

Peer Heinlein

# Das Postfix-Buch

Sichere Mailserver mit Linux

3., aktualisierte und erweiterte Auflage

Copyright (C) Open Source Press

# Inhaltsverzeichnis

<b>I Grundlagen</b>	<b>27</b>
<b>1 Funktionsweise eines Mailservers</b>	<b>29</b>
1.1 SMTP und POP3/IMAP	30
1.2 SMTP – die Sprache der Mailserver	30
1.3 „Virtuelle“ Mailadressen	32
1.4 „Relayende“ Mailserver	33
1.5 UUCP-Gateways	33
1.6 Weitere Wünsche	34
1.7 Fachbegriffe	34
<b>2 Parlez-vous RFC?</b>	<b>37</b>
2.1 SMTP richtig sprechen	38
2.1.1 SMTP-Kommandos	38
2.1.2 SMTP-Antworten des Servers	42
2.2 Enhanced Status Notifications (ESN)	45
2.3 Delivery Status Notifications (DSN)	47
2.4 Local Mail Transfer Protocol (LMTP)	48
2.5 Mailheader richtig lesen und setzen	48
2.5.1 Die Headerfelder im Einzelnen	51
2.5.2 Der Unterschied zwischen Sender: und From:	53
2.5.3 Der Unterschied zwischen To:, CC: und BCC:	55
2.6 E-Mails und Zeichensätze	56
2.6.1 Die Zeichensatzdefinition im Mailheader	56
2.6.2 Headerzeilen dürfen nur 7-Bit-Zeichen haben!	57

2.7	Dateien und Attachments . . . . .	58
2.7.1	uudecode/uuencode . . . . .	58
2.7.2	MIME-Attachments . . . . .	59
2.7.3	Attachments sind hier uninteressant . . . . .	60
<b>II</b>	<b>Postfix starten</b>	<b>63</b>
<b>3</b>	<b>Installation und Schnellstart</b>	<b>65</b>
3.1	Installation der Programme aus fertigen Paketen . . . . .	65
3.1.1	Postfix finden . . . . .	67
3.2	Besonderheiten und Unterschiede der Distributionen . . . . .	68
3.2.1	Eigenheiten von SUSE – Start von Postfix . . . . .	68
3.2.2	Besonderheiten bei Debian . . . . .	73
3.2.3	Besonderheiten bei Ubuntu . . . . .	75
3.3	Die Postfix Grundkonfiguration . . . . .	76
3.3.1	Postfix-Variablen . . . . .	76
3.3.2	Vorsicht: Doppelte Variablen in der <code>main.cf</code> . . . . .	77
3.3.3	Postfix anpassen . . . . .	79
3.3.4	Die Pfade . . . . .	85
3.4	Läuft Postfix? . . . . .	86
3.5	<code>soft_bounce</code> : Sicher Konfigurationsänderungen vornehmen . . . . .	89
<b>4</b>	<b>Das modulare Konzept von Postfix</b>	<b>91</b>
4.1	Die Erfahrungen mit Sendmail . . . . .	91
4.2	Module müssen her! . . . . .	92
4.3	Die Arbeitsabläufe in Postfix . . . . .	92
4.3.1	Einlieferung durch SMTP . . . . .	93
4.3.2	Einlieferung durch lokalen Programmaufruf . . . . .	94
4.3.3	<code>cleanup</code> und <code>trivial-rewrite</code> sorgen für Ordnung im Header . . . . .	96
4.3.4	<code>(n)qmgr</code> regelt den Rest . . . . .	96
4.3.5	Die eigentliche Zustellung . . . . .	98
4.4	Der Chef des Ganzen und seine <code>master.cf</code> . . . . .	98
4.4.1	Details der <code>master.cf</code> . . . . .	99

