

Jede Minute werden Millionen von Massen- und Werbemails über das Internet versendet. Wir bieten Ihnen verschiedene Möglichkeiten an, sich vor dieser immer größer werdenden Menge unerwünschter E-Mails zu schützen und damit wertvolle Arbeitszeit für sich und Ihre Mitarbeiter zu sparen.



Greylisting

Greylisting basiert darauf, eine Mail im ersten Zustellversuch abzulehnen, die Sendersadresse zwischenspeichern und erst den zweiten Zustellversuch anzunehmen. Durch dieses Vorgehen wird bereits ein großer Teil der SPAM-Mails gar nicht erst angenommen, da die SPAM-Versender meist nach dem Prinzip "Fire and Forget" arbeiten, d. h. die SPAM-Mails werden nur einmal versandt. Das Prinzip von Greylisting ist mit den RFCs

für E-Mail zu 100% konform, durch den Einsatz dieses Verfahrens gehen keine E-Mail verloren, solange der sendende Mailserver die RFC-Standards einhält.

Systemanforderungen

- ▶ Mailserver: Postfix (wir empfehlen unseren kundenspezifisch aufgebauten Proxy-Server auf Linux-Basis)

SpamAssassin (Open Source)

Der OpenSource-Spamfilter SpamAssassin verwendet zur Erkennung von Spam-Mail ein umfangreiches Regelwerk, das kontinuierlich weiterentwickelt wird. Die Software ist kostenlos für Linux/Unix verfügbar, kommerzielle und freie Portierungen existieren für weitere Betriebssysteme, insbesondere auch für Microsoft Windows.

Da SpamAssassin frei und kostenlos eingesetzt werden kann, bildet es den Kern vieler Weiterentwicklungen, Komplettlösungen und Zusatzmodule für E-Mail-Programme.

SpamAssassin wendet bewährte Methoden zum Filtern von E-Mails an:

- ▶ **Realtime Blackhole Lists (RBL)**
- ▶ **Regelbasierte Filterung nach Mustern im E-Mail-Header**

SpamAssassin überprüft den Absender jeder eingehenden E-Mail gegen "Realtime Blackhole Lists" (RBLs, Listen fragwürdiger Absender). Die RBLs werden beispielsweise

vom "Mail Abuse Prevention System" MAPS verwaltet.

SpamAssassin filtert weiterhin eingehende E-Mails in Bezug auf Spam im Message Header (Absender, Empfänger, Betreff, Typ des Inhalts, Datum, Message ID) und verarbeitet Sie nach den eingestellten Optionen weiter. Zusätzlich können für ausgewählte Absender Ausnahmen definiert werden, so dass Mail von diesen Adressen immer angenommen (Whitelist) oder abgewiesen (Blacklist) wird. So ist es möglich, spezifische Absender als akzeptabel zu definieren, die sonst blockiert würden und umgekehrt.

Weitere Merkmale

- ▶ **Heuristische regelbasierte Filterung nach Mustern in Header und Text der E-Mail**
- ▶ **Lernmöglichkeit durch Berücksichtigung des Absenderverhaltens in der Vergangenheit (Auto Whitelist/Blacklist)**

- ▶ einstellbares Reaktionsverhalten auf als Spam erkannte E-Mail
- ▶ Offene, dokumentierte Struktur mit einfachen Erweiterungsmöglichkeiten

Einsatzszenario

SpamAssassin kann für einzelne Benutzer/Mailboxen oder systemweit für den gesamten Mailserver eingerichtet werden. Auf-

grund der optimalen Unterstützung wird als Systemplattform Unix/Linux empfohlen.

Am Markt werden auch bereits fertig aufgebaute Mailserver-Systeme mit integriertem SpamAssassin angeboten, z. B. Collax Business Server oder tuxGate.

SpamAssassin kann ebenfalls auf dem von enbiz angebotenen, kundenspezifisch aufgebauten Proxy-Server eingesetzt werden.

WatchGuard spamBlocker

In Ergänzung zu WatchGuard Firebox X Firewall-Systemen (Core- und Edge-Reihe) kann WatchGuard spamBlocker als optionales Softwaremodul eingesetzt werden. spamBlocker ist in das WatchGuard LiveSecurity-System integriert, so dass Ihr spamBlocker immer auf dem aktuellsten Stand ist.

So funktioniert spamBlocker

spamBlocker verwendet die führende RPD® (Recurrent Pattern Detection)-Technologie von Commtouch, die das Internet auf bestimmte Muster im globalen E-Mail-Verkehr

scannt und Massen-E-Mails sofort bei Auftreten erkennt. Jede eingehende E-Mail wird von spamBlocker automatisch mit den RPD-Datenzentren abgeglichen. spamBlocker erhält sofort die Information, ob die gerade eingegangene E-Mail in ihrem Muster mit bekannten Massen-E-Mails übereinstimmt und blockiert in diesem Fall die unerwünschte E-Mail.

spamBlocker ist voll in das Management der Firebox integriert, Logging- und Reporting-Funktionen stehen zur Verfügung.

Wir bieten Ihnen folgende Dienstleistungen im Bereich Anti-Spam:

- ▶ Analyse Ihres Mailsystems
- ▶ Auswahl der für Sie geeigneten Anti-Spam-Tools
- ▶ Installation und Konfiguration der ausgewählten Anti-Spam-Tools
- ▶ Tips & Tricks zur Feineinstellung
- ▶ Aufbau kompletter Mail- und Web-Proxy-Server auf Linux-Basis