

# Stichwortverzeichnis

## A

Abhören der Teilnehmer-Identitäten 51  
Abhören von Daten 51  
Advanced Encryption Standard 94  
AES 68, 94, 152, 172, 208  
AH-Header 152, 155  
Aktive Angriffe 54  
Aktivierung der Chipkarte 80  
Angreifer 28  
Angriffsrisiko 62  
Anschaffung 233  
Anschaffungskosten 222  
Anwendungsebene 333  
Application Service Provider 196  
Architekturentwurf 236  
ARPA 327  
ARPANET 327  
asymmetrisches Verschlüsselungsverfahren  
69  
Auditor 141  
Aufrechterhaltung des Betriebs 224  
Ausspähen von Daten 309  
Authentizität 31

## B

B2B 196  
Bedrohung 27  
Beeinträchtigung der Aufgabenerfüllung 64  
Benutzerfreundlichkeit 141, 239  
Beschaffungsphase 221  
Betriebsdokumentation 238  
Betriebsumgebung 238  
Black-Box-Lösung 122  
Blockverschlüsseler 84  
Blowfish 92, 172  
Boycott des Kommunikations-Systems  
(Denial of Service) 55  
Browser 350  
Business-to-Business-VPN 199

## C

CAST 117, 172  
Certification Authority 112, 145, 202  
Certification Revocation List 146, 150  
Chancen 31  
CHAP 160  
Chipkarte (SmartCard) 79  
Client-Server 27  
Codebits 346  
Computerdelikte 319  
Computerkriminalität 26, 28, 63, 319  
Computermanipulationen 320  
Cracker 26

## D

Data Encryption Standard 67  
Denial of Service, DoS 161  
DE-NIC 336  
DES 86, 152, 160, 172, 203, 206, 208  
DES-Algorithmus 67  
Destination Unreachable 341  
Diffie-Hellman 97, 152, 167, 172, 174, 206  
Directory-Service 148  
DNS 347  
Domain Name Service 347  
Domainnamen 336  
Down-Sizing 27  
DSA 103

## E

E-Business 16, 195, 201  
ECC 208  
Echo Request 342  
EchoReply 341  
E-Commerce 196, 199  
Editor 141  
Eignung 239  
Einfügen oder Löschen bestimmter Daten 55  
Eintrittswahrscheinlichkeit 62

Einwohnermeldeämter 72  
 elektronische Post (E-Mail) 328  
 ElGamal 103, 172  
 E-Mail 60  
 End-to-End-Verschlüsselung 124  
 Entwicklungsumgebung 237  
 Erpressung 320  
 ESP-Header 152, 156  
 Evaluationsstufe 244  
 Evaluierung 233  
 externe Zugänge 212

## F

Fehlbedienung 58  
 Fehlrouting von Informationen 57  
 Feinentwurf 236  
 Fernmeldegeheimnis 59  
 Finanzielle Auswirkungen 65  
 Firewall-Sicherheitspolitik 209  
 Fortezza 203  
 FTP 349

## G

generic Top Level Domains 336  
 geschützte Leitungsführung 211  
 globale Ausdehnung 28  
 Graphical User Interface 143  
 Grundgesetz 323  
 GSM 199  
 gTLD 336

## H

Hacker 26, 321  
 Hacking 320  
 Hardwarefehler durch Umwelteinflüsse 58  
 Hash-Verfahren 104  
 High-Tech Black Box 122  
 Hijacking 161  
 HMAC 109, 152  
 HTML (Hyper Text Markup Language) 350  
 HTTP 350  
 hybride Verschlüsselungstechnik 71

## I

ICMP 340  
 IDEA 90, 117, 172, 203  
 IKE 151, 166, 171  
 Inbetriebnahme 222  
 Industriespionage 316  
 Infrastruktur 211

infrastrukturelle Sicherheitsmaßnahmen  
 226

Installationsphase 222  
 Integrität 27, 30  
 Internet 27  
 Internet-Adressen 334  
 Intranet 27  
 IP-Optionen 339  
 IP-Protokoll 337  
 IPSec 151, 166  
 IPv4 335  
 IPv6 335  
 IP-Verschlüsselung 132  
 IPX 160  
 ITSEC-Kriterien 234  
 ITSEC-Zertifizierung 234  
 IT-Sicherheit 27  
 IT-Sicherheitskriterien 234