---

4.5	Der systematische Überblick . . . . .	101
<b>5</b>	<b>Tägliche Arbeit: Lookup Tables und Postfix-Tools</b>	<b>105</b>
5.1	Von Tabellen und Datentypen . . . . .	105
5.1.1	postmap kümmert sich um hash und btree . . . . .	109
5.1.2	Reload, Restart – oder gar nichts? . . . . .	109
5.1.3	hash oder btree? . . . . .	110
5.2	Die einzelnen Tabellen im Überblick . . . . .	110
5.2.1	aliases: Wer bin ich? . . . . .	110
5.2.2	virtual: Weiterleitungen und virtuelle Mailadressen	112
5.2.3	canonical-Tabelle: Ich versteck' mich . . . . .	116
5.2.4	generic-Tabelle: Umschreibung bei ausgehenden E- Mails . . . . .	119
5.2.5	transport-Tabelle: Abweichende Zustellung . . . . .	120
5.2.6	relocated-Tabelle: Empfänger verzogen . . . . .	122
5.2.7	access-Tabelle: Wer darf, wer darf nicht? . . . . .	123
5.2.8	Header-, Body- und MIME-Checks: Mail filtern . . . . .	128
5.3	Die Datenquellen im Überblick . . . . .	129
5.3.1	Lokale Dateien: DBM mit hash und btree . . . . .	130
5.3.2	Wenn es um Subnetze geht: cidr . . . . .	132
5.3.3	RegExp – das unbekannte Wesen . . . . .	133
5.3.4	Perl Compatible Regular Expressions (PCRE) . . . . .	136
5.3.5	Network Information Service (NIS) . . . . .	136
5.3.6	MySQL . . . . .	137
5.3.7	Lightweight Directory Access Protocol (LDAP) . . . . .	140
5.3.8	proxy: Der Lookup-Table-Proxy . . . . .	142
5.3.9	Weitere Datenquellen . . . . .	142
5.4	Die weiteren Tools . . . . .	143
5.4.1	postmap – Herrscher über alle Lookup Tables . . . . .	143
5.4.2	postconf – Herrscher über alle Parameter . . . . .	145
5.4.3	postsuper – Herrscher über die E-Mails . . . . .	146
5.4.4	postqueue – Herrscher über die Mail-Queue . . . . .	147
5.4.5	postcat – Mails aus der Queue lesen . . . . .	148
5.4.6	postfix – The master himself . . . . .	149

<b>6</b>	<b>DNS-Einträge und redundanter Mailempfang</b>	<b>151</b>
6.1	Das Domain Name System (DNS) für Mailserver . . . . .	151
6.1.1	Die Zonen-Einträge für einen Mailserver . . . . .	152
6.1.2	Beachtenswertes bei der DNS-Konfiguration . . . . .	154
6.2	Mehrere Mailserver für eine Domain? . . . . .	156
6.2.1	Backup über Store-and-Forward . . . . .	156
6.2.2	Mailrouting am MX-10 vorbei . . . . .	158
6.2.3	Gemeinsam genutzte Dateisysteme . . . . .	159
6.2.4	Tipps aus der Praxis . . . . .	160
<b>7</b>	<b>Fehleranalyse</b>	<b>161</b>
7.1	Vorgehensweise und Hilfsmittel . . . . .	162
7.2	Fehlersuche als Admin auf dem Server . . . . .	164
7.2.1	Fehler bei der Annahme/Abholung von Mails . . . . .	164
7.2.2	Fehler bei der Bearbeitung und Zustellung von Mails . . . . .	169
7.2.3	Weitere Fehler . . . . .	173
7.3	(Fern-)Fehlersuche beim Kunden . . . . .	174
7.3.1	Den Fehler einkreisen: Seien Sie Pessimist . . . . .	175
7.3.2	Die beliebtesten Fehler . . . . .	175
7.4	Postfix Debug-Modus . . . . .	178
7.4.1	Logfile-Debugging einzelner Verbindungen . . . . .	178
7.4.2	Logfile-Debugging einzelner Module . . . . .	180
7.4.3	Echtes Debugging . . . . .	180
<b>III</b>	<b>Postfix im praktischen Einsatz</b>	<b>183</b>
<b>8</b>	<b>Die Restrictions – das Hirn von Postfix</b>	<b>185</b>
8.1	Schutz durch Restrictions . . . . .	186
8.1.1	So werden Restrictions durchlaufen . . . . .	188
8.1.2	Der Blinddarm von Postfix . . . . .	190
8.1.3	Der Einstieg am lebenden Beispiel . . . . .	191
8.2	Alle Prüfungen auf einen Blick . . . . .	193
8.2.1	Endgültige Entscheidungen . . . . .	193
8.2.2	Relaying erlauben oder verbieten . . . . .	194

