Den mailbox.org-Spamfilter konfigurieren

Hinweis für Business-Kunden: Diese Einstellungen müssen durch Ihren Administrator über die Verwaltung freigegeben werden.

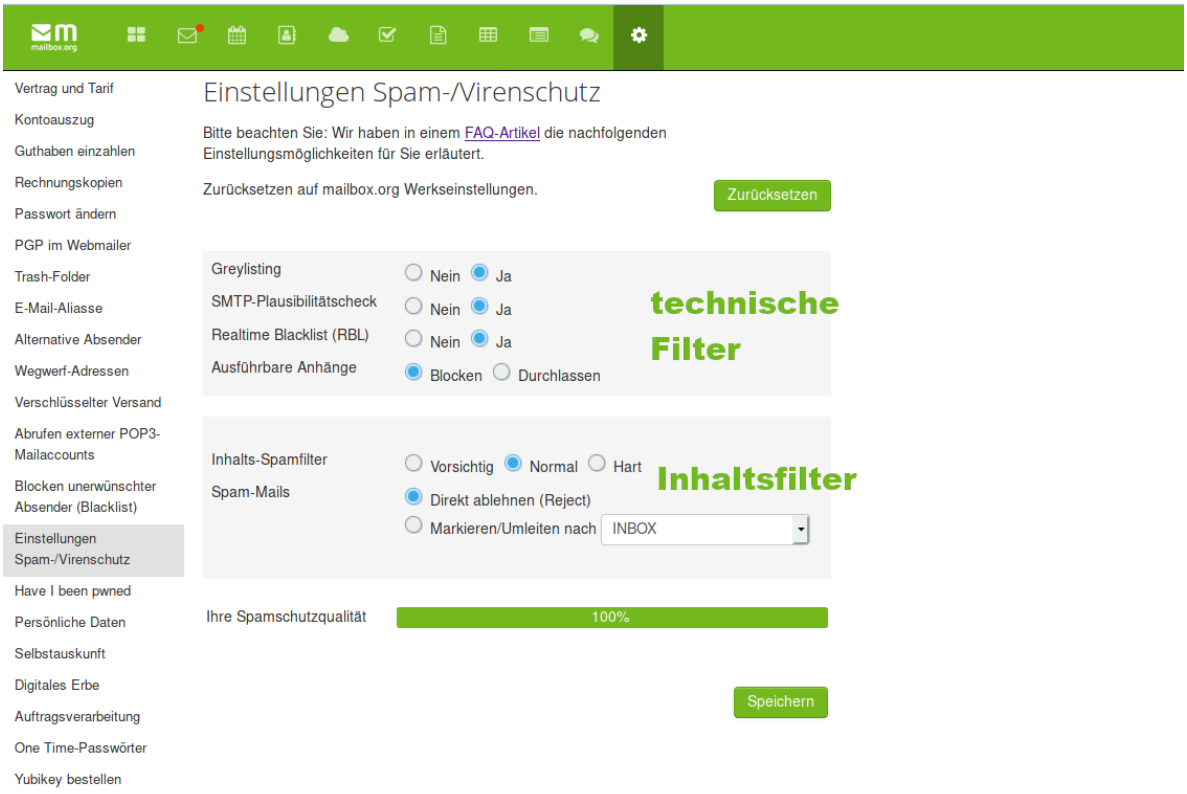
Der Spamschutz bei mailbox.org ist für Sie bereits optimal konfiguriert. Möchten Sie dennoch einzelne Komponenten deaktivieren, informieren Sie sich bitte vorher **hier** über die Funktionsweise der einzelnen Mechanismen. Sie finden die Konfiguration Ihres Spamfilters im Webclient unter „**Einstellungen -> mailbox.org -> Einstellungen Spam- / Virenschutz**“.

Um die nachfolgenden Erläuterungen einfacher zu gestalten, verwenden wir in diesem Artikel folgende Fachbegriffe:

- **Client:** Das System, das sich mit unseren Servern verbindet und versucht eine E-Mail zuzustellen, also ein anderer Mailserver oder ein Spam- / Viren-Botnetz.
- **False Positive:** Eine E-Mail, die zu unrecht als Spam gewertet wurde.
- **False Negative:** Eine Spammail, die nicht erkannt wurde.

Wird eine E-Mail von unseren Systemen als Spam erkannt, so wird diese „**Rejected**“: Unser Server verweigert also die Annahme der E-Mail. In diesem Fall erzeugt das System des Absenders („**Client**“) eine Unzustellbarkeitsbenachrichtigung („**Bounce**“) zurück an den Absender. Dieser erhält also in jedem Fall durch seinen eigenen Provider Kenntnis vom erfolglosen Versuch, seine E-Mail zu versenden. Dieser Bounce-Mechanismus funktioniert genauso, als hätte man versucht, eine E-Mail an einen nicht existierenden Empfänger zu versenden.

Die Einstellungen gliedern sich im Wesentlichen in zwei Bereiche:



Der Bereich "technische Filter" stellt den Bereich dar, der auf Protokollebene stattfindet, also noch bevor der Server die eigentliche Nachricht "sieht"

Der Bereich "Inhaltsfilter" stellt den Bereich dar, der inhaltsbasiert filtert, also nach bestimmten bekannten Mustern in der E-Mail sucht. das ganze passiert ebenfalls noch bevor die Nachricht tatsächlich angenommen bzw. abgelehnt wird. Ob eine als Spam erkannte E-Mail direkt abgelehnt wird oder in einen frei wählbaren Order geschoben wird, können Sie nach Ihrer persönlichen Vorliebe anpassen. Falls Sie den Spam gerne im gleichnamigen Ordner vorfinden möchten, dann wählen Sie „**Junk**“ aus.

Wichtig: Die Optionen im Bereich der technischen Filter führen immer zur Ablehnung (Ausnahme Greylisting, hier erfolgt die Ablehnung nur temporär), wenn sie zutreffen (Also auch, wenn im unteren Bereich eingestellt wird, dass im Inhaltsfilter erkannter Spam in einen Unterordner verschoben werden soll).

Greylisting als Spamschutz

Beim sogenannten „**Greylisting**“ lehnt ein Mailserver Verbindungen bislang unbekannter Clients zunächst temporär ab. Unser Mailserver sendet einmalig ein Besetztzeichen, genau wie bei der belegten Telefonleitung eines Faxgeräts. Nach fünf Minuten darf der Client die E-Mail

erneut einliefern. Sobald er einen erneuten Zustellversuch unternimmt, nehmen wir die E-Mail an. Die eingehende E-Mail wird bei diesem Verfahren also nicht endgültig geblockt oder gar zurückgeschickt, so dass quasi kein Risiko besteht, dass eine E-Mail aufgrund dieser Technik nicht ankommt.

Warum macht man das?

Spammer und (Viren-) Botnetze haben aus verschiedenen Gründen Schwierigkeiten oder kein Interesse daran, mehrere Zustellversuche zu unternehmen. Für normale Mailserver gehört dieses Besetztzeichen jedoch zum Alltag und tritt auch vielmals aus ganz anderen Gründen im Mailtransport auf. Aus bereits erfolgreichen E-Mail-Transaktionen bekannte Mailsysteme werden nicht mehr gegreylisted, so dass über 98% aller „normalen“ E-Mails ohne Verzögerung übermittelt werden.

Zusammenfassung

Risiko, dass versehentlich E-Mails geblockt werden: quasi nicht vorhanden.
Unsere Empfehlung: Greylisting unbedingt aktiviert lassen

SMTP-Plausibilitätscheck

Bei diesem Test überprüfen wir, ob der Hostname des Absenders bzw. Clients (z.B. „Ich bin mailbox.org“), der als Teil der Nachricht übertragen wird, mit der Zeichenkette übereinstimmt, der für diese IP-Adresse als Hostname im DNS hinterlegt ist (dieses Verfahren heißt „Reverse DNS-Lookup“). Laut RFC-Vorschrift müssen diese Zeichenketten bei Mailservern exakt übereinstimmen. Spammer und Botnetze haben jedoch verschiedene Vorteile, wenn sie dort falsche Angaben machen.

