PC WELT SONDERHEFT
Juli/August/September 04/2004
www.tecChannel.de

NEU!

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

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

Sicherheit
für Netzwerk & Server

- Linux: Hacker und Viren abwehren
- Windows-Server absichern
- Ausfallsicherheit erhöhen

Unentbehrliches Basiswissen für Netzwerk-Profis

WINDOWS 2003
- Sicherheit weiter erhöhen
- Policies richtig einsetzen

PRIVACY
- Spam: Mailserver absichern
- IP-VPN: Sicherer durch Managed Services

SAFETY
- Backup-to-Disk, RAID
- Netze ausfallsicher planen

WEBSERVER
- Angriffe abwehren & verhindern
- Schutz vor Cross-Site Scripting und SQL Injection

LINUX
- Virenschutz für Client & Server
- Schutz mit Proxy und Firewall

GRUNDLAGEN
- Beweissicherung, Biometrie, Buffer Overflow, Backup, USV, Common Criteria u.v.m.

4 195914 906900 40

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Chef vom Dienst / Textchef: Kerstin Lohr
Grafik: stroemung, Michael Rupp, Oliver Eismann, Köln; h2design, München; Yvonne Reittinger, Wien

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: Uwe Becker, Bernhard Haluschak, Mike Hartmann, Thomas Käfer, Heinz Kraus, Christoph Lange, Jörg Luther, Tanja Möhler, Stefan Mutschler, Konstantin Pfliegl, Stefan Rubner, Thomas Wölfer; Korrektorat: Claudia Feige

Quelle Titelfoto: Fujitsu-Siemens

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: Dirk Limburg, Tel.: 0 89/3 60 86-871
Anzeigendisposition: Rudolf Schuster (leitend), 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 / Produktion:
Vertrieb: Josef Kreitmair (leitend), Katrin Elsler
Vertriebsmarketing: Peter Priewasser (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 86-0, Fax: -501

Geschäftsführer: York von Heimburg
Verlagsleitung: Frank Klinkenberg

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 International Data Group Inc., Boston, USA

Vorstand: York von Heimburg, Keith Arnot, Pat Kenealy
Mitglieder der Konzerngeschäftsleitung: Karin Giffhorn, Stephan Scherzer, Josef Lohner
Aufsichtsratsvorsitzender: Patrick McGovern

tecCHANNEL-Compact erscheint im Verlag der PC-WELT. Darüber hinaus gehören zu unserer Verlagsgruppe folgende Zeitschriften:

COMPUTERWOCHE ComputerPartner PC WELT DigitalWorld Macwelt GameStar CIO GamePro

Leser- und Abo-Service:
Dialog-Service-Center GmbH, Konrad-Zuse-Straße 16, 74172 Neckarsulm, Telefon: 0 18 05/9 99-802, Fax: 0 71 32/9 59-166, E-Mail: tecchannel@d-s-center.de

Inhalt

	Editorial	**3**
	Impressum	**4**
1.	**Security**	**10**
1.1	**Linux als Proxy-Server**	**10**
1.1.1	Squid installieren	11
1.1.2	Installation konfigurieren	11
1.1.3	Grundkonfiguration und erster Start	13
1.1.4	Proxy-Clients konfigurieren	14
1.1.5	Einfache Authentifizierung aktivieren	16
1.1.6	Authentifizierung über Windows-Domain	18
1.1.7	Beschränkung nach Ziel und Zeit	18
1.1.8	URL-Filterung	20
1.1.9	Cache-Strategien anpassen	21
1.1.10	Cache-Speicher vergrößern und verteilen	23
1.1.11	ACLs mit SquidGuard vereinfachen	24
1.1.12	Squid als Anonymisierer	28
1.1.13	Ausblick	29
1.2	**Linux als Firewall**	**30**
1.2.1	Setup: Lieber von Hand	30
1.2.2	Die Arbeitsweise von iptables	31
1.2.3	Die WWW-Faustregel	32
1.2.4	Die schärfere Variante	34
1.2.5	Eigene Server einrichten	34
1.2.6	Eigene Ketten definieren	35
1.2.7	Ausgehende Verbindungen beschränken	37
1.2.8	Traffic-Shaping	38
1.2.9	Eine Warnung zum Schluss	40
1.3	**Spurensuche: Computer-Forensik**	**41**
1.3.1	In eigenem Interesse	41
1.3.2	Incident Response	42
1.3.3	Status quo bewahren	42
1.3.4	Alarmierungsplan	43
1.3.5	Datenschutz	44
1.3.6	Anfertigen von Arbeitskopien	44
1.3.7	Analyse der Daten	45
1.3.8	Interessante Fundstellen	46
1.3.9	Zugriffszeiten	46
1.3.10	Netzwerkanalyse	47
1.3.11	E-Mail-Analyse	48
1.3.12	Protokollierung	50

