

NEU!

www.tecChannel.de Juni/Juli/August 2002

tecCHANNEL

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 9,90
Österreich € 10,90
Benelux € 11,40
Schweiz SFR 19,80

Linux professionell einsetzen

Know-How und Praxis-Lösungen für den
erfolgreichen Einsatz von Linux



Tux goes Business

Linux auf Desktops, Servern,
Clustern und Großrechnern

Nie mehr Windows

Linux als Router, File/Print-,
Messaging- und Webserver

Tuning

Die besten Bootkonfigurationen
und Kernel-Einstellungen

Security

Workstations abschotten,
Hackerangriffe abwehren

Netze abdichten

Firewalls aufsetzen und optimieren,
Masquerading im Detail

Intra- und Internet

TCP/IP und DSL unter
Linux optimal einrichten



Editorial

tecCHANNEL-Compact – praktisch und kompetent

Mit tecCHANNEL-Compact halten Sie die erste Ausgabe des tecCHANNEL-Kompendiums in Händen, mit dem wir Ihnen ein kompetentes Nachschlagewerk zu jeweils einem bestimmten Themenkomplex bieten. Das handliche Format des Magazins verbindet die Vorteile einer Zeitschrift mit denen eines Buches. Das beliebte Pocket-Format mit auf diese Größe angepassten Schriften und Bildern und eine von Büchern übernommene Leseführung sind die ideale Voraussetzung für eine intensive Lektüre und das effektive Umsetzen der Inhalte am Arbeitsplatz. Daneben finden Sie in der Compact-Ausgabe die bewährten Elemente aus dem tecCHANNEL-Magazin wie beispielsweise Links zum Thema, weiterführende Links, Glossare und die Webcodes für zusätzliche Informationen im Online-Angebot von www.tecChannel.de. Downloads von Scripts, Listings und Tools zu den Beiträgen können Sie online über die zu jedem Beitrag am unteren Seitenrand angegebenen Webcodes vornehmen.

In der ersten Ausgabe behandeln wir das Thema Linux für den professionellen Einsatz. Neben allgemeinen Informationen zur Entwicklung und Verbreitung des populären Opensource-Betriebssystems bietet Ihnen tecCHANNEL-Compact zahlreiche Know-how-Beiträge und Workshops zu fast allen Einsatzgebieten von Linux. So lesen Sie im Kapitel „Linux-Optimierungen“ unter anderem, wie Sie die Bootoptionen und Kernel optimal einrichten oder Linux via DSL ans Internet anbinden.

Im Abschnitt „Linux im Servereinsatz“ zeigen unsere Workshops die möglichen Einsatzgebiete von Linux im Firmenumfeld. Speziell Umsteiger von Unix- oder Windows-Systemen finden hier die wichtigsten Grundlagen für eine Portierung ihrer Anwendungen auf Linux. In den Kapiteln „Linux und Sicherheit“ und „Linux als Firewall“ gehen wir auf die Besonderheiten von Linux in sicherheitsrelevanten Umgebungen ein und zeigen, wie Sie Desktops und Firmennetze effektiv gegen Viren und Angreifer von außen schützen.

Viel Spaß mit der ersten Ausgabe von tecCHANNEL-Compact
wünscht Ihnen

Frank Klinkenberg
Chefredakteur/Associate Publisher tecCHANNEL

Wir freuen uns über Kritik und Anregungen zu dieser Compact-Ausgabe. Unter www.tecchannel.de/compact können Sie uns in einem Online-Fragebogen Feedback geben.

Impressum

Chefredakteur / Ass. Publisher: Frank Klinkenberg, (verantwortlich, Anschrift der Redaktion)

Chef vom Dienst: Kerstin Lohr

Grafik: H2Design, München; stroemung, Michael Rupp, Oliver Eismann, Köln; Yvonne Reittinger

Redaktion tecCHANNEL:

Leopoldstraße 252b, 80807 München, Tel.: 0 89/3 60 86-897, Fax: -878

Homepage: www.tecChannel.de, E-Mail: redtecchannel@idginteractive.de

Autoren dieser Ausgabe: Dr. Peter Bieringer, Oliver Drees, Mike Hartmann, Jörg Luther, Peter Klau, Oliver Müller, Konstantin Pfliegl, Holger Reibold, Jörg Reitter, Michael Rupp

Textredaktion: Kerstin Lohr, Claudia Feige

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Interactive GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags nicht zulässig.