8.2.3	White- und Blacklisting . . . . .	196
8.2.4	Anforderungen an Mailadressen . . . . .	197
8.2.5	Anforderung an den HELO und Client-DNS . . . . .	199
8.2.6	Protokollverstöße . . . . .	200
8.2.7	Debugging und andere besondere Parameter . . . . .	201
8.2.8	Verisign: Der Müllplatz der Geschichte . . . . .	202
8.3	Weitere Prüfungen außerhalb der Restrictions . . . . .	203
8.4	Postfix will kein „Open Relay“ sein . . . . .	203
8.5	Verstehen Sie die Restrictions! Schreiben Sie sich welche! . . . . .	205
8.5.1	Aufgabenstellung . . . . .	206
8.5.2	Die Vorgehensweise . . . . .	207
8.5.3	Wenn Sie glauben fertig zu sein. . . . .	208
8.6	Backup MX 20 – oder: Das Insel-Problem . . . . .	208
8.7	Do and Don't . . . . .	210
8.8	Eine Musterlösung . . . . .	212
8.9	Zu unflexibel? . . . . .	213
8.10	Ein allerletzter Tipp . . . . .	213
<b>9</b>	<b>Wenn's komplizierter wird: Postfix Policy Delegation</b>	<b>215</b>
9.1	Das Policy Delegation Protocol . . . . .	216
9.2	Greylisting . . . . .	218
9.2.1	So funktioniert Greylisting . . . . .	219
9.2.2	Wollen Spammer überhaupt Greylisting überleben? . . . . .	221
9.2.3	Spammer haben es bereits getestet . . . . .	222
9.2.4	E-Mails dürfen nicht verzögert werden! . . . . .	223
9.2.5	postgrey installieren . . . . .	225
9.2.6	Greylisting ist ein hervorragender Virenschutz! . . . . .	228
9.2.7	Die Grenzen von Greylisting . . . . .	228
9.3	policyd-weight . . . . .	228
9.3.1	Prüfungen . . . . .	229
9.3.2	Installation . . . . .	231
9.3.3	Logmeldungen . . . . .	232
9.3.4	False Positives . . . . .	233
9.4	policyd . . . . .	235

<b>10 Spamschutz mit Postfix-Bordmitteln</b>	<b>237</b>
10.1 „In zwei Jahren von heute an ist das Spam-Problem gelöst.“	238
10.2 Wie mit Spam Geld verdient wird	240
10.3 Wie Spam versendet wird	242
10.3.1 Botnetze	242
10.3.2 Formular-Spam	243
10.3.3 Bullet-Proof-Server	243
10.4 Wie Spammer an Mailadressen kommen	245
10.5 Schutz vor Adressenklaue	248
10.5.1 „Getarnte“ Mailadressen	248
10.5.2 Challenge-Response-Mechanismen	250
10.6 Die Rechtslage	250
10.7 Spamschutz ist keine persönliche Angelegenheit	252
10.8 Spammer fälschen Absender: Backscatter-Problematik	254
10.9 Taggen führt zu Mailverlust!	256
10.10 Zu vorsichtiges Filtern führt zu Mailverlust!	258
10.11 Realtime Blackhole Lists	260
10.11.1 DNSBL / RBL	261
10.11.2 RHSBL	265
10.11.3 URIBL	266
10.12 Vor- und Nachteile von RBL / RHSBL	266
10.12.1 Bin ich gelistet? Der schnelle Check	267
10.12.2 Probleme bei Backup-Mailservern (Insel-Problem)	267
10.12.3 Tipps aus der Praxis	268
10.13 SpamAssassin – der erfolgreiche Killer	269
10.14 Anti-Spam-Initiativen	269
10.14.1 abuse.net	269
10.14.2 cauce.org	271
10.14.3 spamhaus.org	271
10.14.4 spamcop.net	271
10.14.5 samspade.org	272
10.15 Gefälschte Mailheader: Spammer identifizieren	272
10.16 Sender Policy Framework (SPF)	276
10.17 Microsoft Caller-ID / Sender-ID	282

