn SPAM erkannt wird?

Im Text der Antwort-E-Mail wird der an dieser Stelle generierte Name eingefügt. Sie können statt mit Ihrem persönlichen Namen auch z.B. mit Ihrem Firmennamen antworten.

#### Ablehnung von sog. Open Relay Servern

Open Relay Server sind Mailserver, die auf Grund ihrer mangelnden Sicherheit von fremden Mailversendern missbraucht werden können. Spamversender nutzen vielfach diese Server für die Verbreitung ihrer Werbe-E-Mails. Wir aktualisieren unsere Kontrollfunktionen ständig, u. a. über [www.ordb.org](http://www.ordb.org).

### Ablehnung von LOG/COMPARE

Diese Regel ist die komplexeste aller hier verwendeten Regeln. Unser Algorithmus berechnet anhand der Beurteilung aller Benutzer des SPAM-MAIL-BLOCKERS die SPAM-Wahrscheinlichkeit einer neuen E-Mail. Daher entscheidet Ihr persönliches „Filter-Verhalten“ mit darüber, wie neue E-Mails insgesamt gefiltert werden.

Der SPAM-MAIL-BLOCKER vergleicht anhand aller Empfänger, Absender, Absender-IP-Adressen, Texte und Links in der E-Mail, wie andere Benutzer des SPAM-MAIL-BLOCKERS diese E-Mail einstufen. Somit erhalten Sie auch keine „neuen E-Mails“ mehr, die bereits andere Benutzer überwiegend als Spam eingestuft haben.

### Selbst lernende Regeln

Der Logarithmus des Filters reagiert auf alle Beurteilungen aller Benutzer. Damit erweitert sich die Treffsicherheit insgesamt. Jeder Benutzer trägt somit direkt zur Qualitätssteigerung des SPAM-MAIL-BLOCKERS bei.

Das hier aktivierte Regelwerk errechnet einen Wahrscheinlichkeitsindex aus den Beurteilungen aller Benutzer. Dabei werden die individuellen Beurteilungen jedes Einzelnen höher priorisiert als die Summe aller Beurteilungen aller Benutzer.

Sie können drei weitere Kriterien hinzufügen, die eine Verschärfung des Filters zur Folge haben, in Einzelfällen aber auch zu einer kritischen Menge an „false-positives“ führen können. Das bedeutet, dass eventuell E-Mails von Absendern, deren Mailserver nicht korrekt konfiguriert sind, fälschlich als SPAM identifiziert werden. Sollten Sie häufig Mails von Ihnen (bzw. Ihrem Mailsystem) unbekanntem Absendern erhalten, könnte es hilfreich sein, die Regeln 1 und 2 **nicht** zu aktivieren.

#### 1. Überprüfung des MX-Eintrags im DNS des versendenden Mailserver

Hier wird überprüft, ob die eingehende E-Mail von einem authentifizierten Mailserver verschickt wurde. Sollte dieser nicht zu identifizieren sein, ist davon auszugehen, dass es sich um eine unerwünschte E-Mail handelt.

#### 2. Überprüfung des SPF-Eintrags im DNS des versendenden Mailserver

Hier wird überprüft, ob der versendende Mailserver SPF-konform konfiguriert ist. SPF bedeutet „Sender Policy Form“ (siehe auch [www.spf.org](http://www.spf.org)) und stellt in der Kommunikation zwischen sendendem und empfangenden Mailserver sicher, dass der Versender von einem identifizierbaren Mailserver versendet. Da SPAMMER ihre Herkunft verschleiern und über nicht registrierte Mailserver versenden, ist das Fehlen eines SPF-Eintrags ein deutlicher Hinweis auf unerwünschte E-Mails.

#### 3. Löschen von E-Mails mit spamverdächtigen Links

Enthält eine E-Mail einen oder mehrere Links, die von der Mehrzahl der Benutzer als SPAM eingestuft wurden, bzw. wurde diese E-Mail an mehr als fünfzehn unbekannte Empfänger versendet, so wird sie vom System als SPAM eingestuft.

Alle Änderungen müssen mit „abspeichern“ bestätigt werden.

### Sortierreihenfolge in der Protokolldatei / erkannte SPAM E-Mails

Bestimmen Sie hier, ob Sie die ältesten oder die neuesten SPAM E-Mails zuerst angezeigt bekommen. Diese Funktion finden Sie für die einzelne Sitzung auch unter „Erkannte SPAM E-Mails / Sortierung“.

