

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. Da leider nicht auszuschließen ist, dass gültige Nachrichten als vermeintliche SPAM, so genannte False-Positive, identifiziert werden, empfiehlt HEAG MediaNet, die gekennzeichneten Nachrichten durch geeignete Maßnahmen zur Einzelprüfung durch den Nutzer vorzuhalten.

HEAG MediaNet SPAM-Filter Funktionsumfang

Die Nutzung des SPAM-Filters bei Domainpaketen ist kostenfrei und kann für jede über HEAG MediaNet registrierte Domain mit folgenden Leistungsmerkmalen eingerichtet werden:

- Konfiguration der wesentlichen Parameter der beinhalteten Prüfmaßnahme pro Domain durch den Kunden
- Kennzeichnung und Weiterleitung SPAM-verdächtiger E-Mails
- Anwendung der Maßnahmen Realtime Blacklists (RBL), Greylisting, HELO, RAZOR, PYZOR- und DCC
- SPAM Destination (Quarantäne, Tagging)
- SpamAssassin mit Score 5.0 als Standardeinstellung und Spamtagging

Die Nutzung des SPAM-Filters bei Domainpaketen kann vom Nutzer im HEAG MediaNet Konfigurationscenter aktiviert oder deaktiviert werden. Mit der Nutzung 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 Kennzeichnung der als SPAM identifizierten Nachrichten (E-Mail) durch HEAG MediaNet. Der Kunde selbst ist für die Weiterbehandlung der Nach-

richten, insbesondere der markierten, verantwortlich. 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. 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 aufgelöst 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. Greylisting
Greylisting bezeichnet eine Form der SPAM-Bekämpfung bei E-Mails, bei dem die erste E-Mail von unbekanntem Absendern temporär

abgewiesen und erst nach einem zweiten Zustellversuch angenommen wird.

4. **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.
5. **Versanddomain**
Die Domain, die in der Absenderadresse angegeben ist, wird auf Ihre Gültigkeit geprüft. Gültigkeit bedeutet hierbei, ob es einen gültigen MX-Eintrag für die Domain gibt und, ob auch E-Mails zurück gesendet werden können. Sollte das nicht möglich sein, wird geprüft, ob wenigstens ein A-Record vorhanden ist und somit zumindest die Webseite der Domain erreichbar ist.

Die Schritte 1-5 lehnen eingehende Nachrichten ab und senden eine Rückweisungsantwort an den E-Mail Server des Absenders zurück. Damit erhält ein Absender die Chance, seine E-Mail erneut zu senden, die dann beim zweiten Mal die Prüfungen der Schritte 1-5 bestehen wird. Die folgenden Maßnahmen prüfen den Inhalt auf verdächtige Muster und verschieben die Nachricht bei Verdacht in den SPAM-Ordner.

6. **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
7. **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.
8. **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.

9. **SpamAssassin**
Dieses Verfahren bietet Mechanismen, um zwischen erwünschter und unerwünschter E-Mail (HAM und SPAM) zu unterscheiden wie etwa statische Regeln, die auf Basis regulärer Ausdrücke Muster suchen, wie sie typischerweise in SPAM vorkommen.