10.18 DKIM / Yahoo DomainKeys . . . . .	283
10.19 Greylisting und policyd-weight . . . . .	285
10.20 Teergruben/Tarpitting . . . . .	285
10.21 Tipps aus der Praxis . . . . .	287
<b>11 Mails sicher relayen: SASL &amp; Co. . . . .</b>	<b>291</b>
11.1 SMTP-Auth mit Cyrus- und Dovecot-SASL . . . . .	292
11.2 Cyrus-SASL . . . . .	293
11.2.1 Die richtigen Pakete für Cyrus-SASL installieren . . . . .	295
11.2.2 Cyrus-SASL konfigurieren: smtpd.conf . . . . .	296
11.2.3 saslauthd: Konfiguration, Vor- und Nachteile . . . . .	298
11.2.4 Cyrus-SASL debuggen: testsaslauthd und saslfinger . . . . .	300
11.3 „Authentication Backends“ von Cyrus-SASL . . . . .	301
11.3.1 Gegen einen Mailserver authentifizieren: rimap . . . . .	301
11.3.2 Separate Passwortdatei: sasldb2 . . . . .	303
11.3.3 LDAP . . . . .	305
11.3.4 SQL . . . . .	306
11.3.5 PAM und shadow . . . . .	307
11.4 SMTP-Auth für den Mailempfang mit Cyrus-SASL . . . . .	308
11.4.1 SASL weiter absichern . . . . .	311
11.4.2 Erlaubte Absenderadressen kontrollieren . . . . .	311
11.5 SMTP-Auth für den Mailempfang mit Dovecot-SASL . . . . .	312
11.6 Die Port-25-Sperre und submission . . . . .	313
11.7 SMTP-Auth für den Versand von Mails . . . . .	314
11.7.1 Klartextmethoden erlauben . . . . .	315
11.7.2 Unterschiedliche Login-Daten parallel benutzen . . . . .	316
11.7.3 Unterschiedliche Relayhosts nutzen . . . . .	316
11.8 Passwörter sicher speichern und übertragen . . . . .	317
11.9 Mit SSL/TLS-Zertifikaten authentifizieren . . . . .	318
11.10 SMTP-after-POP . . . . .	319
11.11 Dynamic Relay Authentication Control (DRAC) . . . . .	324
<b>12 Unterschiede je nach Einsatzkonzept . . . . .</b>	<b>325</b>
12.1 Postfix als eingehendes Mailrelay vor einem anderen Server . . . . .	325



12.1.1	Relay-Domains definieren . . . . .	326
12.1.2	Transportweg definieren . . . . .	327
12.1.3	Relay-Domains und Transportweg zugleich definieren! . . . . .	327
12.2	Empfängervalidierung auf Mailrelays . . . . .	328
12.2.1	Statische Empfängerlisten . . . . .	329
12.2.2	Dynamische Empfänger-Verifizierung . . . . .	331
12.2.3	Dynamische Absender-Verifizierung . . . . .	335
12.3	Mailversand mit dynamischen IP-Adressen . . . . .	336
12.4	Mailversand bei manuellen Einwahlverbindungen (ISDN/UMTS) . . . . .	337
12.5	Mailversand an einen oder mehrere SMTP-Relayhosts . . . . .	341
12.6	Empfang bei Einwahlverbindungen mit dynamischen IP-Adressen . . . . .	342
12.7	Abholung von E-Mails mit Fetchmail & Co. . . . .	344
12.7.1	fetchmail starten lassen . . . . .	345
12.7.2	fetchmail konfigurieren . . . . .	347
12.7.3	Bitte kein „multidrop“! . . . . .	348
12.7.4	Zur weiteren Vertiefung von fetchmail . . . . .	349
12.8	Postfix ein-/ausgehend hinter einem NAT-Router . . . . .	350
12.8.1	Ausgehendes IP-Masquerading/Source-NAT (SNAT) . . . . .	350
12.8.2	SNAT bei statischen IP-Adressen . . . . .	352
12.8.3	SNAT bei dynamischen IP-Adressen . . . . .	353
12.8.4	Eingehendes Port-Forwarding an Router und Firewall . . . . .	354
12.8.5	Eingehendes IP-Masquerading/Destination-NAT (DNAT) . . . . .	355
12.9	Loadbalancer und SMTP-Server . . . . .	356
12.9.1	Auch Exchange kann auf zwei Mailrelays balancen . . . . .	360
12.10	SMTP-Proxies und Application Level Firewalls . . . . .	363
12.11	Postfix als Relay vor Unix/Linux-Workstations . . . . .	366
<b>13</b>	<b>Postfix für Fortgeschrittene</b>	<b>369</b>
13.1	Adressklassen . . . . .	369
13.1.1	Zieldomain in \$mydestination . . . . .	370
13.1.2	Zieldomain in \$virtual_alias_domains . . . . .	371