## K

Key-Management-Protokoll 165  
 Key-Server 150  
 Kommunikationsprotokolle 337  
 Kontrolle der Protokolldaten 213  
 Kosten im Jahr 227  
 Kreditkartenbetrug 313  
 Kriminalitätsprophylaxe 324  
 Kriminalitätsstatistik 310  
 kryptographisch gesicherte logische Netze  
 (VPN) 132  
 kryptographische Prüfsumme 70

## L

LDAP 112, 119, 149

## M

Management-Server 143  
 Management-System 143  
 Manual Keying 166  
 M-Business 16, 195  
 M-Commerce 196  
 MD4 105, 160  
 MD5 106, 117, 152, 172, 203  
 Mechanismen 27  
 Mechanismenstärke 243  
 Message Transfer Agent (MTA) 349  
 Mobilfunk 199  
 Modifikation von Daten 55

**N**

Need-to-know-Prinzip 213  
 negative Außenwirkung 65  
 Network News Transfer Protocol (NNTP) 352  
 Netzwerkebene 333  
 Netzwerkmanagement-System (NMS) 142  
 Netzzugangsebene 333  
 NIST 94  
 NNTP 351  
 NSA 29

**O**

Observer 141  
 ökonomische Aufklärung 29  
 One-Way-Hashfunktion 70  
 Operator 141  
 Opfer 319  
 Organisation 212  
 organisatorische Sicherheitsmaßnahmen  
 226  
 OSI-Referenzmodell 330  
 OSI-Schichtenmodell 160  
 OSPF (Open Shortest Path First) 340  
 Outsourcing 27

**P**

PAP 160  
 Paradigmenwechsel 323  
 Passive Angriffe 50  
 PC-Security-Komponente 124  
 Perfect Forward Secrecy 166  
 Persönlichkeitsrecht 320  
 verletzungen 320  
 Personalausweis 72  
 personelle Sicherheitsmaßnahmen 226  
 PGP 117  
 PKI-Editor 145, 146  
 Policy-Editor 145, 148  
 Portnummern 343  
 potentielle Bedrohungen 62  
 PPTP 151, 159  
 Pre-Shared Keys 172  
 Private-Key-Verfahren 67  
 Produktauswahlverfahren 222  
 Produktpiraterie 320  
 Prüflabor 234  
 Prüfstelle 234  
 Public Key Infrastructure III  
 Public-Key-Verfahren 68

**R**

RC2 203  
 RC4 93, 203  
 RC5 172  
 Recht im Internet 319  
 Rechteverwaltung 141  
 rechtsfolgenfreier Raum 319  
 Redirect 342  
 Reisepass 72  
 Remote-Ankopplung 134  
 Rijndael 94  
 RIP (Routing Information Protocol) 340  
 Risiken 31  
 Risikogesellschaft 324  
 Routing Protokolle 339  
 RSA 99, 152, 172, 206, 208

**S**

Sabotage 320  
 Schlüsselaustausch 165  
 Schlüssellänge 94  
 Schlüssel-Management 150  
 Secure Shell 151, 161, 174  
 Security Administrator 141, 215  
 Security Association 153, 171  
 Security Black Boxes 122  
 Security Bridge 127  
 Security Sublayer 121, 124  
 SET 207  
 SHA 107, 117  
 SHA-1 107, 152, 172, 174, 203, 208  
 sichere Anordnung 212  
 sicherer Betrieb 225  
 sicherer Netzdienst 121  
 Sicherheit in LAN-Segmenten 125  
 Sicherheits-  
 gefühl 209  
 konzept 209  
 lücken 214  
 management 140  
 maßnahmen 210, 225  
 mechanismen 67  
 politik 209  
 schicht 121  
 vorgaben 236  
 ziele 210  
 Site-Hacking 314  
 SKIP 166, 167  
 SmartCard 79

