Mit Open Source-Tools Spam und Viren bekämpfen

Mit Open Source-Tools Spam und Viren bekämpfen

Peter Eisentraut & Alexander Wirt

O'REILLY®

Beijing · Cambridge · Farnham · Köln · Paris · Sebastopol · Taipei · Tokyo

Kommentare und Fragen können Sie gerne an uns richten:
O'Reilly Verlag
Balthasarstr. 81
50670 Köln
Tel.: 0221/9731600
Fax: 0221/9731608
E-Mail: kommentar@oreilly.de

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über *http://dnb.ddb.de* abrufbar.

Lektorat: Volker Bombien, Bonn
Fachliche Unterstützung: Sven Riedel, Hannover, Joachim Wieland, Aachen, Ingo Strauß, Dortmund
Korrektorat: Sibylle Feldmann, Düsseldorf
Satz: Finn Krieger, Wuppertal
Umschlaggestaltung: Ellie Volckhausen, Boston
Produktion: Karin Driesen, Köln
Belichtung, Druck und buchbinderische Verarbeitung:
Druckerei Kösel, Krugzell; www.koeselbuch.de

ISBN 3-89721-377-X

Dieses Buch ist auf 100% chlorfrei gebleichtem Papier gedruckt.

Inhalt

Vorwort

Spam und Viren sind die Plagen des Internets. Jede zweite E-Mail im Internet beinhaltet entweder unerwünschte Werbung oder versucht, Schaden auf dem Rechner des Empfängers anzurichten. Dieses Buch behandelt die Bekämpfung dieser Heimsuchungen mit Open Source-Software.

Zielgruppe

Dieses Buch richtet sich primär an die Administratoren von E-Mail-Systemen in kleinen, mittleren und großen Netzwerken. Es wird davon ausgegangen, dass der Leser grundlegende Erfahrungen mit der Administration eines Mailservers hat und die Konzepte von E-Mail kennt.

Dieses Buch soll keine Softwaredokumentation ersetzen. Es soll vielmehr dabei helfen, Konzepte zu erarbeiten, sinnvolle Vorgehensweisen zu entdecken und diese dann mit den passenden Werkzeugen umzusetzen.

Struktur dieses Buchs

Dieses Buch besteht aus 14 Kapiteln und den Anhängen A bis C. Die ersten zwei Kapitel bieten eine allgemeine Einführung.

Kapitel 1, Einführung
: Definiert, was Spam und Viren sind, und gibt einen Überblick über deren Ursachen und Konsequenzen.

Kapitel 2, Strategien gegen Spam und Viren
: Gibt einen konzeptionellen Überblick über die möglichen Strategien gegen Spam und Viren.

Die folgenden Kapitel stellen konkrete Softwarelösungen gegen Spam und Viren vor.

Kapitel 3, Spam- und Virenabwehr mit Postfix, Exim und Sendmail
Erklärt Maßnahmen gegen Spam und Viren, die in den genannten Mail Transport Agents implementiert werden können.

Kapitel 4, SpamAssassin
Stellt das mächtige Spam-Erkennungspaket SpamAssassin vor.

Kapitel 5, DNS-basierte Blackhole-Lists
Stellt ein Verfahren vor, bei dem im Internet schwarze Listen zusammengestellt werden, mit deren Hilfe man bekannte Absender von Spam und Viren blockieren kann.

Kapitel 6, Zusätzliche Ansätze gegen Spam
Stellt verschiedene weitere Ansätze gegen Spam vor, die über die üblichen regelbasierten Systeme hinausgehen. Dazu gehören das Greylisting, verteilte Spam-Erkennung mit DCC und Pyzor, sowie Systeme, die die Fälschung von Absendern unterbinden wollen, wie SPF und Yahoo Domain-Keys.

Kapitel 7, Virenscanner
Behandelt den Einsatz von Virenscannern auf Mailservern und stellt den Open Source-Virenscanner ClamAV vor.

Kapitel 8, AMaViS
Stellt das E-Mail-Filter-Framework AMaViS vor, das Spam- und Virenerkennung vereint und viele weitere Konfigurationsmöglichkeiten bietet.

Kapitel 9, MailScanner
Stellt das E-Mail-Filter-Framework MailScanner vor, das ebenfalls die Spam- und Virenerkennung abwickeln und flexibel konfiguriert werden kann.

