

---

# IT-Sicherheit

---

Konzepte – Verfahren – Protokolle

---

Von  
Claudia Eckert

---

4., überarbeitete Auflage

---

Oldenbourg Verlag München Wien

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Grundlegende Begriffe . . . . .	1
1.2	Schutzziele . . . . .	6
1.3	Schwachstellen, Bedrohungen, Angriffe . . . . .	13
1.4	Computer Forensik . . . . .	25
1.5	Sicherheitsstrategie . . . . .	27
1.6	Sicherheitsinfrastruktur . . . . .	30
<b>2</b>	<b>Spezielle Bedrohungen</b>	<b>35</b>
2.1	Einführung . . . . .	35
2.2	Buffer-Overflow . . . . .	37
2.2.1	Einführung . . . . .	37
2.2.2	Angriffe . . . . .	40
2.2.3	Gegenmaßnahmen . . . . .	43
2.3	Computerviren . . . . .	45
2.3.1	Eigenschaften . . . . .	45
2.3.2	Viren-Typen . . . . .	47
2.3.3	Gegenmaßnahmen . . . . .	53
2.4	Würmer . . . . .	57
2.5	Trojanisches Pferd . . . . .	63
2.5.1	Eigenschaften . . . . .	63
2.5.2	Gegenmaßnahmen . . . . .	65
2.6	Mobiler Code . . . . .	69
2.6.1	Eigenschaften . . . . .	69
2.6.2	Sicherheitsbedrohungen . . . . .	70
2.6.3	Gegenmaßnahmen . . . . .	72
<b>3</b>	<b>Internet-(Un)Sicherheit</b>	<b>75</b>
3.1	Einführung . . . . .	75
3.2	Internet-Protokollfamilie . . . . .	77
3.2.1	ISO/OSI-Referenzmodell . . . . .	77
3.2.2	Das TCP/IP-Referenzmodell . . . . .	83
3.2.3	Das Internet-Protokoll IP . . . . .	85

3.2.4	Das Transmission Control Protokoll <b>TCP</b>	88
3.2.5	Das User Datagram Protocol <b>UDP</b>	90
3.2.6	DHCP und NAT	92
3.3	Sicherheitsprobleme	92
3.3.1	Sicherheitsprobleme von IP	92
3.3.2	Sicherheitsprobleme von ICMP	100
3.3.3	Sicherheitsprobleme von ARP	100
3.3.4	Sicherheitsprobleme von UDP und <b>TCP</b>	104
3.4	Sicherheitsprobleme von <b>Netzdiensten</b>	103
3.4.1	Domain Name Service ( <b>DNS</b> )	109
3.4.2	Network File System ( <b>NFS</b> )	114
3.4.3	Network Information System ( <b>NIS</b> )	120
3.4.4	World Wide Web ( <b>WWW</b> )	122
3.4.5	Weitere Dienste	133
3.4.6	Angriffsszenario	133
3.5	Analysetools und Systemhärtung	144
<b>4</b>	<b>Security Engineering</b>	<b>15</b>
4.1	Entwicklungsprozess	15
4.1.1	Allgemeine Konstruktionsprinzipien	15
4.1.2	Phasen	15
4.1.3	BSI-Sicherheitsprozess	15
4.2	Strukturanalyse	15
4.3	Schutzbedarfsermittlung	15
4.3.1	Schadensszenarien	16
4.3.2	Schutzbedarf	16
4.4	Bedrohungsanalyse	16
4.4.1	Bedrohungsmatrix	16
4.4.2	Bedrohungsbaum	16
4.5	Risikoanalyse	17
4.5.1	Attributierung	17
4.5.2	Penetrationstests	17
4.6	Sicherheitsstrategie und -modell	17
4.7	Systemarchitektur und Validierung	18
4.8	Aufrechterhaltung im laufenden <b>Betrieb</b>	18
4.8.1	Dynamische Überwachung	18
4.8.2	Der elektronische Sicherheitsinspektor ( <b>eSI</b> )	18
4.9	Sicherheitsgrundfunktionen	18
4.10	Realisierung der Grundfunktionen	19
4.11	Beispiel: Elektronische Shopping Mall	19
4.11.1	Systemanforderungen und Einsatzumgebung	19
4.11.2	Bedrohungsanalyse	19

