

Inhaltsverzeichnis

1	Aspekte der Rechnersicherheit	11
	Einleitung	13
	Die »Dreieinigkeit« der Rechnersicherheit	13
	Verfügbarkeit	14
	Integrität	18
	Vertraulichkeit	20
	Sicherheitsverletzungen	22
	Verlust	23
	Ausspähung	23
	Modifikation und Fälschung	24
	Problemstellungen im Rahmen der individuellen Datenverarbeitung	24
	Normen und Gesetze im Bereich ITSEC	30
	Spezielle Regelungen im Strafgesetzbuch	31
	Auswirkungen des Bundesdatenschutzgesetzes	35
	ITSEC	43
	Literaturliste	47
2	IT-Sicherheitskonzepte	49
	Einleitung	51
	Vorgehensmodell	51
	Risikoanalyse	54
	Aufstellung der wesentlichen Bestandteile des IS	55
	Ermittlung der möglichen Schwachstellen	56
	Festlegung von Eintrittswahrscheinlichkeiten	57
	Kostenbetrachtung und Gewichtung	58
	Security Policy	59
	Notfallmanagement	60
	Literaturliste	63
3	Datensicherungen	65
	Einleitung	67
	Sinn und Zweck von Backups	67
	Ziele der Datensicherung	69
	Aufwand für Backup-Maßnahmen	72
	Benutzerverhalten in der Praxis	73

Sicherungsbedürftige Objekte	75
Backup-Medien	78
Bandsicherungsgeräte	80
Disketten	81
Wechselplatten	82
Optische Speichermedien	83
Hard- und Software für Datensicherungen	86
Sicherheits- und Datenschutzaspekte bei Backups	88
Bedienungspersonal und Verantwortlichkeit	90
Organisation, Strategien und Risiken	91
Strategien und Medien	92
Latenzzeit	93
Periodizität	93
Generationen und Alterung	94
Verifikation und Tests	95
Literaturliste	96
4 Zugriffsschutz für Personalcomputer und lokale Netzwerke ..	97
Einleitung	99
Schutzwürdige Daten	101
Bedrohungen	102
Die Grundfunktionen sicherer Systeme	105
Funktionstrennung	106
Identifizierung und Authentisierung	107
Authentisierung durch »Wissen«	107
Paßwort-Regeln	108
Sichere Paßwortspeicherung	111
Sonderproblem Personalcomputer	112
Benutzeranmeldung in Netzen	114
Authentisierung durch »Besitz und Wissen«	115
Magnetstreifen- oder Chipkarte	115
Schlüsselkarten (Tokens) für das Challenge/Response-Verfahren	117
Authentisierung durch »Merkmale«	118
Zugangsschutz in Arbeitspausen	118
Rechteverwaltung und -prüfung	118
Rechtedatei	118
Systemverwaltung	119
Subjekte und Objekte der Rechteverwaltung	119
Rechtevergabe	120
Beweissicherung	120

Wiederaufbereitung	122
Besonderheiten in lokalen Netzen (LAN)	122
Gesetze und Normen	123
Strafgesetzbuch	124
Bundes-Datenschutzgesetz (BDSG)	124
Empfehlungen des Bundesrechnungshofes	125
Das neue Urheberrechts-Gesetz (1993)	125
Bewertungskriterien	126
The Orange Book	126
Das Grüne Buch	127
Die europäischen Bewertungskriterien ITSEC	127
Funktionalitätsklasse F-C2 (Anforderungen)	128
Vertrauenswürdigkeit/Korrektheit Stufe E2	129
Zusammenfassung	130
Auswahlkriterien	131
Literaturliste	132