13.1.3	Zieldomain in <code>\$relay_domains</code> . . . . .	371
13.1.4	Keine Vermischung dieser Adressklassen! . . . . .	373
13.2	Unterschiedliche Einstellungen auf unterschiedlichen IP-Adressen/Ports . . . . .	374
13.2.1	... bei der Annahme von E-Mails . . . . .	374
13.2.2	... für den Versand von E-Mails . . . . .	376
13.2.3	Variablen in der <code>main.cf/master.cf</code> nutzen . . . . .	377
13.2.4	<code>receive_override_options</code> . . . . .	378
13.3	Mails durch eigene Programme verarbeiten . . . . .	380
13.3.1	Programme über die <code>aliases-Map</code> starten . . . . .	381
13.3.2	Programme als Transportmethode starten . . . . .	382
13.4	Eigene Bounce-Templates . . . . .	383
13.5	Filtern von E-Mails nach Inhalt . . . . .	385
13.5.1	<code>pcre</code> ist schneller als <code>regex</code> . . . . .	386
13.5.2	Pattern optimieren, Ressourcen sparen . . . . .	387
13.5.3	Kodierungen berücksichtigen . . . . .	388
13.5.4	Body- und Header-Checks selektiv einsetzen . . . . .	389
13.6	Benutzerspezifische Einstellungen – Postfix Restriction Classes . . . . .	390
13.6.1	Individuelle <code>access</code> -Tabellen . . . . .	391
13.6.2	Flexible Spam-Politik . . . . .	392
13.7	Fortlaufendes Backup aller E-Mails . . . . .	393
13.8	Urlaubs-/Abwesenheitsmeldungen . . . . .	394
13.8.1	... für lokale Shell-Nutzer . . . . .	394
13.8.2	... basierend auf LDAP . . . . .	395
13.9	Eigene RBL/RHSBL aufsetzen . . . . .	398
13.10	Mail Address Extensions . . . . .	399
13.11	Delivery Status Notifications (DSN) . . . . .	400
13.11.1	DSN-Anweisungen im SMTP-Dialog . . . . .	401
13.11.2	DSN zu verbieten kann erstrebenswert sein . . . . .	402
13.11.3	DSN auf der Kommandozeile mit <code>sendmail</code> . . . . .	404
13.12	Shared Connection Caching . . . . .	405
13.13	Die Pflichtadressen <code>abuse@</code> und <code>postmaster@</code> . . . . .	408
13.14	Rate-Limiting gegenüber Clients durchsetzen . . . . .	409

13.14.1	Anzahl der Verbindungen eines Clients limitieren . . .	410
13.14.2	Anzahl der E-Mails eines Clients limitieren . . . . .	411
13.14.3	Anzahl der Empfänger eines Clients limitieren . . . . .	411
<b>14</b>	<b>Postfix tunen – Performance-Überlegungen</b>	<b>413</b>
14.1	Hardware-Ausstattung . . . . .	413
14.2	Linux-Optimierung . . . . .	415
14.3	Last-Überwachung . . . . .	418
14.4	Last managen . . . . .	419
14.4.1	Task-Beschränkungen . . . . .	419
14.4.2	Last erzeugen: Der Stresstest für Ihr Mailsystem . . . .	421
14.4.3	Was passiert, wenn Postfix überlastet ist? . . . . .	423
14.5	Prioritäten setzen: Stress-Dependent Configuration . . . . .	427
14.6	Das Datenbankformat btree . . . . .	429
14.7	Queue-Haltezeiten anpassen . . . . .	430
<b>15</b>	<b>Logfiles, Auswertungen und Monitoring</b>	<b>433</b>
15.1	Logmeldungen und syslogd . . . . .	433
15.1.1	Der „alte“ Syslogd . . . . .	434
15.1.2	Der „neue“ Syslog-ng . . . . .	435
15.2	Die Einrichtung eines zentralen Logservers . . . . .	437
15.2.1	Auf einem alten Syslog . . . . .	438
15.2.2	Auf einem neuen Syslog-ng . . . . .	438
15.2.3	Zentrales Logging mit zwei Mailservern über Kreuz . .	441
15.3	Logfiles auswerten . . . . .	441
15.3.1	Einfache Auswertung selbst gemacht . . . . .	441
15.3.2	pflogsumm . . . . .	442
15.3.3	mailgraph . . . . .	443
15.3.4	Eine Statistik für MRTG . . . . .	445
15.4	Monitoring von Mailservern . . . . .	445
15.4.1	Fieber messen: Was machen die Queues? . . . . .	446
15.4.2	qshape.pl – Den Überblick in der Queue behalten . .	450
15.4.3	qtop: Der Live-Blick in die Queue . . . . .	451