Anzeigen:

Anzeigenleitung: Dominique Remus, Tel.: 0 89/3 60 86-871

Leitung Anzeigendisposition: Rudolf Schuster, Tel.: 0 89/3 60 86-135, Fax -328

Anzeigentechnik: Martin Mantel, Andreas Mallin

Digitale Anzeigenannahme: Thomas Wilms, leitend, Tel.: 0 89/3 60 86-604, Fax -328

Vertrieb:

Vertriebsleitung: Josef Kreitmair

Vertriebsmarketing: Peter Prieuwasser (leitend), Stefanie Kusseler

Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113, E-Mail: mzv@mzv.de, Website: www.mzv.de

Produktionsleitung: Heinz Zimmermann

Druck: Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen

Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in tecCHANNEL-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Verlag:

IDG Interactive GmbH, Leopoldstraße 252b, 80807 München, Tel.: 0 89/3 60 86-02, Fax: -501

Leserservice:

CSJ, Postfach 140220, 80452 München, Tel.: 0 89/20 95 91 32, Fax: 0 89/20 02 81 11

Geschäftsführer: York von Heimburg

Verlagsleitung: Stephan Scherzer (Mitglied der Geschäftsleitung)

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Interactive GmbH ist die IDG Communications Verlag AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.

Vorstand: Keith Arnot, Kelly P. Conlin, York von Heimburg, Ralph Peter Rauchfuss

Aufsichtsratsvorsitzender: Patrick McGovern

Inhalt

	Editorial	3
	Impressum	4
	Inhalt	5
1	Linux im Überblick	10
1.1	Linux, wie alles begann	10
1.1.1	Der erste Schritt	10
1.1.3	Torvalds gegen Tanenbaum	12
1.1.5	Die Story geht weiter	14
1.1.6	Linux gegen Windows	15
1.1.7	Ausblick	16
1.2	Tux goes Biz	18
1.2.1	Standardisierung für Linux	18
1.2.2	Kernel 2.4	19
1.2.3	Linux auf dem Server	20
1.2.4	Linux 2.4 im Enterprise-Markt	22
1.2.5	Kernel 2.5 und IA64	22
1.2.6	Einstieg der Big Player	23
1.2.7	Linux-Elefantenhochzeit	23
1.2.8	Engagement der Software-Industrie	24
1.2.10	Ausblick	27
1.3	Linux auf dem Mainframe	28
1.3.1	S/390 im Überblick	28
1.3.4	Linux auf dem Mainframe	31
1.3.5	Distributionen	32
1.3.6	Betriebsarten	33
1.3.7	Linux im z/VM-Modus	33
1.3.8	Vorteile und Einsatzgebiete	34
1.3.9	E-Business	35
1.3.10	Performance	37
1.3.11	Fazit	38
2	Linux-Optimierungen	40
2.1	Linux-Bootkonfigurationen	40
2.1.1	Notbremse: Bootdisketten erstellen	40
2.1.2	Systemstart unter Linux	41
2.1.3	LILO-Basics	41
2.1.5	Schaltzentrale init	43
2.1.6	Konfiguration über Runlevels	44
2.1.7	Login und Shut-down	45
2.1.8	inittab und boot	45
2.1.9	Runlevel-Änderung über ksysv	47
2.1.13	Fazit	51