1.3.13	Faktor Überwachung	50
1.3.14	Fazit	51
1.4	**Common Criteria: TÜV für IT-Sicherheit**	**53**
1.4.1	TCSEC und ITSEC	53
1.4.2	Common Criteria	54
1.4.3	Evaluierungsstufen	54
1.4.4	Umfang der Evaluierung	55
1.4.5	Schutzprofile	55
1.4.6	Fazit	56
1.5	**Windows Server 2003 – Secure per Default**	**58**
1.5.1	Nicht installierte Komponenten	59
1.5.2	Sicherheitskonfiguration für IE	60
1.5.3	Windows-Update: Automatisch	61
1.5.4	Änderungen an den Default-Einstellungen	62
1.5.5	Änderungen an „Everyone“	62
1.5.6	Änderungen bei den Diensten	63
1.5.7	Änderungen beim Internet Information Server	63
1.5.8	Wie man den Server noch sicherer macht	65
1.6	**Sicherheits-Tuning für Windows Server 2003**	**69**
1.6.1	Orientierung mit Security Guides	70
1.6.2	Domänenweite Vorgaben	70
1.6.3	Server-Security: Baseline und Spezialtypen	71
1.6.4	Arbeitshilfen: Excel-Sheets und Templates	72
1.6.5	Dienstekonfiguration optimieren	73
1.6.6	Verfügbaren Arbeitsspeicher erhöhen	74
1.6.7	Angriffspunkte reduzieren	75
1.6.8	Registry manipulieren	75
1.6.9	Schutz vor Angriffen	76
1.6.10	Sicherheit erhöhen mit IPsec	76
1.7	**Cross-Site Scripting und SQL-Injection: Gefahren für Webseiten**	**78**
1.7.1	Grundlagen des XSS	78
1.7.2	Dynamische Webseiten und HTML	79
1.7.3	Bösartiger Code	79
1.7.4	Selbst versendeter bösartiger Code	80
1.7.5	Jeder Input ist böser Input	81
1.7.6	Angriff auf Datenbanken: SQL-Injection	83
1.8	**Basiswissen Buffer Overflow**	**86**
1.8.1	Der Einstieg: Variablen	86
1.8.2	Adressen von Variablen	87
1.8.3	Ein Beispielprogramm	87
1.8.4	Speicher wird beschrieben	88
1.8.5	Verarbeitung der Variablen	89