<b>IV Die Partner von Postfix</b>	<b>453</b>
<b>16 POP3/IMAP und Postfix</b>	<b>455</b>
16.1 POP3	455
16.2 IMAP	457
16.3 Schutz von Passwörtern und Servern	458
16.4 Die verschiedenen POP3- und IMAP-Server	459
16.5 qpopper von Qualcomm	460
16.6 Courier-IMAP	461
16.7 Dovecot-IMAP	462
16.8 Cyrus-IMAP	463
16.8.1 LMTP als mailbox_transport	465
16.8.2 LMTP und ein Setup über relay_domains	465
16.8.3 Anlegen des Nutzers in der sasldb2 und der finale Test	466
16.9 Webmailer	467
<b>17 Virenschutz: SpamAssassin und AMaViS</b>	<b>471</b>
17.1 Viren, Würmern und Trojanern	471
17.2 AMaViS	476
17.3 Funktionsweise von AMaViS	476
17.4 Installation von amavisd-new und SpamAssassin	479
17.5 amavisd-new in Postfix einbinden	479
17.5.1 content_filter versus smtpd_proxy_filter	480
17.5.2 E-Mails an den Filter weiterleiten	481
17.5.3 Postfix-Port 10025 unter SUSE	482
17.5.4 Postfix-Port 10025 unter Debian	484
17.5.5 Die Konfiguration auf Port 10025 optimieren	484
17.5.6 Weitere Unterschiede zwischen Post- und Pre-Queue	485
17.6 Die Grundkonfiguration von AMaViS	486
17.6.1 Mails rejecten, bouncen oder getaggt durchlassen?	487
17.6.2 Das Quarantäneverzeichnis abschalten	490
17.6.3 Besonderheiten unter Debian	491
17.6.4 Besonderheiten unter RedHat	492
17.7 Installation eines Virenkillers	492

17.7.1	ClamAV als primärer und sekundärer Scanner gleichzeitig . . . . .	493
17.7.2	Besonderheiten bei SUSE . . . . .	496
17.7.3	Besonderheiten bei Debian . . . . .	497
17.7.4	Besonderheiten bei RedHat . . . . .	497
17.7.5	Vergessen Sie nicht die Signatur-Updates! . . . . .	498
17.8	AMaViS testen . . . . .	499
17.8.1	Wenn AMaViS als <code>content_filter</code> eingebunden ist . . . . .	501
17.8.2	Wenn AMaViS als <code>smtpd_proxy_filter</code> eingebunden ist . . . . .	501
17.9	Performancetuning von AMaViS & Co. . . . .	503
17.9.1	Der Booster: Eine RAM-Disk für AMaViS . . . . .	504
17.9.2	Die maximal möglichen AMaViS-Prozesse beim <code>smtpd_proxy_filter</code> . . . . .	505
17.9.3	Limitierung und Optimierung bei der Zustellung über <code>content_filter</code> . . . . .	507
17.9.4	Keine Limitierung auf <code>localhost:10025!</code> . . . . .	508
17.10	<code>amavisd.conf</code> : Logik & Syntax für Fortgeschrittene . . . . .	508
17.11	Mails mit AMaViS taggen? . . . . .	511
17.12	Schizophren? Mehr Spaß mit <code>amavisd-new</code> Policy Banks! . . . . .	512
17.13	<code>amavisd-new</code> im Cluster . . . . .	514
17.13.1	<code>content_filter</code> . . . . .	514
17.13.2	<code>smtpd_proxy_filter</code> . . . . .	516
17.14	Training mit SpamAssassin . . . . .	517
17.15	Setup einer MySQL-Unterstützung . . . . .	519
17.15.1	Das Quarantäne-Verzeichnis in MySQL . . . . .	521
17.16	Setup einer LDAP-Unterstützung . . . . .	522
17.17	Filterung durch externe Dienstleister . . . . .	522
17.18	Sicherheitsrisiko Client . . . . .	523
17.18.1	Konfiguration der Clients . . . . .	524
17.18.2	Auswahl der Clients . . . . .	526
17.19	Hoax: Viren, die keine Viren sind . . . . .	526
<b>18</b>	<b>Mailinglisten mit Mailman</b>	<b>535</b>
18.1	Die Geschichte . . . . .	536

