Wie Spam und Viren bei mailbox.org gefiltert werden

Spam- und Virenfilter: unterschiedliche Herangehensweisen

Von anderen E-Mail-Providern kennen Sie vielleicht Spamordner, die Sie regelmäßig durchsuchen müssen um Ihre echte Nachrichten wiederzufinden. Manchmal gibt es auch einen separaten Spam-Quarantäne-Ordner, in den Sie sich regelmäßig einloggen müssen, um Ihre verloren gegangenen Nachrichten wiederzufinden.

Spamhandhabung bei mailbox.org

Standardmäßig ist in Ihrem mailbox.org Account ein derartiges Verhalten deaktiviert. Statt alle fraglichen Nachrichten in einen Spam- oder Quarantäne-Ordner zu verschieben, sind wir in der Lage, Spam- und Virennachrichten in Echtzeit zu filtern. Das bedeutet, die Prüfung findet direkt im Annahmeprozess der jeweiligen E-Mail statt. Zeigt sich, dass es sich bei der betreffenden E-Mail um Spam handelt, so wird die Nachricht von unseren System direkt abgelehnt und die E-Mail geht mit einer Unzustellbarkeitsmeldung (!) zurück an den Absender. Diese Vorgehensweise hat zahlreiche Vorteile:

- Sie (als Empfänger) haben den rechtlichen Vorteil, dass Ihnen nicht Kenntnis der (sich z.B. in Quarantäne befindlichen) E-Mail zugerechnet werden kann.
- Absender und Empfänger haben kommunikative Vorteile, da der Absender sofort erfährt, falls eine Nachricht ihr Ziel nicht erreicht hat.

Sie haben allerdings auch die Möglichkeit, unsere empfohlenen **Spamfilter-Einstellungen nach Ihren persönlichen Vorlieben anzupassen** - eine entsprechende Anleitung gibt es ebenfalls in unseren FAQ. Bitte beachten Sie, dass wir keinen Support für Probleme leisten können, die aus der Veränderung der empfohlenen Einstellungen resultieren - beispielsweise stark erhöhtes Spamaufkommen.

Zur Arbeitsweise unseres Spamfilters

Unser Spamfilter nimmt die Spam-Bewertung im übrigen nur zu einem sehr geringen Maß anhand des Inhalts einer Nachricht vor. Wir bewerten daher hauptsächlich **wer** uns etwas schickt und nur sehr eingeschränkt, **was** er uns schickt. Dabei kommen zahlreiche sich überlagernde Methoden zum Einsatz, die sich gegenseitig ergänzen und damit das optimal mögliche Ergebnis herausholen. Auf diese Methoden werden wir im Abschnitt zu den technischen Hintergrundinformationen (siehe unten) noch vertiefend eingehen.
E-Mails von seriösen Anbietern (wie z.B. eBay, Facebook und vielen anderen) werden nach technischen Merkmalen bewertet. Gerade, wenn sie seriös und uns bekannt sind, gibt es keinen Grund, zu befürchten, dass E-Mails von diesen Anbietern nicht ankommen würden.
Das eigentliche Problem sind Spam-Mails, die über sogenannte „Botnetze“ (z.B. über virenverseuchte Windows-PCs) verschickt werden. Diese haben allerdings sehr charakteristische, technische Merkmale, anhand derer man solche Quellen von echten Mailservern unterscheiden kann.

Links und Empfehlungen

Hier noch einige Links zu weiteren Artikeln, die für Sie interessant sein könnten:

- Wie Sie selbst Veränderungen an den Einstellungen unseres Spamfilters durchführen können, erfahren Sie in dem Artikel „Den mailbox.org-Spamfilter konfigurieren“
- Wenn Sie mehr über die Funktionsweise unseres Spamfilters erfahren wollen, empfehlen wir Ihnen die Lektüre unseres FAQ-Artikels „Warum bekomme ich Spam?“.
- Weitere Argumente und Details zur Frage, ob Spam-Ordner sinnvoll sind, können Sie in unserem Vortrag „Spam-Tagging und Quarantäne - der große Irrtum“ einsehen.
- Falls Sie sich dafür interessieren, wer die Spammer dieser Welt sind, wie Spam funktioniert und wie man mit Spam Geld verdient, dann werfen Sie einen Blick in unseren Vortrag: „Spam mal anders — Wie funktioniert Spam und wer steckt dahinter?“.

Ein paar technische Hintergrundinformationen

Zu den von uns verwendeten Spamfiltertechniken gehört neben dem Einsatz sogenannter „**RBL-Checks**“, durch die bekannte Spam-versendende Mailserver geblockt werden, auch „**Greylisting**“ sowie der Einsatz von **Textmustererkennung**. Durch die Kombination verschiedener charakteristischer Merkmale können wir mit sehr hoher Sicherheit Spam identifizieren und Viren-E-Mails herausfiltern.

RBL-Checks

In den meisten **RBL**s („**R**eal-time **B**lackhole **L**ist“) werden IP-Adressen von Rechnern gelistet, von denen in der Vergangenheit Spam, Viren oder Malware versendet wurden. Unsere Mailserver nutzen ausgewählte Listen zur Spam-Erkennung direkt beim Eingang einer E-Mail. Man kann sich das so vorstellen, als würde der Briefträger von sich aus klar erkennbare Werbeprospekte gar nicht erst in den Briefkasten werfen.

Greylisting

Wird unser Mailserver kontaktiert, um eine E-Mail in Empfang zu nehmen, so werden folgende Angaben überprüft:

1. Die IP-Adresse des versendenden Mailservers
2. Die E-Mail-Adresse des Absenders
3. Die E-Mail-Adresse des Adressaten

Falls unser Mailserver noch nie eine E-Mail von der IP-Adresse des versendenden Mailservers (1) oder von der E-Mail-Adresse des Absenders (2) empfangen hat - oder falls beides zutrifft - dann wird der Zustellversuch durch unseren Mailserver abgelehnt. Der versendende Mailserver erhält die Fehlermeldung, dass ein temporärer Fehler aufgetreten sei. Das führt bei allen vernünftig konfigurierten Mailservern dazu, das die Zustellung nach einer Mindestwartezeit (normalerweise etwa 5 Minuten) erneut versucht wird. Ob und wann ein erneuter Zustellversuch unternommen wird, hängt letztlich allein vom versendenden Mailserver ab.
Wird unserem Mailserver dann erneut eine E-Mail mit der selben Kombination der Daten ((1) und (2)) zugestellt, dann wird diese E-Mail akzeptiert.

Textmustererkennung

Die Textmustererkennung wird mit Hilfe von manuell gepflegten Zeichenketten umgesetzt, anhand derer überprüft wird, ob Textabschnitte der Nachricht mit Elemente bekannter Spam-E-Mails übereinstimmen.
Wenn z.B. eine E-Mail das Textmuster

```
ViAgra for S$le
```

enthält, dann handelt es sich vermutlich um Spam, da sich selten jemand in dieser Form ausdrücken würde.
Die entsprechende Regel zur Filterung könnte dann wie folgt aussehen:

```
/ViAgra for S$le/i REJECT Body-Spamschutzregel 0815
```

Welche Muster wir derzeit zur Spamerkennung verwenden, ist für Administratoren online einsehbar. Technisch versierte oder interessierte Nutzer können einen Blick in den zugehörigen Blogeintrag werfen.

Virenerkennung

Zur Virenerkennung verwenden unsere Systeme vor allem **ClamAV**, einen frei verfügbaren Virenscanner und Phishing-Filter. Wenn unser Mailservern eine E-Mail empfängt, werden die gesamten Daten der E-Mail (also auch Anhänge) auf bekannte Virenmuster geprüft. Sollte es notwendig sein, dann entpacken Virenscanner auch Anhänge (beispielsweise .zip-Dateien), um die enthaltenen Dateien auf Schadcode zu überprüfen.
Falls ein Schadprogramm in der E-Mail gefunden wird, verweigert unser Mailserver die Annahme.

Verwandte Artikel

- Wie Spam und Viren bei mailbox.org gefiltert werden
- Den mailbox.org-Spamfilter konfigurieren
- Meine Sieve-Filter funktionieren nicht
- Kann ich Sieve-Regeln verwenden
- Warum bekomme ich Spam