2.2	Linux-Kernel-Tuning	52
2.2.1	Werkzeugkasten	52
2.2.2	x11perf, bonnie und unixbench	53
2.2.3	Kernel-Kompilierung als Benchmark	54
2.2.4	CPU-gerechte Kompilierung	54
2.2.5	Kompilierung ohne Module	56
2.2.6	Powertweak für Linux	57
2.2.9	Fazit	60
2.3	TCP/IP-Netze mit Linux	62
2.3.1	Linux und die Netzwerkkarte	62
2.3.4	IP-Adressen auf die Schnelle	65
2.3.5	Netzanbindung mit ifconfig	65
2.3.6	Speichern der NIC-Einstellungen	66
2.3.7	Debian-Special	67
2.3.8	Pfad nach außen	67
2.3.9	Testen der Basiskonfiguration	68
2.3.10	Namensauflösung	69
2.3.13	Fazit	70
2.4	DSL unter Linux	72
2.4.1	Treibervarianten	72
2.4.3	Installation	73
2.4.6	Test der Hardware	77
2.4.7	Einrichten des Zugangs	78
2.4.8	Konfiguration des pppd	79
2.4.10	Manuelle Einwahl	80
2.4.11	Internet für alle	81
2.4.12	Einwahl mit Komfort	82
2.5	Sichere Linux-Workstation	84
2.5.1	Linux vs. Windows	84
2.5.2	Sichern des Bootvorgangs	85
2.5.7	Passwortschutz	89
2.5.8	MD5 und Shadow	89
2.5.9	PAM	90
2.5.15	SUID root beschränken	95
2.5.16	Serverdienste	96
2.5.22	Andere Dienste	100
2.5.23	Fazit	101
3	Linux im Servereinsatz	102
3.1	Linux als Windows-Server	102
3.1.1	Was ist Samba?	103
3.1.5	Grundlegende Konfiguration	105
3.1.8	Verschlüsselte Passwörter	107
3.1.9	Benutzerverwaltung	108
3.1.11	File-Shares	109
3.1.13	Grafische Oberflächen	111
3.1.14	Samba-Client an Windows XP	113
3.1.15	Fazit	114

3.2	Linux als Printserver	116
3.2.1	Postscript oder RAW?	116
3.2.2	Drucker am Client	117
3.2.3	Automatische Treiberinstallation	118
3.2.4	Referenzinstallation anlegen	118
3.2.5	Druckerdefinition für Samba	119
3.2.7	Treiber bereitstellen	120
3.2.8	Drucker freigeben	121
3.2.9	Abschluss und Test	123
3.3	Linux als Dial-up-Router	124
3.3.1	Dial-up-Router mit Dial-on-Demand	124
3.3.2	IP-Masquerade	125
3.3.6	Module laden	128
3.3.7	IP-Forwarding aktivieren	129
3.3.8	Regeln erstellen	129
3.3.9	Sicherung des Gateways	130
3.3.10	Windows-Clients einrichten	131
3.3.11	Linux-Clients einrichten	132
3.3.12	Wählen nach Bedarf	133
3.3.14	PAP-Konfiguration	134
3.3.17	Fazit	138
3.4	Proxy-Server unter Linux	140
3.4.1	Proxy-Server: Zugriffskontrollen	140
3.4.2	Squid: Installation	141
3.4.3	SquidGuard	142
3.4.5	Konfiguration	143
3.4.7	Zugriffskontrolle: Filtern von URLs	144
3.4.8	Zugriffskontrolle: Filtern von Stichwörtern	145
3.4.9	Zugriffskontrolle: Administration	145
3.4.10	Proxy-Server ins System einbinden	146
3.4.11	Webalizer: Überwachen des Proxys	147
3.4.12	Webalizer: Auswertung der Logfiles	147
3.4.13	Einsatz eines Proxy-Servers und Datenschutz	149
3.5	Linux als Webserver	152
3.5.1	Das erste Rüstzeug	152
3.5.2	Scripts für den Webserver	153
3.5.3	Der erste Start	153
3.5.4	Standarddokumente	154
3.5.5	Andere Verzeichnisse im HTTP-Baum	155
3.5.6	Das Ruder in der Hand - Zugriff steuern	156
3.5.7	Wer darf und wer nicht?	157
3.5.8	Gezielter steuern	158
3.5.9	Sicherheit eine Stufe höher	159
3.5.10	Fazit	160
3.6	Instant-Messaging-Server Jabber	162
3.6.1	Jabber im Detail	162
3.6.2	Jabber-Server einrichten	163