18.1.1	Usenet-Foren	536
18.1.2	Mailinglisten	536
18.2	Lokale Verteilerlisten durch Mailclients	537
18.3	Die Lösung: Mailman	538
18.3.1	Installation und Konfiguration	539
18.3.2	Apache vorbereiten	541
18.3.3	Mailman anpassen	542
18.3.4	Notwendige Einträge in der crontab	543
18.3.5	Wichtig: Die Liste mailman anlegen	544
18.3.6	Mailman in Postfix einbinden: <code>aliases</code>	544
18.3.7	Mailman in Postfix einbinden: <code>postfix-to-mailman.py</code>	548
18.4	Das Web-Interface	549
18.5	Steuerbefehle per E-Mail	552
18.6	Digests	554
18.7	Archive	554
18.8	Verhaltensregeln und spezielle Konfigurationen	555
18.8.1	<code>who</code> : Schutz der Mailadressen	555
18.8.2	Attachments filtern	556
18.8.3	Mailinglisten moderieren / Notmoderation	556
18.8.4	Administrativa – Ein-/Austragung	558
18.8.5	Confirmation Request / Approval	559
18.8.6	Opt-In/Opt-Out	560
18.8.7	Mehrere Domains mit einem Mailman	561
18.8.8	Eine Mailingliste aller Listenadmins	562
18.9	Bugfixes und Korrekturen zur deutschen Übersetzung	563
<b>V</b>	<b>Sicherheit</b>	<b>565</b>
<b>19</b>	<b>Sicherer Serverbetrieb</b>	<b>567</b>
19.1	„Sicherheit“ ist relativ	568
19.2	chroot – Ein Gefängnis für Postfix	568
19.2.1	Was bringt chroot?	570
19.2.2	chroot unter SUSE	570

19.3	Einführung in die Firewall-Einrichtung . . . . .	572
19.3.1	Wie Firewalls funktionieren . . . . .	572
19.3.2	Warum Firewalls notwendig sind . . . . .	573
19.3.3	ipfwadm, ipchains, iptables . . . . .	575
19.3.4	Die Firewall-Policy . . . . .	576
19.3.5	Die Charakteristiken der Dienste . . . . .	577
19.3.6	Ein Beispielskript zum Anpassen . . . . .	577
19.4	Das LAN ist nicht vertraulich: Der „Man-in-the-Middle“ . . . . .	581
19.5	root- und Login-Rechte vermeiden . . . . .	584
19.6	Nicht vergessen: Das Backup! . . . . .	585
19.7	Patches, die nicht eingespielt werden, nützen nichts! . . . . .	588
<b>20</b>	<b>Der Lauscher an der Wand</b>	<b>589</b>
20.1	Leistungsfähigkeit von Abhöreinrichtungen . . . . .	590
20.2	SSL/TLS – Schutz durch verschlüsselte Verbindungen . . . . .	592
20.2.1	Key-Generierung mit OpenSSL . . . . .	596
20.2.2	Die automatische Key-Generierung unter SUSE . . . . .	599
20.2.3	Die automatische Key-Generierung unter Debian und RedHat . . . . .	602
20.2.4	Postfix mit SSL/TLS . . . . .	602
20.2.5	telnet einmal anders: SSL/TLS testen . . . . .	606
20.2.6	stunnel sichert alles andere . . . . .	608
20.3	Pretty Good Privacy (PGP) und der GNU Privacy Guard (GNUPG) . . . . .	610
20.3.1	Geschichte und Technik von PGP . . . . .	611
20.3.2	PGP-Software und Waffenexport . . . . .	611
20.3.3	Vorsicht vor PGP 5.x . . . . .	612
20.3.4	OpenPGP, GNUPG und PGP . . . . .	612
20.3.5	PGP im Einsatz . . . . .	613
20.4	Schutz vor Wirtschafts- und Betriebsspionage . . . . .	615
<b>21</b>	<b>Rechtliche Aspekte</b>	<b>617</b>
21.1	Auskunftsverpflichtungen über Kundendaten und Logfiles . . . . .	620
21.1.1	Bestandsdaten, § 111 und § 113 TKG . . . . .	621
21.1.2	Verbindungsdaten, § 3 Nr. 5 TKG . . . . .	621