### Löschen von eindeutigen SPAM E-Mails

Bestimmen Sie hier, ob Spam E-Mails, die im Filteralgorithmus höherrangig als solche eingestuft werden, direkt gelöscht werden sollen. In der Folge finden Sie weniger E-Mails in Ihrem SPAM Postfach.

TIPP: Falls Sie eingehende E-Mails vermissen, können Sie weiterhin im Ordner Protokolldatei unter „gelöscht“ nach diesen suchen und sie sich ggf. erneut zustellen lassen.

Diese Regel erleichtert die tägliche Kontrolle des SPAM Postfaches, wobei Ihnen über die Protokolldatei trotzdem die Möglichkeit erhalten bleibt, vermisste E-Mails aufzufinden.

Für jede Änderung der Einstellungen Ihres SPAM Postfaches ist es nötig, abschließend entweder auf den „ok“-Button oder auf „abspeichern“ zu klicken.

#### b) Aufbewahrungszeiten

Hier können die Standard-Aufbewahrungszeiten für die eingehenden E-Mails kostenpflichtig erweitert werden. Wählen Sie für die jeweilige Rubrik die gewünschte Dauer im Scrollfenster aus und bestätigen Sie diese mit „ok“ oder „abspeichern“. In der Folge finden Sie ein Kontrollfenster, welches Sie über die monatlichen Kosten informiert.

Sollten Sie nicht an einer Speicherung einzelner Kategorien interessiert sein, können Sie diese auch über die ja/nein-Radio-Buttons deaktivieren. Dies ist bei den „erkannten SPAM E-Mails“ nicht vorgesehen.

### 5. Sonstiges

#### a) Statistik

Diese Seite gibt Ihnen einen Überblick über die vom SPAM-MAIL-BLOCKER erfassten Absender. Die Statistik wird monatsweise geführt. Den Monat und das Jahr wählen Sie in der ersten Zeile, indem Sie den gewünschten Zeitraum in den Fenstern „Monat“ und „Jahr“ einstellen und auf „Anfrage absenden“ klicken.

Die Verteilung zwischen erwünschten und unerwünschten E-Mails sehen Sie rechts oben mit absoluten Zahlen und prozentualen Anteilen.

#### b) Funktionsweise

Anhand der Grafik auf der Webseite [www.spam-mail-blocker.de](http://www.spam-mail-blocker.de) sehen Sie in einer vereinfachten Darstellung, welchen Weg die eintreffenden E-Mails bis zu Ihrem PC bzw. in Ihr SPAM Postfach nehmen. Hier öffnet sich ein eigenes Fenster, welches Sie separat schließen müssen.

#### c) Rechner

Unter Zugrundelegung einer Studie des BSI (Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/literat/studien/antispam/antispam.pdf>) haben wir eine Beispielrechnung für einen Mitarbeiter mit einem durchschnittlichen Stundensatz von Euro 40,00 aufgemacht. Die Rechnung bezieht sich auf einen Monat und beinhaltet ebenso Kosten für Hardware, Traffic und Administration.

## III. Benutzermenü

Willkommen zur Administration Ihres privaten Bereichs

: [Cookies löschen](#)



### [Einstellungen](#)

Definieren Sie hier Ihre persönlichen Einstellungen.



### [Kennwort ändern](#)

Hier können Sie Ihr Kennwort neu definieren.



### [Protokoll Datei](#)

Hier können Sie überprüfen, welches Email wie verarbeitet wurde! Zuerst werden alle zugestellten Emails angezeigt, falls welche vorhanden sind!



### [Ihr SPAM Postfach](#)

Hier können Sie Ihre erkannten SPAM-Mails qualifizieren.



### [Spam Postfach zurücksetzen](#)

Hier werden alle erkannten SPAM E-Mails als unqualifiziert eingestuft.



### [Erhaltene Mails zuordnen](#)

Welche empfangenen E-Mails, von wem, werden wie in Zukunft behandelt!



### [Absender](#)

Hier entscheiden Sie wie Emails von bestimmten Absendern behandelt werden sollen.