3.6.3	Installation	164
3.6.4	Konfiguration	164
3.6.5	Starten des Servers	165
3.6.6	Jabber aufgebohrt	165
3.6.7	Installation des Konferenzmoduls	166
3.6.8	Jabber-Chat-Raum einrichten	167
3.6.9	Jabber User Directory (JUD)	168
3.6.10	Außenanbindung	169
3.6.11	Konfiguration der AIM-Schnittstelle	170
4	Linux und Sicherheit	172
4.1	Viren unter Linux	172
4.1.1	Warum die Viren auf sich warten ließen	172
4.1.2	Hausgemachtes Problem?	173
4.1.3	Binary-Viren sind unmöglich? Falsch!	174
4.1.4	Verbreitung per Daemon	174
4.1.5	E-Mail-Viren sind unmöglich? Falsch!	175
4.1.6	Linux ist sicher? Falsch!	175
4.1.7	Angriffspunkt Buffer Overflow	176
4.1.8	Fazit: Die Gefahr ist real!	176
4.2	Hacker-Angriffe unter Linux	178
4.2.1	Spuren im Logfile	178
4.2.2	Logfiles auf Remote-Host	179
4.2.3	Logfiles schützen	180
4.2.4	Modular Syslog	181
4.2.5	Der Protokollierung letzter Schliff	182
4.2.6	Simple Intrusion Detection	182
4.2.7	Baselines	183
4.2.11	Aktive Audits	185
4.2.12	Überwachung mit Isof	186
4.2.13	Gelöscht und doch offen?	187
4.2.14	Versteckte Dateien anzeigen	187
4.2.15	Fazit	188
4.2.16	Intrusion Detection Systeme	190
4.3	Desktop-Firewall mit Linux 2.4	192
4.3.1	Iptables	192
4.3.3	Firewall Builder	193
4.3.4	Rahmenbedingungen	194
4.3.5	Basiskonfiguration	194
4.3.6	Das Firewall-Objekt	195
4.3.7	Firewall-Interfaces	196
4.3.8	Compilierung und Installation	196
4.3.9	Hosts und Netzwerke	197
4.3.10	Dienste und Protokolle	198
4.3.13	Die Firewall-Policy	200
4.3.14	Regeln für FTP und HTTP	201
4.3.15	Regeln für DNS	202
4.3.16	Regeln für Mail und News	203

4.3.17	Regeln für Managementtools	204
4.3.18	Regeln für Windows-Netze	204
4.3.19	Firewall starten	205
4.3.20	Fazit	206
5	Linux als Firewall	208
5.1	Firewall-Grundlagen	208
5.1.1	Definition einer Firewall	208
5.1.2	Zentraler Sicherheitsknoten	209
5.1.3	Nachteile und Begrenzungen	209
5.1.4	Komponenten einer Firewall	210
5.1.5	Paketfilterungs-Router	211
5.1.6	Abwehr von Angriffen	211
5.1.7	Vorteile von Paketfilterungs-Routern	212
5.1.8	Nachteile	213
5.1.9	Proxy-Server	213
5.1.11	Bastion-Host	214
5.1.14	Verbindungs-Gateways	215
5.1.15	Hybrid-Firewalls	215
5.1.16	Hochsicherheits-Firewalls	216
5.1.17	Fazit	216
5.2	Linux als Firewall	218
5.2.1	Hard- und Softwareauswahl	218
5.2.2	Installation	219
5.2.4	Deaktivieren unnötiger Dienste	220
5.2.5	Wichtige Proxies	221
5.2.6	Konfiguration und Verbindungen	221
5.2.7	Weitere Tools zur Netzwerkkontrolle	223
5.2.8	Grundschutz durch den Linux-Kernel	223
5.2.9	Grundschutz im Detail	225
5.2.11	Kontrolle der Paketweiterleitung	227
5.2.12	Fazit	227
5.3	Masquerading mit Linux	228
5.3.1	Masquerading	228
5.3.2	Konfiguration von Masquerading	229
5.3.3	Masquerading Proxies	230
5.3.4	Masquerading von innen nach außen	231
5.3.5	Verbindung zu PGP-Keyservern	231
5.3.6	Sonderfall T-Online	232
5.3.7	Absicherung bei T-Online	233
5.3.8	Transparente Proxies	234
5.3.10	Fazit	235
	Service	191
	Glossar	237
	Index	247
	Vorschau	250

1 Linux im Überblick

Als Linus Torvalds 1991 mit der Entwicklung von Linux begann, war nicht abzusehen, dass sich aus dem Hobby des jungen Finnen ein ernst zu nehmendes Betriebssystem entwickelt. In diesem ersten Kapitel geben wir Ihnen einen Überblick über die Geschichte von Linux und darüber, wie sich das Open-source-Betriebssystem immer mehr auch im professionellen Umfeld etabliert.

