

Die Aufgabenstellung

Ungewollt zugesandte elektronische Post, im Fachjargon SPAM, hat sich zu einer großen Plage für alle Internet-Teilnehmer entwickelt. Sie verbraucht einen Großteil der Anschlussbandbreite und verstopft nicht selten die Postfächer der Nutzer mit der Folge, dass erwünschte Nachrichten nicht mehr zugestellt werden können oder in der SPAM-Flut untergehen. Die Abwehr von SPAM gleicht einem Hase-Igel-Spiel: SPAM-Autoren ersinnen immer neue Tricks, die erkannt und durch Erarbeitung von Abwehrmechanismen unwirksam gemacht werden müssen. Dabei zeigt sich, dass die SPAM-Flut nur durch Kombination verschiedener Abwehrtechniken einzudämmen ist.

HEAG MediaNet hat einen Service entwickelt, der über eine hohe SPAM-Identifikationsrate verfügt und die identifizierten Nachrichten schon vor dem Übertragungsweg abfängt. Da leider nicht auszuschließen ist, dass gültige Nachrichten als vermeintliche SPAM, so genannte False-Positive, identifiziert werden, erhält jeder Nutzer eines HEAG MediaNet Webmail-Kontos die Möglichkeit, seinen SPAM-Ordner über seinen Webmail-Zugang einzusehen und zu kontrollieren.

HEAG MediaNet SPAM-Filter Funktionsumfang

HEAG MediaNet stellt seinen Freeservice-Kunden die folgenden Anwehrmechanismen zur Verfügung, die vom Kunden selbst über dessen Webmail-Zugang als Gesamtpaket mit folgenden Leistungsmerkmalen ein- oder ausgeschaltet werden können:

- Bereitstellung eines Ordners zur Aufnahme von SPAM-verdächtigen E-Mails.
- Prüfung gegen Realtime Blacklists (RBL)
- Überprüfung der versendenden Server (HELO + SPF)
- Anwendung des RAZOR-Verfahrens
- Anwendung des PYZOR-Verfahrens
- Anwendung des DCC-Verfahrens

Die Nutzung des SPAM-Filters beim Freeservice ist kostenfrei und kann vom Nutzer im HEAG MediaNet Konfigurationscenter aktiviert oder deaktiviert werden. Mit der Aktivierung nimmt der Nutzer zur Kenntnis, dass es keine sichere Vorkehrung gegen SPAM gibt und HEAG MediaNet keine entsprechende Zusicherung abgibt. Weiterhin akzeptiert der Nutzer, dass eine eindeutige Identifikation als SPAM nicht möglich

ist und akzeptiert ebenso die Eigenkontrolle des Ordners, in den die HEAG MediaNet die als SPAM identifizierten Nachrichten verschiebt. Die Allgemeinen Geschäftsbedingungen für „Telekommunikationsdienste + Serviceleistungen“ und die „Leistungsbeschreibung Internetdienste“ der HEAG MediaNet GmbH gelten weiterhin in ihrer jeweils aktuellen Form.

HEAG MediaNet SPAM-Filter im Überblick

Die HEAG MediaNet Lösung kombiniert mehrere Techniken bei der Identifizierung von SPAM. Jede Prüfung beinhaltet die folgend aufgeführten Schritte.

1. HELO-Prüfung

Beim HELO-Verfahren wird gleich zu Beginn der Kommunikation gegen andere Mailserver geprüft, ob es sich um einen gültigen (validen) Kommunikationspartner handelt. Jeder Mailserver meldet sich zu Beginn einer E-Mail Transaktion mit seinem Namen beim anderen Mailserver. Dieser Name muss bestimmte Kriterien erfüllen. Beispielsweise muss der Name, wenn er aufgelöst wird, mit der IP-Adresse des Gesprächspartners übereinstimmen. Wird die IP-Adresse zurück zum Namen aufgelöst, muss der Name wieder in dem Kommando enthalten sein, mit dem die HELO /EHLO Anfrage ausgelöst wurde.

2. Sender Policy Framework

SPF (früher Sender Permitted From), ist eine Technik, die das Fälschen des Absenders einer E-Mail auf SMTP-Ebene erschweren soll. Dazu wird in der DNS-Zone einer Domäne ein so genannter Resource Record vom Typ TXT oder SPF mit Informationen darüber hinterlegt, welche Computer E-Mails für diese Domäne versenden dürfen. Anhand dieser Informationen soll nach RFC 4408 der Empfangs-Server dann sowohl die "MAIL FROM"-Identität als auch die "HELO"-Identität des Senders nachprüfen. Absenderangaben im E-Mail-Header werden nicht überprüft. Ist eine Weiterleitung von beispielsweise gmx.de oder web.de auf einem HEAG MediaNet Account konfiguriert, so wird SPF nicht die gewünschten Ergebnisse liefern, da diese Provider den so genannten Envelope Sender nicht umschreiben und eine legitime E-Mail dann fälschlicherweise von diesen Providern abgelehnt wird.

3. Realtime Blackhole List (RBL)
Als Realtime Blackhole List (RBL) oder DNS-based Blackhole List (DNSBL) werden in Echtzeit (Realtime) abfragbare Schwarze Listen bezeichnet, die verwendet werden, um E-Mail zweifelhafter Herkunft als SPAM zu klassifizieren.

Die Schritte 1–3 lehnen eingehende Nachrichten ab und senden eine Rückweisungsantwort an den Mailserver des Absenders zurück. Damit erhält ein Absender die Chance, seine E-Mail erneut zu senden, die dann beim zweiten Mal die Prüfungen der Schritte 1-3 bestehen wird. Die folgenden Maßnahmen prüfen den Inhalt auf verdächtige Muster und verschieben die Nachricht bei Verdacht in den SPAM-Ordner.

4. RAZOR
Razor basiert auf einem verteilten SPAM-Katalog, der durch Benutzerrückmeldungen ständig aktualisiert wird. E-Mail-Clients und -Server können dadurch bekannten SPAM filtern. Die Erkennung erfolgt über statistische und randomisierte (zufällige) Signaturen. Die Benutzerrückmeldungen werden anhand eines rückgekoppelten Bewertungssystems gewichtet: Benutzer erhalten eine Reputation, die die Zuverlässigkeit ihrer Rückmeldungen bewertet. Die Reputation wird anhand von (übereinstimmenden) Rückmeldungen angepasst.
5. PYZOR
Bei diesem Verfahren handelt es sich um eine in der Programmiersprache Python geschriebene Alternative von RAZOR mit einem eigenen Protokoll und einer leistungsfähigen Datenbank.
6. DCC
Dieser Test prüft eine einkommende E-Mail per Prüfsummenverfahren gegen eine verteilte Datenbank. Haben bereits viele Benutzer eine E-Mail als SPAM markiert, so wird diese auch bei HEAG MediaNet als SPAM eingestuft. Das Besondere an Prüfsummen ist, dass sie auch auf E-Mails zutreffen, die nur in kleinen Teilen geändert wurden.