11.3	Risikoanalyse . . . . .	201
11.4	Sicherheitsstrategie . . . . .	206
11.5	Sicherheitsarchitektur . . . . .	209
	<b>Bewertungskriterien</b>	<b>211</b>
1	TCSEC-Kriterien . . . . .	211
1.1	Sicherheitsstufen . . . . .	211
1.2	Kritik am Orange Book . . . . .	214
1.3	Erkennen verdeckter Informationskanäle . . . . .	215
2	IT-Kriterien . . . . .	215
2.1	Mechanismen . . . . .	216
2.2	Funktionsklassen . . . . .	217
2.3	Qualität und Zertifikat . . . . .	218
3	ITSEC-Kriterien . . . . .	219
3.1	Evaluationsstufen . . . . .	220
3.2	Qualität und Bewertung . . . . .	221
4	Zertifizierung . . . . .	222
5	Common Criteria . . . . .	224
5.1	Einführung . . . . .	224
5.2	Überblick über die CC . . . . .	225
5.3	CC-Funktionsklassen . . . . .	230
5.4	Schutzprofile . . . . .	231
5.5	Vertrauenswürdigkeitsklassen . . . . .	233
	<b>Sicherheitsmodelle</b>	<b>241</b>
1	Modell-Klassifikation . . . . .	241
1.1	Objekte und Subjekte . . . . .	242
1.2	Zugriffsrechte . . . . .	243
1.3	Zugriffsbeschränkungen . . . . .	244
1.4	Sicherheitsstrategien . . . . .	244
1.5	Klassifikationsschema . . . . .	246
2	Zugriffskontrollmodelle . . . . .	247
2.1	Zugriffsmatrix-Modell . . . . .	248
2.2	Rollenbasierte Modelle . . . . .	256
2.3	Chinese-Wall Modell . . . . .	263
2.4	Bell-LaPadula Modell . . . . .	268
3	Informationsflussmodelle . . . . .	275
3.1	Verbands-Modell . . . . .	275
4	Einsatz-Leitlinien . . . . .	278
	<b>Kryptografische Verfahren</b>	<b>281</b>
1	Einführung . . . . .	281
2	Steganografie . . . . .	283

7.2.1	Linguistische Steganografie . . . . .	28
7.2.2	Technische Steganografie . . . . .	28
7.3	Grundlagen kryptografischer Verfahren . . . . .	28
7.3.1	Kryptografische Systeme . . . . .	28
7.3.2	Anforderungen . . . . .	29
7.4	Informationstheorie . . . . .	29
7.4.1	Stochastische und kryptografische Kanäle . . . . .	29
7.4.2	Entropie und Redundanz . . . . .	29
7.4.3	Sicherheit kryptografischer Systeme . . . . .	29
7.5	Symmetrische Verfahren . . . . .	30
7.5.1	Permutation und Substitution . . . . .	30
7.5.2	Block- und Stromchiffren . . . . .	30
7.5.3	Betriebsmodi von Blockchiffren . . . . .	30
7.5.4	Data Encryption Standard . . . . .	31
7.5.5	AES . . . . .	32
7.6	Asymmetrische Verfahren . . . . .	32
7.6.1	Eigenschaften . . . . .	32
7.6.2	Das RSA-Verfahren . . . . .	32
7.7	Kryptoanalyse . . . . .	34
7.7.1	Klassen kryptografischer Angriffe . . . . .	34
7.7.2	Substitutionschiffren . . . . .	34
7.7.3	Differentielle Kryptoanalyse . . . . .	34
7.7.4	Lineare Kryptoanalyse . . . . .	34
7.8	Kryptoregulierung . . . . .	34
7.8.1	Hintergrund . . . . .	34
7.8.2	Internationale Regelungen . . . . .	34
7.8.3	Kryptopolitik in Deutschland . . . . .	35
<b>8</b>	<b>Hashfunktionen und elektronische Signaturen</b>	<b>35</b>
8.1	Hashfunktionen . . . . .	35
8.1.1	Grundlagen . . . . .	35
8.1.2	Blockchiffren-basierte Hashfunktionen . . . . .	35
8.1.3	Dedizierte Hashfunktionen . . . . .	36
8.1.4	Message Authentication Code . . . . .	36
8.2	Elektronische Signaturen . . . . .	37
8.2.1	Anforderungen . . . . .	37
8.2.2	Erstellung elektronischer Signaturen . . . . .	37
8.2.3	Digitaler Signaturstandard (DSS) . . . . .	37
8.2.4	Signaturgesetz . . . . .	38
<b>9</b>	<b>Schlüsselmanagement</b>	<b>38</b>
9.1	Zertifizierung . . . . .	38