[Statistik ... beansprucht mehr Rechnerlast, wir bitten daher um ein wenig Geduld.](#)

### a) Einstellungen

#### Automatische Berichte

Hier bestimmen Sie, wann und wie oft Ihnen Berichte automatisch per Mail zugestellt werden. In diesen finden Sie z.B. wie viele Emails als SPAM identifiziert wurden oder welche Absender noch zu qualifizieren sind.

Bei Aktivierung können Sie zwischen „täglich“ (Montag bis Freitag) und „wöchentlich“ (jeden Montag) wählen.

#### Sortierreihenfolge in der Protokolldatei / erkannte SPAM E-Mails

Bestimmen Sie hier, ob Sie die ältesten oder die neuesten SPAM E-Mails zuerst angezeigt bekommen. Diese Funktion finden Sie für die einzelne Sitzung auch unter „Erkannte SPAM E-Mails / Sortierung“.

#### Welche Sprache wird standardmäßig verwendet?

Hier können Sie zwischen deutsch und englisch wählen. Entsprechend der Einstellung wird auch die tägliche/wöchentliche Benachrichtigungs-E-Mail versendet.

#### Löschen von E-Mails mit eindeutigen Verlinkungen in der E-Mail?

Enthält eine E-Mail einen oder mehrere Links, die von der Mehrzahl der Benutzer als SPAM eingestuft wurden, bzw. wurde diese E-Mail an mehr als fünfzehn unbekannte Empfänger versendet, so wird sie vom System als SPAM eingestuft.

#### Löschen von eindeutigen SPAM-E-Mails

Bestimmen Sie hier, ob Spam E-Mails, die im Filteralgorithmus höherrangig als solche eingestuft werden, direkt gelöscht werden sollen. In der Folge finden Sie weniger E-Mails in Ihrem SPAM Postfach.

TIPP: Falls Sie eingehende E-Mails vermissen, können Sie weiterhin im Ordner Protokolldatei unter „gelöscht“ nach diesen suchen und sie sich ggf. erneut zustellen lassen.

Diese Regel erleichtert die tägliche Kontrolle des SPAM Postfaches, wobei Ihnen über die Protokolldatei trotzdem die Möglichkeit erhalten bleibt, vermisste E-Mails aufzufinden.

#### Welche Informationen werden in die E-Mail eingetragen, wenn SPAM erkannt wird?

Falls eine eingehende E-Mail als SPAM erkannt wurde, wird eine Antwort-E-Mail an den Absender erzeugt, worin dieser informiert wird, dass seine E-Mail in das SPAM-Postfach verschoben und nicht an den Adressaten zugestellt wurde. Der Absender hat dann die Möglichkeit, mit Hilfe eines Links Ihnen die E-Mail korrekt zuzustellen. Im Text Ihrer Antwort-E-Mail wird der an dieser Stelle generierte Name eingefügt. Sie können statt mit Ihrem persönlichen Namen auch z.B. mit Ihrem Firmennamen antworten.

#### Welcher Benutzer darf die SPAM-MAILS bearbeiten?

Wählen Sie hier eine gültige E-Mail-Adresse, wenn Sie einen Vertreter bestimmen möchten, der in Ihrer Abwesenheit Ihr SPAM Postfach pflegt. Wenn Ihr Vertreter einen neuen Absender als vertrauenswürdig eingestuft hat, wird Ihnen die E-Mail ordnungsgemäß zugestellt, Sie müssen ihn

jedoch noch aktiv in die Liste Ihrer vertrauenswürdigen Absender übernehmen. Es genügt dabei, diesem einfach zu antworten.

Für jede Änderung der Einstellungen ist es nötig, abschließend entweder auf den „ok“-Button oder auf „abspeichern“ zu klicken.

## b) Kennwort ändern

### Kennwort ändern.

Diese Änderung wird erst ab der nächsten vollen Stunde um viertel nach (z.B. 13:15 Uhr) aktiv. Ändern Sie z.B. Ihr Kennwort um 11:23 Uhr, wird dieses tatsächlich erst um 12:15 Uhr geändert. Um sich auf in dieser WebInterface Seite um 11:40 einloggen zu können, brauchen Sie aber bereits Ihr neues Kennwort.

[zurück zur Auswahl](#)

Neues Kennwort

Neues Kennwort wiederholen

Geben Sie Ihr neues Kennwort in das erste Feld ein, bestätigen Sie dieses im zweiten Feld und betätigen Sie „abspeichern“.