In der Praxis kann es in seltenen Fällen Probleme mit authentischen, aber unzulässig konfigurierten Mailservern geben. Falls die Administratoren dieser Mailserver falsche Hostnamen eingetragen haben und noch weitere Faktoren hinzukommen, kann es sogar passieren, dass solch ein Mailserver im Einzelfall geblockt wird.

Der SMTP-Plausibilitätscheck ist eigentlich der einzige Spamtest, der zu „False Positives“ führen kann. Bisher kamen Meldungen von Nutzern über „False Positives“ so gut wie immer durch diesen Check zustande.

Zusammenfassung

Risiko von „False Positives“: gering - aber vorhanden.
Unsere Empfehlung: SMTP-Plausibilitätscheck bei Bedarf deaktivieren (falls Ihnen bestimmte E-Mails nicht zugestellt werden)

Realtime Blacklists (RBL)

RBLs sind öffentlich verfügbare Datenbanken, die Clients enthalten, welche derzeitig durch Versenden von Spam aufgefallen sind. Provider können diese Datenbanken abfragen und so ihre Kunden schützen.
Solche Spam versendenden Clients können beispielsweise vireninfizierte PCs sein, gehackte Server, aber auch Mailserver mit gehackten Nutzer-Accounts. Durch massenhaften Spamversand stellen sie eine Gefahr für alle dar - die Spammails müssen daher geblockt bzw. nicht zugestellt werden.

Wir sehen viele RBLs sehr kritisch, da es unzählige Blacklisten gibt, die oft mit einer fragwürdig aggressiven Politik vorgehen. mailbox.org setzt darum lediglich drei oder vier verschiedene, angesehene RBLs ein, die von fast allen Providern genutzt werden und allesamt extrem vorsichtig vorgehen und nur bei konkret vorhandenen, akuten Vorfällen Clients blacklisten. Keiner der Einträge wird grundlos auf den von uns verwendeten RBLs stehen, aber natürlich könnten sich hier auch „normale“ Mailserver befinden, falls von diesen akut eine Gefährdung durch Spam- oder Virenversand ausgeht.

Zusammenfassung

Risiko von False Positives: sehr, sehr gering.
Unsere Empfehlung: Realtime Blacklists unbedingt aktiviert lassen

Inhaltsspamfilter

Beim Inhaltsspamfilter handelt es sich um die bekannte Software „SpamAssassin“, die die Wahrscheinlichkeit, dass es sich bei einer E-Mail um Spam handelt, anhand ihrer technischen und inhaltlichen Merkmale berechnet. Ist die Wahrscheinlichkeit zu hoch, kann eine E-Mail direkt abgelehnt oder in einen bestimmten Ordner umgeleitet werden.
Folgende Einstellungsmöglichkeiten bieten wir Ihnen:

- **Vorsichtig:** Das Risiko eines False Positives ist kaum noch messbar, aber im Gegenzug kommen vermehrt Spammails („False Negatives“) durch.
- **Normal:** Das Optimum zwischen maximalen, geblockten Spammails und minimalem False Positives-Risiko, gespeist aus jahrelanger Erfahrung. Von uns definitiv empfohlen.
- **Hart:** E-Mails werden bereits sehr niederschwellig als Spam erkannt. Das blockt viele Spammails - das Risiko für False Positives steigt jedoch.