SMTP 349  
SMTP-Protokoll 350  
Social Engineering 218  
Softwarediebstahl 320  
Software-Fehler 58  
Software-Piraterie 316  
Source Quench 342  
Spionage 26, 320  
SSL 202  
Stärke der Sicherheitsmechanismen 239  
STOA 315  
Strafgesetzbuch 323  
Stromverschlüsseler 82  
symmetrisches Verschlüsselungsverfahren  
67

## T

TCP 345  
TCP/IP-Protokollarchitektur 332  
TCP/IP-Technologie 329  
technische Sicherheitsmaßnahmen 226  
Telekommunikationsgesetz 323  
Telnet 348  
Tests 237  
TLS 202  
transparente Lösung 121  
Transportebene 333  
Triple-DES 88, 117, 152, 172, 203, 208  
Trittbrettfahrer 56  
Trustcenter 72  
Tunneling 131

## U

UDP 344  
Übertragungsfehler 58  
UMTS 199  
Unrechtsbewusstsein 28  
unterbrechungsfreie Stromversorgung  
(USV) 211

## V

Veränderung der Geschäftsprozesse 28  
Verantwortlichkeiten 212  
Verbindlichkeit 31  
Verfügbarkeit 31  
Verkehrsflussanalyse 52

Verstoß gegen Gesetze/Vorschriften/  
Verträge 63  
vertrauenswürdiger Administrator 217  
Vertraulichkeit 27, 30  
Vertretungsregelungen 217  
Virtual Private Network 37  
Vortäuschung einer falschen Identität  
(Maskerade-Angriff) 56  
VPN 37  
Beschaffung 222  
Einsatz 212  
Protokolle 151  
Realisierungen 136  
Topologien 136  
Tunnel 137

## W

WAP 204  
WAP-Architektur 205  
WAP-Gateway 198  
WAP-Server 198  
Wartungs- und Reparaturarbeiten 215  
WDP 204  
Wert der Informationen 27  
Widerspruchsfreiheit 141  
Wiederholen oder Verzögern  
von Informationen 55  
Wirksamkeit 239  
Wirtschaftsspionage 29, 312, 315, 322  
WML 204  
World Wide Web 328  
WSP 204  
WTLS 204  
WTP 204

## X

X.509 112, 152, 172

## Z

Zertifizierung 233  
Zertifizierungs-Systeme 72, 145  
zugangsgesicherter Raum 211  
Zugangskontrolle 27, 141  
Zugriffsrechte 212  
zukünftige Entwicklungen 306  
zusätzliche Sicherheitsmaßnahmen 210



ISBN 3-8266-0935-2  
[www.mitp.de](http://www.mitp.de)

**Franz-Joachim Kauffels**

## **Durchblick im Netz, 5. Auflage**

Kauffels wendet sich mit diesem jetzt in der fünften Auflage vorliegenden Buch an alle, die wissen wollen, wie Netze und Kommunikationstechnik funktionieren, und was man damit anfangen kann. Dem neugierigen Leser sollen die Spannweite und Funktionsweise der heutigen Datenkommunikation vor Augen geführt werden, ohne dass er dabei allzusehr mit technischen Einzelheiten belastet wird.

Aus dem Inhalt:

- Vom Draht zum Downsizing
- Bauplan/Systemarchitektur von Netzen
- Wie Bits reisen
- PC-Netze, der große Erfolg
- Serverbetriebssysteme: NetWare, Windows , UNIX/Linux
- Integration der Netze und Dienste: ISDN, xDSL, ATM
- Internetworking: Bridging, Routing, Switching
- Entwicklung optischer Netze
- Wireless LANs / Drahtlose Netze
- TCP/IP, Internet, WWW
- GroupWare, Intranet
- Netzwerksicherheit, E-Commerce

