

NEU!

tecCHANNEL

tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

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

IT-Security

Viren · SPAM · Clients · Datensicherheit · Netze · Server

Unentbehrliches
Know-How für
den IT-Profi

Grundlagen, Konzepte und Workshops
für mehr Desktop- und Netzwerk-Sicherheit

XP-Dienste optimieren

Services richtig konfigurieren und kritische Funktionen abschalten

PKI im Unternehmen

Authentifizierung & Verschlüsselung zentral planen und managen

SPAM-Abwehr

Schützen Sie Ihr Netzwerk vor unerwünschten Massenmails

WLANs absichern

So umgehen Sie die Schwächen des WLAN-Standards

Ausfallsichere Systeme

Desktops, Web- und Fileserver auf mehr Zuverlässigkeit trimmen

Die Portreferenz

Die wichtigsten TCP/IP-Ports und Funktionen zur Firewall-Konfiguration



Impressum

Chefredakteur: Michael Eckert (mec), (verantwortlich, Anschrift der Redaktion)

Chef vom Dienst: Kerstin Lohr

Grafik: stroemung, Köln, Michael Rupp, Oliver Eismann, h2design, München, Yvonne Reitinger

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 :

Mike Hartmann, Albert Lauchner, Jörg Luther, Klaus Manhardt, Konstantin Pfielgl, Thomas Rieske, Detlef Schumann, Axel Sikora

Textredaktion: Kerstin Lohr

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 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 im 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

Leserservice:

A.B.O Verlagsservice GmbH, Ickstattstraße 7, 80469 München, Tel: 0 89/20 95 91 32, Fax: 0 89/20 02 81 11

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 IDG Inc., Boston, Mass., USA.

Vorstand: Keith Arnot, York von Heimburg, Ralph Peter Rauchfuss

Aufsichtsratsvorsitzender: Patrick McGovern

Inhalt

	Editorial	5
	Impressum	6
1	Grundlagen	12
1.1	Kryptographie im Überblick	12
1.1.1	Safety und Security	12
1.1.2	Kryptographie	13
1.1.3	Transposition vs. Substitution	14
1.1.4	Symmetrische Substitution	14
1.1.6	Asymmetrische Substitution	15
1.1.7	Vorteile von Public-Key-Verfahren	16
1.1.8	Absicherung der asymmetrischen Substitution	16
1.1.9	Trust Center	17
1.1.10	Hash-Funktionen	18
1.1.11	Substitution vs. Signatur	18
1.1.12	Hybride Verschlüsselungsverfahren	19
1.1.13	Ende-zu-Ende vs. abschnittsweise Sicherheit	19
1.1.15	Angriffsverfahren	21
1.1.19	Angriffsarten	24
1.1.20	Ausblick	25
1.2	Kryptographische Verfahren	26
1.2.1	Symmetrische Verschlüsselungsverfahren	26
1.2.2	RC-4	27
1.2.3	DES	28
1.2.6	IDEA	30
1.2.7	Asymmetrische Verschlüsselungsverfahren	31
1.2.8	RSA	31
1.2.9	Diffie-Hellman	32
1.2.11	Einweg-Hash-Funktionen	33
1.2.12	MD-5	33
1.2.13	SHA-1	34
1.2.14	DSA	34
1.3	Public-Key-Infrastrukturen	36
1.3.1	Teil I: Public-Key-Infrastrukturen	36
1.3.2	Digitales Zertifikat	37
1.3.3	Trustcenter	39
1.3.4	Die Dienste der CA und RA im Überblick	40
1.3.5	PKI Enabled Applications	41
1.3.6	Integration einer PKI in die Firmenstruktur	42
1.3.7	Stufenmodell	43
1.3.8	Trustcenter-Betrieb – intern oder extern?	44

1.3.11	Gesetzeskonform signieren – ja oder nein?	46
1.3.13	Offene Systeme für die Außenkommunikation	47
1.3.14	Traurige Realität	48
1.3.15	Europaweite Lösung	49
1.3.17	Teil II: PKI Fallstudien und Produkte	51
1.3.18	Utimaco Safeware	51
1.3.19	TC TrustCenter	52
1.3.20	Secude	53
1.3.21	Integralis	53
1.3.22	RSA Security	54
1.3.23	D-Trust	55
1.3.24	T-TeleSec	56
1.3.25	Baltimore Technologies	57
1.3.26	Microsoft	57
1.3.27	Fallstudien für PKI-Lösungen	58
1.3.33	Anlaufstellen für PKI und Informationsquellen	64
1.3.34	Fazit	66
1.4	Firewall-Grundlagen	67
1.4.1	Definition einer Firewall	67
1.4.2	Zentraler Sicherheitsknoten	68
1.4.3	Nachteile und Begrenzungen	68
1.4.4	Komponenten einer Firewall	69
1.4.5	Paketfilterungs-Router	69
1.4.9	Proxy-Server	71
1.4.11	Bastion-Host	72
1.4.14	Verbindungs-Gateways	73
1.4.15	Hybrid-Firewalls	74
1.4.16	Hochsicherheits-Firewalls	74
1.4.17	Fazit	75
2.	Netzwerk-Sicherheit	76
2.1	Ports im Überblick	76
2.1.1	Was sind Portnummern?	76
2.1.2	Sockets	78
2.1.3	Portgruppen	79
2.1.4	Welcher Port wird verwendet?	79
2.1.5	Beispiel für eine Verbindung	81
2.1.6	Router: Masquerading	82
2.1.7	Router: Port-Forwarding	82
2.1.8	Ports – ein offenes Tor	83
2.1.9	Einrichten einer Firewall	83
2.1.10	Standarddienste	84
2.1.12	Mail- und Newsdienste	86
2.1.13	Audio und Video	87
2.1.15	Kommunikation und Chat	88