Alle 15 Minuten nach einer vollen Stunde werden die neuen Einstellungen vom System aktualisiert und sind von diesem Zeitpunkt an gültig.

Ändern Sie z.B. Ihr Kennwort um 11:32 Uhr, wird dieses tatsächlich erst um 12:15 Uhr geändert. Um sich auf diesem Webinterface auf der Startseite um 11:40 Uhr erneut einloggen zu können, benötigen Sie jedoch bereits das neue Kennwort.

## c) Protokolldatei

Hier erhalten Sie Informationen darüber, wer Ihnen wann eine E-Mail gesendet hat. Bei „Startdatum“ können Sie definieren, an welchem Datum (24 Stunden) oder von welchem Datum an gesucht werden soll. Dabei können Sie den Zeitraum für den **Monat** und das **Jahr** bestimmen. Standardmäßig ist das aktuelle Datum eingestellt. Haben Sie alle Felder definiert, klicken Sie auf "**Anfrage absenden**"

Falls die **Zeile rot hinterlegt** ist, wurde diese Mail vom Absender über das Challenge / Response Verfahren zugestellt.

**Zeile grün hinterlegt** Diese Mail wurde von dem gleichen Absender, wie der Empfänger versendet. Diese könnte vertrauenswürdig sein. Bitte qualifizieren Sie diese.

- **Startdatum**  
Definieren Sie hier ein Startdatum, ab wann E-Mails angezeigt werden (siehe oben).
- **Finde**  
Geben Sie einen Begriff ein, der in Absender, Empfänger und Betreff gesucht wird.
- **Details anzeigen**  
Es wird angezeigt, durch welches Kriterium eine E-Mail gefunden wurde.




Dabei können Sie in folgenden Kategorien suchen:



- **Alle Mails**  
Es werden alle E-Mails angezeigt, die empfangen wurden.
- **zugestellt (standardmäßige Einstellung)**  
Es werden nur die zugestellten E-Mails angezeigt, die von Absendern empfangen wurden, die von Ihnen noch nicht qualifiziert wurden. In diesen E-Mails wurden keine SPAM Kriterien gefunden.



- **gelöscht**  
Es werden nur die E-Mails angezeigt, die durch das System gelöscht wurden, also wenn z.B. ein Absender als zu löschender Absender eingetragen wurde.
- **spam**  
Es werden nur die E-Mails angezeigt, die nach SPAM Regeln erkannt wurden.
- **vertrauenswürdig**  
Es werden nur die E-Mails angezeigt, die Ihnen als vertrauenswürdig zugestellt wurden.

Symbole:

-  E-Mail erneut zustellen  
Hier wird Ihnen die E-Mail erneut zugestellt.
-  E-Mail anzeigen  
Hier erhalten Sie ein neues Fenster, in dem die komplette E-Mail in Ihrem ursprünglichen Format angezeigt wird.
-  Absender vertrauen  
Falls Sie hier klicken, wird dieser Absender als vertrauenswürdig gekennzeichnet. Falls der Absender bereits als zu löschender Absender eingetragen ist, muss dieser zuerst manuell gelöscht werden.

Eine bereits gelöschte E-Mail, die Sie sich zustellen lassen wollen, muss zuerst als vertrauenswürdig qualifiziert werden  , anschließend wählen Sie „E-Mail erneut zustellen“  . Der Absender dieser E-Mail kann künftig ungefiltert E-Mails an Ihr Postfach schicken.

Falls sich noch andere E-Mails des Absenders in der Protokolldatei befinden, werden Ihnen diese automatisch angezeigt. Sie können sie sich ebenfalls zustellen lassen.

#### d) Ihr SPAM Postfach

Hier erhalten Sie Informationen darüber, welche E-Mails als SPAM erkannt wurden.

**Zeile rot hinterlegt** Diese Mail wurde vom Absender über das Challenge / Response Verfahren zugestellt. Diese E-Mail kann Ihnen dann nicht erneut zugestellt werden, da der Absender schon dafür gesorgt hat und damit in die Vertrauensliste eingefügt wurde.

**Zeile grün hinterlegt** Diese Mail wurde von dem gleichen Absender, wie der Empfänger versendet. Diese könnte vertrauenswürdig sein. Bitte qualifizieren Sie diese.