1.1	Zertifikate . . . . .	390
1.2	Zertifizierungsstelle . . . . .	391
1.3	Public-Key Infrastruktur . . . . .	395
2	Schlüsselerzeugung und -aufbewahrung . . . . .	402
2.1	Schlüsselerzeugung . . . . .	403
2.2	Schlüsselspeicherung und -vernichtung . . . . .	405
3	Schlüsselaustausch . . . . .	408
3.1	Schlüsselhierarchie . . . . .	409
3.2	Naives Austauschprotokoll . . . . .	411
3.3	Protokoll mit symmetrischen Verfahren . . . . .	412
3.4	Protokoll mit asymmetrischen Verfahren . . . . .	416
3.5	Leitlinien für die Protokollentwicklung . . . . .	418
3.6	Diffie-Hellman Verfahren . . . . .	420
4	Schlüsselerückgewinnung . . . . .	426
4.1	Systemmodell . . . . .	427
4.2	Grenzen und Risiken . . . . .	432
<b>0</b>	<b>Authentifikation</b> . . . . .	<b>437</b>
0.1	Einführung . . . . .	438
0.2	Authentifikation durch Wissen . . . . .	440
0.2.1	Passwortverfahren . . . . .	440
0.2.2	Authentifikation in Unix . . . . .	451
0.2.3	Challenge-Response-Verfahren . . . . .	457
0.2.4	Zero-Knowledge-Verfahren . . . . .	462
0.3	Smartcard . . . . .	465
0.3.1	Architektur . . . . .	466
0.3.2	Sicherheit . . . . .	469
0.4	Biometrie . . . . .	478
0.4.1	Einführung . . . . .	478
0.4.2	Biometrische Techniken . . . . .	480
0.4.3	Biometrische Authentifikation . . . . .	484
0.4.4	Fallbeispiel: Fingerabdruckerkennung . . . . .	486
0.4.5	Sicherheit biometrischer Techniken . . . . .	489
0.5	Authentifikation in verteilten Systemen . . . . .	493
0.5.1	RADIUS . . . . .	494
0.5.2	Remote Procedure Call . . . . .	499
0.5.3	Secure RPC . . . . .	500
0.5.4	Kerberos-Authentifikationssystem . . . . .	503
0.5.5	Microsoft Passport-Protokoll . . . . .	514
0.5.6	Authentifikations-Logik . . . . .	529

<b>11</b>	<b>Zugriffskontrolle</b>	<b>53</b>
11.1	Einleitung . . . . .	53
11.2	Speicherschutz . . . . .	54
11.2.1	Betriebsmodi und Adressräume . . . . .	54
11.2.2	Virtueller Speicher . . . . .	54
11.3	Objektschutz . . . . .	54
11.3.1	Zugriffskontrolllisten . . . . .	54
11.3.2	Zugriffsausweise . . . . .	55
11.4	Zugriffskontrolle in Unix . . . . .	55
11.4.1	Identifikation . . . . .	56
11.4.2	Rechtevergabe . . . . .	56
11.4.3	Zugriffskontrolle . . . . .	56
11.5	Zugriffskontrolle unter Windows 2000 . . . . .	56
11.5.1	Architektur-Überblick . . . . .	57
11.5.2	Sicherheitssystem . . . . .	57
11.5.3	Datenstrukturen zur Zugriffskontrolle . . . . .	57
11.5.4	Zugriffskontrolle . . . . .	58
11.6	Verschlüsselnde Dateisysteme . . . . .	58
11.6.1	Einführung . . . . .	58
11.6.2	Klassifikation . . . . .	58
11.6.3	Encrypting File System (EFS) . . . . .	58
11.7	Systembestimmte Zugriffskontrolle . . . . .	59
11.8	Sprachbasierter Schutz . . . . .	59
11.8.1	Programmiersprache . . . . .	59
11.8.2	Übersetzer und Binder . . . . .	59
11.9	Java-Sicherheit . . . . .	60
11.9.1	Die Programmiersprache . . . . .	60
11.9.2	Sicherheitsarchitektur . . . . .	60
11.9.3	Sicherheitsmodelle . . . . .	61
11.9.4	Fazit . . . . .	61
11.10	Trusted Computing . . . . .	61
11.10.1	Einführung . . . . .	61
11.10.2	TCG-Architektur-Überblick . . . . .	62
11.10.3	TPM . . . . .	62
11.10.4	TPM-Schlüssel . . . . .	63
11.10.5	Sicheres Booten . . . . .	63
11.10.6	Einsatzmöglichkeiten für TCG-Plattformen . . . . .	64
11.10.7	Fazit und offene Probleme . . . . .	64
<b>12</b>	<b>Sicherheit in Netzen</b>	<b>65</b>
12.1	Firewall-Technologie . . . . .	65
12.1.1	Einführung . . . . .	65