5 Betriebssysteme	133
Einleitung	135
DOS	136
Zugriffsschutz	137
Speicherschutz	137
Dateischutz	137
Kernel-Schutz	137
OS/2	138
Allgemein	138
Kernel-Schutz	139
Zugriffsschutz	140
Speicherschutz	140
DOS-Emulation (VDM)	141
Dateischutz (Dateisysteme HPFS und FAT)	142
Bedrohung durch Computer-Viren	143
Unix	143
Allgemein	143
Zugriffsschutz	144
Speicherschutz	144
Dateischutz	145
Kernel-Schutz	145
Gefahren	146
Anforderungen an sichere Betriebssysteme	147

6	Netzwerke	149
	Netzwerke	151
	Entscheidung für ein LAN	151
	Einsatzgebiete von Netzwerken	154
	Nachrichtenaustausch	154
	Zentrale Betriebsmittel	156
	Zentraler Datenbestand	158
	Sicherung der Arbeitsplatzrechner	162
	Diskless-Workstation	162
	Zentrale Datensicherung	163
	Sicherung des Dateiservers	164
	Das Netzwerk-Betriebssystem	164
	Unterbrechungsfreie Stromversorgung (UPS)	164
	Standort des Dateiservers	164
	Plattenspiegelung (disk mirroring)	165
	Plattenduplizierung (disk duplexing)	165
	Gespiegelte Server	165
	Abschließende Bemerkung	166
	Literaturliste	166
7	Verschlüsselung	167
	Einleitung	169
	Die Algorithmen	171
	Einweg-Funktionen	171
	Die symmetrischen Verfahren	172
	DES (Data Encryption Standard)	172
	Electronic Code Book (ECB)	173
	Cipher Block Chaining (CBC)	174
	FEAL (Fast Encryption Algorithm)	175
	Asymmetrische Public-Key-Verfahren	175
	RSA-Verfahren	175
	Das Hybrid-Verfahren	177
	Anwendung von Verschlüsselung	177
	Vertraulichkeit	177
	Online-Verschlüsselung	177
	Online-Verschlüsselung lokal	178
	Online-Verschlüsselung im lokalen Netzwerk	179
	Verschlüsselung für die Datenübertragung	179
	Offline-Verschlüsselung	179
	Manipulationsschutz	180
	Elektronische Unterschrift	180
	Schlüssel-Management	182

8 Computer-Anomalien	183
Trojanische Pferde	186
Zeit- bzw. Logikbomben	188
Computerviren	189
Würmer	197
Arten von Computerviren	197
Systemviren	198
Das Booten	200
Festplatten	201
Bootsektor-Viren	202
Benutzerschwachsinn????	204
Partitionssektor-Viren	205
Datei-Viren	206
COM-Dateien	207
EXE-Dateien	208
Batch-Viren	209
Companion-Viren	209
Filesystem-Viren	210
Multi-Partite-Viren	210
Infektionswege	211
Direkt	211
Indirekt	212
Verschlüsselungen	214
Einfache Verschlüsselung	214
Einfache Verschlüsselung mit variablem Schlüssel	214
Polymorphismus	215
Stealth	216
Infektionsposition	217
Bedingungen für die erfolgreiche Verbreitung von Viren	218
Viren in Netzen	218
Schaden	229
Entdeckung von Viren	221
Scanner	221
Offline-Scanner	222
Residente Scanner	223
Integritäts-Checker	223
Entfernung von Viren	224
Standardmaßnahmen	225
Vorsichtsmaßnahmen und Tips	226
Erkennung von Viren mit Standardmitteln	226
Benutzung von Opfer-Dateien	226
Benutzung von Debuggern und Disassemblern	227

9 Computer-Kriminalität	229
Der Betrüger	233
Der Hacker	235
Der Zerstörer	237
Entdeckung und Nachweis eines Computer-Mißbrauchs	238
Stichwortverzeichnis	241

Das Autorenteam dieses Titels:

Horst Görtz	uti-maco GmbH
Oliver Meng	S&S International (Deutschland)
Michael Reinschmiedt	S&S International (Deutschland)
Jörg Steindecker	S&S International (Deutschland)
Morton Swimmer	S&S International (UK)