Sie finden oberhalb der Liste eine Wahlmöglichkeit, mit der Sie die Anzahl der angezeigten E-Mails pro Seite variieren können. Standardmäßig sind

- 20 E-Mails pro Seite bei bis zu 1000 SPAM-E-Mails
- 50 E-Mails pro Seite bei über 1000 SPAM-E-Mails

eingestellt. Die Anzahl der Seiten finden Sie rechts daneben. Diese Seiten sind einzeln abrufbar. Je nach Einstellung der Menge (alle, 20, 50, 100, 200, 500) ergibt sich eine andere Anzahl der Seiten. Falls diese Einstellung verändert wird, wird der gespeicherte Wert auch beim nächsten Aufruf der Seite dargestellt. Die aktive Seite erscheint fett. Die Anzahl der Seiten verringert sich bei fortschreitendem Bearbeiten.

Bearbeitung:

Nach dem Anklicken von „Aktion durchführen“ können Sie auf der Bestätigungsseite oben „zum SPAM Postfach“ anklicken, um auf die nächste Seite zu gelangen. So verfahren Sie bis zur letzten Seite, können den Vorgang aber auch durch Klicken auf „Dieses Fenster schließen“ (auf der letzten Seite einzige Möglichkeit) beenden. Die restlichen SPAM-E-Mails bleiben im SPAM-Postfach, bis Sie diese durch erneutes Aufrufen bearbeiten.

Filterkriterien:

### Sortierung

Definieren Sie hier, ob Sie nach Datum (neueste oder älteste zuerst), nach Absender, nach Empfänger, nach Betreff (jeweils alphabetisch) oder nach Filterkriterium sortieren wollen.

### Filter

Hier ist automatisch „spam“ eingestellt, Sie können aber auch „alle E-Mails“ oder „gelöscht“ einstellen.

### Finde

Geben Sie einen Begriff ein, der in Absender, Empfänger oder Betreff gesucht werden soll und betätigen Sie „Anfrage absenden“.

### Details anzeigen

Es wird angezeigt, durch welches Kriterium eine E-Mail gefunden wurde.

Um eine als Spam erkannte E-Mail trotzdem zuzustellen, wählen Sie den "Radio-Button" „vertrauen“. Dieser Absender wird dann in Ihre Vertrauensliste eingefügt und künftig nicht mehr auf Spam Inhalt überprüft.

Falls Sie nichts verändern und auf "Aktion durchführen" klicken, wird diese E-Mail als "zu löschen" in Ihre Liste eingefügt. In Zukunft werden alle gleichlautenden E-Mails gelöscht.

Mit der **Lupe** können Sie sich jede E-Mail anzeigen lassen.

## e) Spam Postfach zurücksetzen

### Spam Postfach zurücksetzen

[Hilfe](#)

Hier werden alle bisher erkannten SPAM E-Mails als unqualifiziert eingestuft. Diese E-Mails können aber nachwievor auch in der Protokolldatei eingesehen werden.

[zurück zur Auswahl](#)

aktuelles Datum in der Datenbank: 2008-05-06 07:01:08

neues Datum: 2008-05-06 14:07:34

Sollten Sie einmal keine Zeit oder Gelegenheit für die sorgfältige Durchsicht der erkannten Spam-E-Mails haben, benutzen Sie den Button „Spam Postfach zurücksetzen“. Alle darin befindlichen E-Mails werden nach „Aktion durchführen“ daraufhin nicht qualifiziert und bei erneutem Eintreffen als noch unbekannt behandelt. Für die Dauer der Aufbewahrungszeit befinden sie sich jedoch weiterhin in der Protokolldatei.

Damit wird die Gefahr ausgeschlossen, bei der Durchsicht des Spam-Postfachs versehentlich eventuell doch seriöse E-Mails zu übersehen und zu löschen. Das kann besonders in der Situation eine Hilfe sein, wenn Sie einige Tage keine Gelegenheit hatten, das SPAM Postfach zu leeren, und sich dadurch eine große Menge E-Mails darin angesammelt hat, Sie aber sich nicht der Mühe unterziehen möchten, dieses zu bearbeiten.

Angezeigt wird das Datum der letzten Bearbeitung sowie das Datum der aktuellen Sitzung.