21.1.3	Auskünfte gegenüber Privaten . . . . .	622
21.2	Durchsuchungen und Beschlagnahmen . . . . .	624
21.3	Die rechtlichen Probleme der Spamfilterung . . . . .	625
21.3.1	Strafbarkeit der Unterdrückung anvertrauter Nachrichten . . . . .	625
21.3.2	Spamfilterung und die private Mailnutzung am Arbeitsplatz . . . . .	628
21.4	Die Verarbeitung von Daten und Logfiles . . . . .	631
21.4.1	Datenschutz: Das Gebot der „Datensparsamkeit“ . . . . .	632
21.4.2	Die Vorratsdatenspeicherung . . . . .	634
21.4.3	Der Datenschutzbeauftragte . . . . .	636
21.5	Zivilrechtliche Vertragsfragen und AGB . . . . .	637
21.5.1	Verfügbarkeitsgarantien und Schadensersatz . . . . .	637
21.5.2	Missbrauch und Sperre des Postfachs . . . . .	639
21.6	Signaturen und die Archivierung elektronischer Handelsbriefe . . . . .	639
21.6.1	Die E-Mail-Signatur . . . . .	640
21.7	„Disclaimer“ auf Webseiten und in E-Mails . . . . .	642
21.8	Tipps zur Wahl Ihres Anwalts . . . . .	643
<b>VI</b>	<b>Projekte</b>	<b>645</b>
<b>22</b>	<b>MySQL-basierter IMAP-Server mit Courier</b>	<b>647</b>
22.1	Die MySQL-Datenbank . . . . .	648
22.2	Die Einrichtung von Courier-IMAP . . . . .	652
22.3	Die Anpassungen bei Postfix . . . . .	654
22.4	Die Vollendung des Mailsystems . . . . .	657
22.5	Besonderheiten und wichtige Hinweise . . . . .	660
<b>23</b>	<b>LDAP-basierter IMAP-Server mit Dovecot</b>	<b>663</b>
23.1	Das LDAP-Schema im Eigenbau . . . . .	664
23.1.1	Die Kundenaccounts im LDAP . . . . .	665
23.1.2	Die Domainverwaltung im LDAP . . . . .	666
23.1.3	Die Mailadressen . . . . .	667
23.1.4	Das Anlegen des LDAP-Schemas . . . . .	668



23.1.5	Einrichten von Verwaltungsaccounts und ACLs . . . . .	670
23.1.6	Die ersten Dummy-Daten im LDAP . . . . .	672
23.2	Die zentrale User-ID der Mailaccounts . . . . .	675
23.3	Die Anbindung an Postfix . . . . .	676
23.3.1	\$relay_domains im LDAP . . . . .	676
23.3.2	Auf dem Zielhost: Mails an Dovecot relays . . . . .	677
23.3.3	Die Anbindung von Dovecot-IMAP an LDAP . . . . .	679
23.3.4	\$virtual_alias_maps im LDAP . . . . .	682
23.4	Der Test . . . . .	683
23.5	Der weitere Ausbau . . . . .	684
<b>VII</b>	<b>Anhang</b>	<b>685</b>
<b>A</b>	<b>Best Practice: Die Checkliste</b>	<b>687</b>
A.1	Die Checkliste für Postmaster . . . . .	687
A.2	Die Checkliste für Programmierer . . . . .	689
<b>B</b>	<b>Was sich die letzten Jahre getan hat: Von Postfix 2.1 zu Postfix 2.5</b>	<b>691</b>
B.1	Die Änderungen . . . . .	692
B.1.1	Neu in Postfix 2.2 . . . . .	693
B.1.2	Neu in Postfix 2.3 . . . . .	693
B.1.3	Neu in Postfix 2.4 . . . . .	695
B.1.4	Neu in Postfix 2.5 . . . . .	695
B.2	Postfix upgraden . . . . .	696
<b>C</b>	<b>Postfix kompilieren</b>	<b>699</b>
C.1	Vorbereitungen . . . . .	700
C.2	Wie Makefiles erzeugt werden . . . . .	701
C.3	Installation und Upgrade . . . . .	705
<b>D</b>	<b>Einen Nameserver einrichten</b>	<b>707</b>
D.1	Das Domain Name System (DNS) . . . . .	707
D.2	bind – der Nameserver-Dämon . . . . .	712
D.3	Den Nameserver testen . . . . .	719
D.4	Tipps zur Fehlersuche . . . . .	721

D.5 Zusammenfassung . . . . .	722
<b>E Subnetzmasken</b>	<b>723</b>
<b>F Die Postfix-Referenz</b>	<b>725</b>

Copyright (C) Open Source Press