2.1.16	ICMP: Internet Control Message Protocol	89
2.1.19	Fehlermeldungen	91
2.1.20	Problemmeldungen	91
2.1.21	Informationsmeldung	92
2.1.22	File-Sharing-Tools	92
2.1.24	Microsoft-Netzwerk	93
2.1.29	Microsoft Exchange	96
2.1.30	Ports im Überblick	97
2.2	Spam-Schutz für Server	98
2.2.1	Wie arbeiten Spammer?	99
2.2.2	Relaying – unerlaubtes Versenden von Mails	100
2.2.3	Relaying möglich?	101
2.2.4	Relaying möglich – was nun?	102
2.2.6	Relaying und Sendmail	103
2.2.7	Heikle SMTP-Kommandos	104
2.2.8	Blackhole Lists und andere Maßnahmen	104
2.2.9	Teergruben	104
2.2.10	Anbieter rüsten auf	105
2.3	Sicherheit im WLAN	106
2.3.1	Mangelhafte Sicherheit mangelhaft genutzt	106
2.3.2	Kostenlose Werkzeuge für den Angriff	106
2.3.3	Sicherheitsarchitektur und Authentifizierung	107
2.3.4	Zugangskontrolle	108
2.3.5	Mehr Sicherheit mit WEP	109
2.3.6	Unendlich langer Pseudo-Schlüssel	109
2.3.7	WEP-Sicherheitsrisiken	110
2.3.8	Gegenmaßnahmen	111
2.3.9	Aufwendigere Verschlüsselung	112
2.3.10	Authentifizierung via EAP und 802.1X	113
2.3.11	IEEE802.1X im Detail	114
2.3.14	MS-CHAP2 mit LEAP	116
2.3.15	Fazit	118
3	Client-Sicherheit	119
3.1	XP-Dienste aufräumen	119
3.1.1	Unverzichtbare Dienste	120
3.1.2	Ablagemappe	121
3.1.3	Anmeldedienst	121
3.1.4	Anwendungsverwaltung	122
3.1.5	Arbeitsstationsdienst	122
3.1.6	Automatische Updates	122
3.1.7	COM+-Ereignissystem	122
3.1.8	Computer-Browser	123
3.1.9	Designs	123

3.3.15	Was tun bei Virenbefall?	169
3.3.16	Nicht vergessen: Nachsorge	170
3.3.17	Fazit	170
3.4	Sicher im Web unterwegs	171
3.4.1	Browsen – aber sicher	172
3.4.2	Das Zonenmodell des Internet Explorer	173
3.4.4	Alternativen: Netscape und Opera	175
3.4.5	Outlook (Express)	176
3.4.6	Starke und schwache Passwörter	178
3.4.7	Risiko Windows Script Host	178
3.4.9	0190-Dialer	180
3.4.12	Fazit	183
4	Katastrophenvorsorge	185
4.1	Katastrophenschutz mit Plan	185
4.1.1	Vorbeugung vs. Katastrophenvorsorge	186
4.1.2	Vorarbeiten	189
4.1.3	Notfallhandbuch	190
4.1.4	Notfallübungen	192
4.2	Ausfallsichere Systeme	193
4.2.1	Die kleinen Dinge	193
4.2.2	Günstiges IDE-RAID	195
4.2.3	SCSI-RAID	196
4.2.5	Software-RAID mit Windows NT, 2000 und XP	197
4.2.7	Absicherung des Netzwerks	198
4.2.8	Schneller und sicherer durch Teaming	198
4.2.9	Redundante Netzteile	199
4.2.10	Weitere Absicherungen	200
4.2.11	Absicherung durch Backup-Server	201
4.2.12	Cluster-Lösungen und Cluster-Software	202
4.2.13	Fazit	203
4.3	Sicherheitsbewusstsein im Mittelstand	204
4.3.1	Aspekte der IT-Sicherheit	204
4.3.3	Gefahrenpotenzial	206
4.3.5	Vorhandene Sicherheitslücken im Mittelstand	209
4.3.6	Etablierung eines IT-Sicherheitsmanagements	210
4.3.8	Entwicklung eines Sicherheitskonzepts	212
4.3.9	Regelmäßige Sicherheits-Audits	213
4.3.10	Sensibilisierung des Sicherheitsbewusstseins	213
4.3.13	Internet-Nutzung	215
4.3.14	Festlegung der Sicherheitspolitik für E-Mail	215
4.3.15	Fazit	216
	Glossar	217
	Index	231