Zusammenfassung

Unsere Empfehlung: Die Einstellung „Normal“ verwenden

Ausführbare Anhänge blocken

Standardmäßig blockiert mailbox.org verdächtige Dateinamen (z.B. doppelte Dateiendungen bei Windows-Programmen), da diese eigentlich stets gefährlich und nicht normal sein können. Außerdem werden ausführbare Dateien geblockt, wenn diese direkt in der E-Mail angehängt wurden. Die Gefahr einer Vireninfektion durch Trick-Mails ist zu hoch. Ausführbare Dateien innerhalb eines .zip-Archivs hingegen werden aufgrund der geringeren Gefährdung durchgelassen. Wenn Sie diesen Mechanismus deaktivieren, erhalten Sie alle Dateianhänge, gleich welchen Typs.

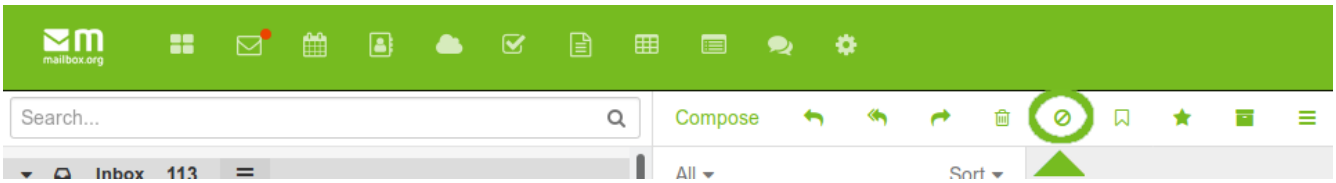
Bitte beachten Sie: Angehängte Dateien, die von namhaften Virenscannern als infiziert erkannt werden, blockieren wir auch weiterhin.

Zusammenfassung

Risiko von False Positives: minimal, betrifft kaum normale E-Mails.
Unsere Empfehlung: Diese Option unbedingt aktiviert lassen, da die Gefahr durch Viren sonst zu groß ist

Anlernbarer Spamfilter

Wenn Sie trotz aller Maßnahmen noch immer Spam erhalten, können Sie einen persönlichen Filter auf einfache Weise anlernen.
Dazu wählen Sie zunächst die entsprechende Nachricht. Klicken Sie nun auf das "Spam"-Symbol:



Alternativ können Sie die Nachricht auch einfach in den Spam-Ordner verschieben, dadurch wird ebenfalls der Lernprozess ausgelöst.
Sollten Sie sich vertan haben, verschieben Sie die Nachricht
einfach wieder aus dem Spam-Ordner in den Posteingang.

Zum Anlernerfolg: der hier angelernte Filter braucht möglicherweise eine gewisse Anzahl an Beispielen, um die Nachrichten zuverlässig als Spam zu erkennen. Der Lernerfolg hängt direkt auch
mit dem Inhalt der Nachrichten zusammen.

Fazit

Die einzige Komponente des mailbox.org-Spamschutzes, die als problematisch angesehen werden kann, ist der SMTP-Plausbilitätscheck. Zu keinem anderen unserer Spamschutzmechanismen liegen uns relevante Support-Tickets vor. **Daher können wir es verstehen, falls Sie den SMTP-Plausibiltätscheck bei Bedarf deaktivieren.**

Wir raten dringend, alle anderen Komponenten aktiviert zu lassen.

Bitte beachten Sie: Ein erfolgreicher Spamschutz basiert immer auf dem Zusammenspiel vieler verschiedener Mechanismen. Nur so kann das Risiko falsch gefilterter E-Mails („False Positives“) gering gehalten werden. Bitte haben Sie Verständnis dafür, dass wir keine Beschwerden über unzureichenden Spamschutz akzeptieren können, falls einzelne Komponenten aus diesem Gesamtwerk deaktiviert wurden.

Verwandte Artikel

- Den Tor-Exit-Node von mailbox.org verwenden
- Team Mail - ehemals Familienaccounts: Freigaben einrichten
- E-Mail-Einrichtung mit Mozilla Thunderbird
- Team Mail - ehemals Familienaccounts: E-Mails teilen
- Wie Spam und Viren bei mailbox.org gefiltert werden