2.1.2	Paketfilter	655
2.1.3	Proxy-Firewall	670
2.1.4	Applikationsfilter	674
2.1.5	Architekturen	678
2.1.6	Risiken und Grenzen	681
2.2	OSI-Sicherheitsarchitektur	687
2.2.1	Sicherheitsdienste	687
2.2.2	Sicherheitsmechanismen	690
2.3	Sichere Kommunikation	696
2.3.1	ISO/OSI-Einordnung	697
2.3.2	Virtual Private Network (VPN)	704
2.4	IPSec	708
2.4.1	Überblick	710
2.4.2	Security Association und Policy-Datenbank	712
2.4.3	AH-Protokoll	717
2.4.4	ESP-Protokoll	721
2.4.5	Schlüsselaustauschprotokoll IKE	725
2.4.6	Sicherheit von IPSec	730
2.5	Secure Socket Layer (SSL)	736
2.5.1	Überblick	736
2.5.2	Handshake-Protokoll	739
2.5.3	Record-Protokoll	743
2.5.4	Sicherheit von SSL	745
2.6	Sichere Anwendungsdienste	748
2.6.1	Elektronische Mail	748
2.6.2	Elektronischer Zahlungsverkehr	767
<b>3</b>	<b>Sichere mobile und drahtlose Kommunikation</b>	<b>777</b>
3.1	Einleitung	778
3.1.1	Heterogenität der Netze	778
3.1.2	Entwicklungsphasen	779
3.2	GSM	783
3.2.1	Grundlagen	783
3.2.2	GSM-Grobarchitektur	784
3.2.3	Identifikation und Authentifikation	785
3.2.4	Gesprächsverschlüsselung	789
3.2.5	Sicherheitsprobleme	792
3.2.6	Weiterentwicklungen	795
3.2.7	GPRS	797
3.3	UMTS	799
3.3.1	UMTS-Sicherheitsarchitektur	800
3.3.2	Authentifikation und Schlüsselvereinbarung	802

13.3.3	Vertraulichkeit und Integrität . . . . .	80
13.3.4	Fazit . . . . .	80
13.4	Funk-LAN (WLAN) . . . . .	80
13.4.1	Einführung . . . . .	80
13.4.2	Technische Grundlagen . . . . .	81
13.4.3	WLAN-Sicherheitsprobleme . . . . .	81
13.4.4	Einbindung eines WLAN in die Netztopologie . . . . .	82
13.4.5	WEP im Überblick . . . . .	82
13.4.6	WEP-Authentifikation . . . . .	82
13.4.7	WEP-Integrität . . . . .	82
13.4.8	WEP-Vertraulichkeit . . . . .	82
13.4.9	Zusätzliche Sicherheitsmaßnahmen . . . . .	83
13.4.10	Weiterentwicklungen des 802.11-Standards . . . . .	83
13.4.11	802.1X-Framework und EAP . . . . .	83
13.4.12	TKIP . . . . .	84
13.5	Bluetooth . . . . .	84
13.5.1	Einordnung und Abgrenzung . . . . .	84
13.5.2	Technische Grundlagen . . . . .	85
13.5.3	Sicherheitsarchitektur . . . . .	85
13.5.4	Schlüsselmanagement . . . . .	86
13.5.5	Authentifikation . . . . .	86
13.5.6	Bluetooth-Sicherheitsprobleme . . . . .	87
13.6	Future Net . . . . .	87
13.6.1	Entwicklungsstufen . . . . .	87
13.6.2	Vom Informations- zum Wissensmanagement . . . . .	87
13.6.3	Next Generation Networks . . . . .	87
	<b>Literaturverzeichnis</b>	<b>88</b>
	<b>Glossar</b>	<b>89</b>
	<b>Index</b>	<b>90</b>