ADMIN IT-Praxis & Strategie IT Administrator

Freie Software gegen Spam

Markus Feilner, Oliver Frommel

So groß wie das Problem, so unübersichtlich ist das Angebot der freien Anti-Spam-Software. Dieser Artikel gibt einen Überblick über freie Softwareprojekte.

An Spamassassin zwar kommt kein Admin vorbei, der auf der Basis freier Software Spam ausfiltern will. Aber viele Alternativen sind zum Marktführer kompatibel oder als Addon verfügbar, und fast immer verbessert die Kombination die Resultate. Grund genug für eine Marktübersicht der freien Anti-Spam-Softwareprojekte. Den Anfang dieses Artikels machen die Mailserver, gefolgt von Tools für die lokale Zustellung und Erweiterungen für Spamassassin. Sowohl für White-, Black und Greylisting als auch für RBLs existieren zahlreiche nützliche Tools. Ebenfalls einen ganzen Block stellt die lange Liste Alternativen zu Spamassassin dar – abschließend wirft der Artikel einen Blick auf Exoten, die mit ungewöhnlichen Ansätzen antreten oder für andere Szenarien dienen.

Postfix

Wer Spam stoppen will, braucht nicht immer extra Anti-Spam-Software. Die Mailserver Postfix, Sendmail, Exim und Qmail selbst beherrschen bereits von sich aus einige Techniken, die Spammer erfolgreich aussperren lassen. Postfix kennt dafür beispielsweise das Regel-Set der Unsolicited-Commercial-Email-Controls (UCE) [1]. Damit lassen sich schon beim Eingang einer Mail Regeln für Header, Body, IP- und DNS-Adressen, Helo-Namen und vieles mehr definieren und verdächtige Sender abweisen. Ein gut konfigurierter Postfix-Server kann so schon den Großteil der Spam-Mails abweisen. Ein weiteres Mittel der Wahl bei der Spam-Abwehr mit Postfix ist Greylisting per Postgrey (siehe unten)
[2] Postfix UCE-Controls:
http://www.postfix.org/uce.html
http://www.chains.ch/docs/postfix-UCE-HOWTO-de.html
http://jimsun.linxnet.com/misc/postfix-anti-UCE.txt

Sendmail

Auch die aktuellen Versionen von Sendmail kennen zahlreiche Optionen und Features, mit denen der Admin sowohl den Zugriff auf den Server einschränken als auch Antispam-Maßnahmen integrieren kann. Erste Anlaufstelle hier sind die Anti-Relay-Tipps auf der Sendmail-Webseite und die detaillierten Beispiele der Anti-Spam Provisions.
[3] Sendmail: http://www.sendmail.org/tips/relaying.php
http://www.sendmail.org/m4/anti_spam.html

Exim

Der freie Mailer Exim ist unter Debian sehr beliebt und kann dank seiner Access Control Lists ebenfalls schon während der Annahme der Mail nach IPs, Blacklists, Helo-Namen, Sender und Empfänger filtern. Selbstverständlich integriert auch Exim zahlreiche Spamlösungen, wobei Version 4 das deutlich besser löst als die Vorgängerversionen. Dem interessierten Admin helfen die Online-Doku und das Howto weiter.
[4] Exim: http://www.exim.org/exim-html-4.20/doc/html/spec_37.html
http://www.maretmanu.org/homepage/inform/exim-spam.html
http://www.clues.ltd.uk/howto/debian-sa-fprot-HOWTO.html

Qmail

Chris Hardie hat für Qmail ein eigenes Anti-Spam-Howto verfasst, das immer aktuell scheint und einen guten, vollständigen Überblick bietet. Eingebaute Anti-Spam-Mechanismen wie »qmaillocalfilter« und »qmail-spamthrottle« stehen extra Qmail-Anwendungen wie Spamdyke und Simscan zur Seite, die schon bei der SMTP-Verbindung filtern.
[5] Qmail: http://www.chrishardie.com/tech/qmail/qmail-antispam.html
http://www.jfitz.com/qmail-localfilter
http://spamthrottle.qmail.ca/man/qmail-spamthrottle.5.html
http://www.spamdyke.org
http://www.inter7.com/?page=simscan

Lokale Zustellung

Auch beim Ablegen der Mails in lokale Postfächer kann der Admin noch einiges drehen. Sowohl Procmail als auch das Sieve-Protokoll bringen zahlreiche Features mit, die sich fürs Aussortieren, Entfernen, Weiterleiten und Bouncen von Spam-Mails nutzen lassen. Die Uni Köln verwendet gar ein zweistufiges Sieve-Konzept zur Abwehr von Spam, welches ihre Benutzer übers Web-Frontend Smartsieve direkt auf dem IMAP-Server konfigurieren können. Benutzer von POP-Konten greifen auf Tools wie Camel's Eye, Mailfilter oder Popfile zurück.
[6] Procmail: http://www.procmail.org
http://www.spambouncer.org
[7] Sieve: http://www.ietf.org/rfc/rfc3685.txt
http://www.uni-koeln.de/rrzk/mail/software/sieve/spam
[8] Camel's Eye POP3 Email Filter: http://sourceforge.net/projects/camelseye/