## f) Erhaltene Mails zuordnen

Betätigen Sie den jeweiligen „Radio-Button“ der Rubriken „in Zukunft vertrauen“, „spam“, „löschen“ oder „nichts“ und klicken Sie „Aktion durchführen“, um die eingegangenen E-Mails zu qualifizieren. Wenn Sie das Häkchen in einem Feld in der Überschriftenzeile anklicken, werden alle angezeigten E-Mails nach dieser Kategorie qualifiziert.

vertrauen	= der Absender wird in Ihre Liste der vertrauenswürdigen Absender eingetragen.
spam	= der Absender wird beim nächsten Mal in den Spamordner verschoben.
löschen	= der Absender wird für die Zukunft als zu löschender Absender eingetragen.
nichts	= der Absender wird beim nächsten Mal behandelt, als hätte er noch nie eine E-Mail an den Empfänger geschrieben. Es findet keine Qualifizierung statt.

## Absender

### Absender importieren/exportieren

Absender importieren / exportieren

[Hilfe](#)

Wählen Sie die Datei:

Absender

[Hilfe](#)

Anzeige der Anfangsbuchstaben:  [\[Domains anzeigen\]](#) [\[Adressen über Postausgangsserver eingestuft\]](#)

[zurück zur Auswahl](#)

Anzahl aller Datensätze: 27066

Regel entfernen an von	was ist zu tun	Wann / TimeStamp
Neuer Absender <input type="text"/>	spam <input type="button" value="v"/>	
Neuer Absender <input type="text"/>	spam <input type="button" value="v"/>	
Neuer Absender <input type="text"/>	spam <input type="button" value="v"/>	
Neuer Absender <input type="text"/>	spam <input type="button" value="v"/>	
Neuer Absender <input type="text"/>	spam <input type="button" value="v"/>	

### Datei importieren

Übernehmen von eigenen Adressdateien in die Liste der vertrauenswürdigen Absender:

- Speichern Sie die E-Mail-Adressdatei aus Ihrem Mailprogramm (Outlook, Firefox, etc.) in eine beliebige Datei im Format .csv oder .txt.
- Wählen Sie den Namen der Datei über „Durchsuchen...“ und klicken Sie anschließend "Datei importieren."

In den nachfolgenden Schritten werden alle E-Mailadressen, die sich in der von Ihnen gewählten Datei befinden, als vertrauenswürdig eingestuft.

### Datei exportieren

Um die Suche nach bestimmten Absenderadressen im SPAM-Postfach für den Administrator zu erleichtern, bietet das System hier eine Exportfunktion. In dieser alphabetisch geordneten Liste werden alle jemals eingestuft Adressen gespeichert. Klicken Sie mit der **rechten Maustaste** auf den Link „Download“ und speichern Sie die erstellte Datei.

„Absender suchen“ Tragen Sie in dem freien Feld eine Absenderadresse ein, die Sie z.B. neu qualifizieren wollen.

„Anzeige der Anfangsbuchstaben“ Setzen Sie das Häkchen in das vorgesehene Feld, bestätigen Sie Ihre Wahl durch die Return-Taste und erhalten Sie eine alphabetische Liste aller Anfangszeichen, über die Sie bestimmte Absender suchen und bearbeiten können.

„Domains anzeigen“ Es werden alle komplett eingestuft Domains angezeigt.

„Adressen über Postausgangsserver eingestuft“ Es erscheint eine Liste aller E-Mail-Adressen, an die Sie selber schon E-Mails geschickt haben, und die dadurch als vertrauenswürdig eingestuft wurden.

„Regel entfernen“ Setzen Sie hier ein Häkchen, wird der entsprechende Absender aus der „vertrauenswürdig“-Liste entfernt, nachdem Sie am Ende der Liste „ändern“ geklickt haben.

### g) Statistik

Diese Seite gibt Ihnen einen Überblick über die vom SPAM-MAIL-BLOCKER erfassten Absender. Die Statistik wird monatsweise geführt. Den Monat und das Jahr wählen Sie in der ersten Zeile, indem Sie den gewünschten Zeitraum in den Fenstern „Monat“ und „Jahr“ einstellen und auf „Anfrage absenden“ klicken.

Die Verteilung zwischen erwünschten und unerwünschten E-Mails sehen Sie rechts oben mit absoluten Zahlen und prozentualen Anteilen.