1.8.6	Das Problem: Der Puffer ist zu klein	90
1.8.7	Überschriebener Speicher = kaputte Daten	91
1.8.8	Name: Nicht erkennbar	92
1.8.9	Buffer Overflow als Angriffsvektor	92
1.8.10	Pufferschutz	93
1.8.11	Arbeitsweise von Funktionen	94
1.8.12	Wichtig: Die Rücksprungadresse	94
1.8.13	So wird zurückgesprungen	95
1.8.14	Wichtiger Speicher: Der Stack	96
1.8.15	Lokale Variablen liegen im Stack	97
1.8.16	Buffer Overflow: So passiert es	98
1.8.17	So wird angegriffen	99
1.8.18	Ausführen beliebigen Codes	99
1.9	**Virenschutz unter Linux**	**101**
1.9.1	Spezielle Angriffspunkte unter Linux	101
1.9.2	Sicherheit unter Linux	102
1.9.3	Authentifikation	102
1.9.4	Systemsicherheit mit LIDS und Snort	103
1.9.5	Gefahren durch Konfigurationsfehler und mangelhaftes Patch-Management	103
1.9.6	AV-Lösungen unter Linux	104
1.9.7	Juristische Anforderungen	106
2.	**Privacy/Identity**	**107**
2.1	**Spam-Schutz für Server**	**107**
2.1.1	Wie arbeiten Spammer?	108
2.1.2	Relaying – unerlaubtes Versenden von Mails	109
2.1.3	Relaying möglich?	110
2.1.4	Relaying möglich – was nun?	111
2.1.5	Weitere Maßnahmen gegen Relaying	112
2.1.6	Relaying und Sendmail	112
2.1.7	Heikle SMTP-Kommandos	113
2.1.8	Blackhole Lists	113
2.1.9	Merkmale einer Spam-Mail	114
2.1.10	Bayes-Filter	114
2.1.11	Teergruben	115
2.1.12	Anbieter rüsten auf	115
2.2	**Schutz vor Datenklau**	**117**
2.2.1	Grundschutz	117
2.2.2	Mail und Freemail	118
2.2.3	Beschreibbare oder externe Medien	118
2.2.4	Dokumenten-Management-Systeme	120

3.3	**Schnelle Datensicherung mit Backup-to-Disk**	**159**
3.3.1	Turbo für die Datensicherung	159
3.3.2	Klassische Backup-Tools	160
3.3.3	Backup-to-Disk in Enterprise-Lösungen	162
3.3.4	Schnelles Backup & Restore mit Virtual Tape Libraries	162
3.3.5	Von klein bis groß	163
3.3.6	Kostenloses Backup-to-Disk mit Robocopy	164
3.3.7	Schattenkopien von Windows Server 2003/XP	168
3.4	**RAID im Überblick**	**169**
3.4.1	Vorteile von RAID	169
3.4.2	Software- vs. Hardware-RAID	170
3.4.3	Anforderungen an die Festplatten	171
3.4.4	RAID Level 0	171
3.4.5	RAID Level 1	172
3.4.6	RAID Level 0+1	173
3.4.7	RAID-Verfahren mit Fehlerkorrektur	173
3.4.8	ECC-Overhead bei Schreiboperationen	174
3.4.9	RAID Level 2	175
3.4.10	RAID Level 3	175
3.4.11	RAID Level 4	176
3.4.12	RAID Level 5	177
3.4.13	Kombi-Verfahren auf RAID-5-Basis	178
3.4.14	RAID 6 und RAID 7	178
3.4.15	$RAID^n$	178
3.4.16	Implementation	179
3.4.17	RAID-Varianten im Überblick	180
3.4.18	Verhalten bei Plattenausfall	181
3.4.19	Fazit	182
3.5	**Netze ausfallsicher konzipieren**	**183**
3.5.1	Voraussetzung: Management	184
3.5.2	Grundregeln für das Netzdesign	184
3.5.3	Einfache Konfiguration wichtig	185
3.5.4	Ersatz vorhalten	185
3.5.5	Ausfallsichere Switch-Verbindungen	186
3.5.6	Ausfallsichere Server-Verbindungen	187
3.5.7	Link Aggregation vs. Spanning Tree	188
3.5.8	STP und RSTP	188
3.5.9	Redundanz auf Layer 3	189
3.5.10	Redundanz auf Dienste-Ebene	190
3.5.11	Ausfallsicherheit im WLAN	190
	Glossar	**193**
	Index	**197**
	tecCHANNEL-Leserumfrage – Mitmachen und gewinnen!	**200**