[9] Mailfilter POP3 Spam filter: http://mailfilter.sourceforge.net
[10] POPFile: http://getpopfile.org/docs/index.php

Amavis

Amavis sowie sein Nachfolger Amavisd-new sind schon zu den Klassikern in der Spam- und Virenbekämpfung gereift und in jeder modernen Distribution enthalten. Das deutschsprachi ge Postfix Amavisd-Howto enthält alle relevanten Infos, und das Web-Frontend Myamavis von Stefan Palme scheint viel versprechend.
[11] Amavis: http://www.ijs.si/software/amavisd
http://postfix.state-of-mind.de/patrick.koetter/amavisd-new
[12] Myamavis: http://myamavis.kapott.org

Spamassassin

Ohne Frage ist Spamassassin der Platzhirsch unter den freien Anti-Spam-Lösungen. Was aber die wenigsten Linux-Admins wissen: Spamassas sin gibt's auch für Windows, immer aktuelle Regelsätze zur Spamerkennung liefern Projekte wie Rulesdujour oder SARE. Gefällige Web-Oberflächen für Administration sowie die Benutzer stehen unter Horde und Webmin zur Verfügung, und mit dem Spamassassin Coach melden Clients wie Outlook oder Thunderbird direkt Spam an den zuständigen Spamd – während Plugins wie Razor oder Pyzor die Standardfähigkeiten um kollaboratives Filtern erweitern. [13] Spamassassin: http://spamassassin.apache.org
[14] SpamAssassin for Win32: http://sawin32.sourceforge.net
[15] SA Webmin Modul: http://spammin.sourceforge.net
[16] SpamAssassin Coach für Outlook und Thunderbird: http://sourceforge.net/projects/soc2006spamd
[17] Razor: http://razor.sourceforge.net
[18] Pyzor: http://pyzor.sourceforge.net

White-, Black und Greylisting

Auch bei Programmen, die Positiv- und Negativlisten für Benutzer führen oder an Greylisting-Implementierungen hat der Linux-Admin eine große Auswahl. In einer zentralen MySQLDatenbank speichern der Sqlwhite Postfix Policy Server, Sqlgrey, der Greylist Policy Service (GPS) und der Greylist Daemon GLD ihre Listen, während Postgrey eine Berkeley DB verwendet. »milter-greylist« klinkt sich an das Milter-Interface, wie es beispielsweise Postfix oder Sendmail verwenden, unterstützt allerdings noch keine ex terne Datenbank. Mit Tools wie dem Greylisting Proxy Spey ist am Setup des Mailservers keine Änderung notwendig. Denselben Zweck erfüllt Greylite, gemäß der Webseite jedoch vorzugsweise für Qmail.
[19] SQLWhite Postfix Policy Server: http://sourceforge.net/projects/sqlwhite
[20] SQLgrey Postfix Greylisting Service: http://sqlgrey.sourceforge.net
[21] Greylist Policy Service: http://mimo.gn.apc.org/gps
[22] Postgrey: http://postgrey.schweikert.ch
[23] Postgrey: http://www.admin-magazin.de/Das-Heft/2013/03/Spam-durch-Grey-und-Whitelisting-mit-Postgrey-bekaempfen/
[24] Greylist Daemon GLD: http://www.gasmi.net/gld.html
[25] Greylisting Milter: http://hcpnet.free.fr/milter-greylist

[26] Spey: http://spey.sourceforge.net

DNSBL

Der Einsatz von DNS Blacklists verspricht hohe Spam-Erkennungsraten. Dank ihnen lässt sich eine stattliche Zahl an Spam-Mails bereits während des SMTP-Dialoges ausfiltern. Auf der Webseite »Spamlinks.net« finden interessierte immer aktuelle RBL-Listen und Hosts, die solche anbieten. Bei Postfix integrieren die oben erwähnten UCEs [27] die Listen, für Qmail hilft das Antispam-Howto [28] weiter. Wie RBLs am besten bei Sendmail und Exim eingebunden wer den, zeigen die Links hier:
[29] DNSBL http://www.dnsbl.info/
[30] Exim: http://www.exim.org/howto/rbl.html

Alternativen zu Spamassassin

Spamassassin ist nicht allein auf weiter Flur. Die Open-Source-Szene hat einige Alternativen zu bieten, teilweise mit exotischen Features:

- Der Spamfilter Clapf lässt sich sowohl in die Warteschlangen von Postfix integrieren, kann aber auch als LDA laufen und bringt schon Blackholes, Quarantäne und RBLs mit.
  [31] Clapf: http://clapf.acts.hu
- Der bayes-basierte Quick Spam Filter wird von einem MDA aufgerufen und analysiert die E-Mails aufgrund von Erfahrungswerten, die er in einer eigenen Datenbank speichert.
  [32] Quick Spam Filter: http://www.ivarch.com/programs/qsf
- Mailscanner unterstützt zahlreiche Virenund Spamfilter und klinkt sich tief in vorhan dene Mailserver ein. Unter Postfix-Anhängern geniet er deshalb keinen guten Ruf.
  [33] Mailscanner: http://www.mailscanner.info
- Bogofilter ist nach Spamasassin der zweite bekannte Spamfilter, er verwendet statistische Verfahren und kann vom Benutzer oder Admin trainiert werden.
  [34] Bogofilter: http://bogofilter.sourceforge.net
- Mimedefang verwendet die Milter-API von Sendmail, um Spam zu erkennen. Über ein eigenes MIMEdefang-Protokoll übergibt es die zu prüfenden Mails an einen eingebauten Multiplexer, der Spamassassin sowie andere Perl-Skripte verwenden kann.
  [35] Mimedefang: http://www.mimedefang.org
- Den Anti-Spam SMTP Proxy Server (ASSPSMTP) gibt es mittlerweile in der Version 1.3.3.8 – im Zeichen der Schlange integriert sich das Tool wie ein transparenter SMTPProxy in die Kette der Mailserver. Dabei ist die Integration von anderen SpamerkennungsTechnologien wie Spamassassin oder Clamav möglich.
  [36] Anti-Spam SMTP Proxy Server: http://sourceforge.net/projects/assp
- Die beiden statistischen Filter-Programme Spambayes und Dspam wurden initial von zwei Größen der freien Anti-Spam-Szene entwickelt, für Spambayes und seine zahlreichen Plugins steht Paul Graham, für Dspam Jonathan A. Zdziarski. Letzeres kommt mit vollständigen Web- und Konsolentools und integriert bereits umfangreiche Loggingfunktionen.
  [37] Spambayes: http://spambayes.sourceforge.net

[38] Dspam: http://dspam.nuclearelephant.com

- Sagator ist ein Spam Filter Gateway für beliebige SMTP-Server und kann beliebige Filterprogramme aufrufen. In einem Webinterface zeigt das Tool aktuelle Statistiken und die Mails in Quarantäne.
  [39] Sagator: http://www.salstar.sk/sagator

- Controllable Regex Mutilator CRM114 ist nach einem legendären Radiobauteil in Kubricks „Dr. Seltsam“ benannt und behauptet, eine Erfolgsrate von 99,9 Prozent bei der Spamerkennung zu erreichen, ein Wert, den sonst nur die Marketingabteilungen der proprietären Hersteller melden.
  [40] CRM114: http://crm114.sourceforge.net

- Dcc und der zugehörige Dccd erstellen und sammeln Checksummen, die sie an öffent liche Server übertragen. Sie arbeiten nach dem einfachen Prinzip: Je mehr verschiedene Mailserver die gleiche Checksumme bei einer Mail berichten, umso wahrscheinlicher ist die Nachricht Spam. Ein Spamassassin-Plugin vervollständigt das Tool.
  [41] Dcc und Dccd: http://www.dcc-servers.net/dcc

Exoten

Last but not least einige Projekte, die vielleicht etwas andere Ansätze bei der Spam-Bekämpfung aufweisen: Mxallowd zum Beispiel erstellt geschickte Iptables-Regeln basierend auf der Tatsache, dass viele Spammer nur den ersten MX-Eintrag im DNS versuchen und dann aufgeben. Spampal ist ein Open-Source-Spamfilter für Windows, der als lokaler Proxy läuft und so beliebige Mail-Programme unterstützt. Mit Spamcomplaint können Thunderbird-Benutzer Beschwerdemails (Complaints) an SpamAbsender versenden, und so die Benutzer virenverseuchter PCs informieren, eigentlich ein verpöntes Vorgehen. Dann gibt es noch NotesAntiSpam, ein Open-Source-Plugin für Lotus Notes, und Pennypost, ein erster Ansatz eines Bezahlsystems für E-Mails. Das gibt’s sogar schon als Thunderbird-Plugin. Die Währung ist übrigens Rechenzeit.
[42] Mxallowd: http://michael.stapelberg.de/mxallowd
[43] Penny Post: http://pennypost.sourceforge.net/PennyPost
[44] Knujon: http://www.admin-magazin.de/Das-Heft/2010/01/Knujon-unternimmt-rechtliche-Schritte-gegen-das-Spam-Problem/

Spam und IPv6

Der Einsatz von IPv6 auf Mailservern ist heute technisch kein Problem mehr, erfordert jedoch dennoch eine besondere Herangehensweise, auch beim Spam-Schutz.
[45] Spamschutz in Zeiten von IPv6: http://www.admin-magazin.de/Das-Heft/2012/02/Mailserver-und-Spamschutz-in-Zeiten-von-IPv6/