Kapitel 10, MIMEDefang
Stellt ein umfangreiches E-Mail-Filter-Framework für Sendmail vor.

Kapitel 11, E-Mail-Clients
Behandelt Softwarelösungen, die zur Filterung von E-Mail auf dem Client-Rechner eingesetzt werden können. Daneben wird auch erklärt, wie die verbreiteten E-Mail-Clients sicher konfiguriert und zur Filterung von E-Mail eingesetzt werden können.

Kapitel 12, Procmail
Gibt eine Einführung in das Programm Procmail zur Filterung von E-Mail und stellt eine Reihe von Rezepten vor, die zur Erkennung von Spam und Viren dienen können.

Die letzten zwei Kapitel betrachten die Thematik von einer nicht-technischen Seite:

Kapitel 13, Regeln für Nutzer im Umgang mit Spam und Viren
Enthält einige Regeln und Richtlinien dazu, wie Nutzer durch ihr Verhalten die Gefahr durch Spam und Viren eindämmen können.

Kapitel 14, Juristische Aspekte beim Einsatz von Spam- und Virenfiltern
: Betrachtet die rechtliche Situation von Spam und Viren sowie mögliche juristische Probleme bei der E-Mail-Filterung.

Anhang A erklärt kurz das SMTP-Protokoll. Anhang B bietet eine kleine Einführung in reguläre Ausdrücke. Anhang C listet die Bezugsquellen der verwendeten Software auf.

Software und Bezugsquellen

In vielen Büchern, die irgendeine Software behandeln, wird viel Platz dafür verwendet zu erklären, wie die Software zu installieren sei. Das ist in diesem Buch nicht der Fall und wäre bei einem guten Dutzend Softwarepaketen auch ein erheblicher Platzaufwand. Unserer Erfahrung nach wird die meiste Software gar nicht direkt aus dem Quellcode installiert. »Gibt es dafür ein Paket?«, ist eine viel häufigere Frage als: »Wie installiert man das?«. Aus diesem Grund haben wir in Anhang C die Antworten auf erstere Frage zusammengetragen: eine Auflistung, die Ihnen sagt, für welches freie Betriebssystem welche Software als Paket oder Port verfügbar ist. Außerdem finden Sie dort eine URL zur Website des jeweiligen Softwareprojekts. Für Software, die nicht als Paket erhältlich ist, weil sie noch zu neu, zu unbekannt oder zu klein ist oder nur kommerziell erhältlich ist, haben wir im Text die URL zur Website aufgeführt und verweisen bezüglich Installationsanleitungen dorthin.

Typografische Konventionen

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

Kursivschrift
: Wird für Namen von Dateien, Verzeichnissen sowie für URLs verwendet.

`Nichtproportionalschrift`
: Wird für Namen von Befehlen und Programmen sowie für Codeteile, Codebeispiele und Systemausgaben verwendet.

`Nichtproportionalschrift kursiv`
: Wird in Codebeispielen für Platzhalter dort verwendet, wo Sie selbst eigene Werte einsetzen müssen.

Dieses Symbol kennzeichnet einen Hinweis, der eine nützliche Bemerkung zum nebenstehenden Text enthält.

Dieses Symbol kennzeichnet eine Warnung, die sich auf den nebenstehenden Text bezieht.

Danksagungen

Dank geht an alle Mitarbeiter der credativ GmbH, die uns während der Produktion dieses Buchs ausgehalten und unterstützt haben.

Joachim Wieland hat als technischer Gutachter gearbeitet. Die nützlichen Tipps und Erfahrungen, die er stets mit uns geteilt hat, haben das Buch erheblich aufgewertet.

Ingo Strauß war bei der Recherche für das Kapitel über die juristischen Aspekte der Spam- und Virenfilterung behilflich. Die in diesem Kapitel zusammengetragenen, auch für uns teilweise überraschenden Erkenntnisse wären ohne seine Hilfe nicht zu Stande gekommen.

Volker Bombien war der Lektor bei diesem Buch und hat uns stets geduldig, aber bestimmt auf das Ziel zugesteuert. Durch seine Ideen wurde das Gesamtbild dieses Buchs maßgeblich mitgeprägt.

Wir bedanken uns bei allen Entwicklern von freier Software, ohne die dieses Buch freilich nicht möglich gewesen wäre.