1.1 Linux, wie alles begann

Vor über zehn Jahren hat Linus Torvalds im Usenet zum ersten Mal sein Projekt vorgestellt: „ein (kostenloses) Betriebssystem“. Von „es wird nichts Großes oder Professionelles wie GNU“ kann heute jedoch keine Rede mehr sein. Im Gegensatz zur weit verbreiteten Meinung ging es Linus Torvalds primär nicht darum, einen kostenlosen Unix-Ersatz zu schaffen. Es fing damit an, dass das Rechenzentrum seiner Universität 1990 zwar über eine microVAX mit Ultrix verfügte, aber nicht genug Rechenleistung für die Studenten bereitstellen konnte. Dennoch kam für Torvalds ein 386er nicht in Frage: „Dann hätte ich ja mit diesem lausigen Betriebssystem MS-DOS arbeiten müssen und nichts gelernt“, sagt er 1997 in einem Interview mit „Wired“.

Erst als er in einem Universitätskurs mit Andrew S. Tanenbaums Minix in Kontakt kommt, entscheidet Torvalds sich, einen PC zu kaufen. Zunächst geht es ihm lediglich darum, die Task-Switching-Fähigkeiten des 80386 zu verstehen. Sein erstes Erfolgserlebnis ist ein Minix-Programm aus zwei Prozessen, die abwechselnd die Zeichenfolgen AAAA und BBBB auf den Bildschirm bringen. Im nächsten Schritt erweitert Linus das Programm zu einem Newsreader: Der eine Task bringt die News vom Modem auf den Bildschirm und der andere von der Tastatur zum Modem - allerdings immer noch unter Minix.

Aber Linus Torvalds hat bereits Blut geleckt. „Zu diesem Zeitpunkt hatte ich bereits gemerkt, dass Minix nicht genug ist. Fehlende Jobkontrolle, hässliches Speichermanagement, keine Unterstützung für FPU's und so weiter“, erklärt er der „Linux News“ (<http://alge.anart.no/linux/history/LinuxNews.03A>) Mitte Oktober 1992 in einem Interview.

1.1.1 Der erste Schritt

Weitere Kritikpunkte von Torvalds waren, dass Minix ein rein „akademisches“ Betriebssystem ist und aus Gründen der Portierbarkeit nur den kleinsten gemeinsamen Nenner der damals verfügbaren Prozessorarchitekturen (8088, 68000, Sparc) verwendet. Dementsprechend nutzt es auch nicht die besonderen Fähigkeiten des 80386.

Torvalds beginnt mit seiner Mammutaufgabe: einem komplett neuen Betriebssystem, dessen erstes sichtbares Anzeichen sich am 3. Juli 1991 in Form eines Postings in comp.os.minix offenbart. Darin fragt er nach einer Definition der Posix-Standards, damit sich Anwendungsprogramme leichter auf das zu diesem Zeitpunkt noch namenlose Betriebssystem portieren lassen.

Doch die Posix-Spezifikationen sind nur gegen Bezahlung vom Standardkomitee erhältlich. Linus muss sich einen anderen Weg suchen, um eine Programmierschnittstelle für sein Betriebssystem zu schaffen. Zu diesem Zeitpunkt meldet sich Ari Lemmke bei Linus und verweist ihn auf die GNU libc.a (www.gnu.org), eine Bibliothek mit Funktionen des ANSI-C-Standards und Posix-Features.

Ari richtet auch gleich das erste öffentliche Linux-Verzeichnis (`/pub/OS/Linux`) auf `nic.funet.fi` ein, obwohl dort noch für einige Zeit lediglich ein README zu finden ist: „Dieses Verzeichnis ist für den frei verteilbaren Minix-Clone“. Ari ist es übrigens zu verdanken, dass Linux heute „Linux“ heißt: Linus will das Betriebssystem eigentlich „Freax“ (Kunstwort aus *free*, *freak* und dem *x* von Unix) taufen. Den Arbeitstitel Linux will er nicht verwenden, weil er Angst hat, als „Egomane“ beschimpft und nicht ernst genommen zu werden, erklärt er „Wired“. Doch Ari findet Linux besser und legt somit den Grundstein.

1.1.2 Linux 0.01

Doch immer noch besteht Linux lediglich aus einem rudimentären Protected-Mode-System mit einem AT-Treiber und dem Minix-Dateisystem. Um nicht völlig richtungslos zu entwickeln, wendet sich Linus am 25. August 1991 erneut an die Benutzer von comp.os.minix:

```
Path: icdoc!ukc!mcsun!news.funet.fi!hydra!klaava!torvalds
From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: What would you like to see most in minix?
Summary: small poll for my new operating system
Keywords: 386, preferences
Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI>
Date: 25 Aug 91 20:57:08 GMT
Organization: University of Helsinki
Lines: 20
```

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical