

Vorwort der Herausgeber 11

Teil I: Bestandsaufnahme 13

1. Bedeutung der EDV 15
2. Begriff der Computerkriminalität 16
3. Umfang des Computer-Mißbrauchs 17

Teil II: Erscheinungsformen und beispielhafte Fälle

von Dr. Karlhans Liebl 25

1. Was mit „Computerkriminalität“ nicht gemeint ist 30
2. Erscheinungsformen der Computerkriminalität —
Falldokumentation 34
2.1 Manipulationen im Zusammenwirken von externen
und internen Tätern 34
2.2 Fälschung von Datenbeständen 45
2.3 Unterdrückung der Datenausgabe oder Verhinderung
des Datenzugriffs 51
2.4 Verschiedene Manipulationen durch Ausnutzung
der EDV-Systeme oder der EDV-Organisation 55
2.5 Wirtschaftsspionage und Computerkriminalität 61
2.6 Zeitdiebstahl 68
2.7 Sabotageakte 70
2.8 Computerkriminalität und Datentransfer 73
2.9 Computerkriminalität im Bereich
neuer Anwendungsgebiete 76
3. Der Computertäter und seine Motive 78

Teil III: Organisatorische und softwaregestützte EDV-Sicherheit

von Volkhart Schönberg	83
1. Risikofaktor EDV	89
1.1 Sicherheit in betrieblichen Abläufen	89
1.2 Neue Aspekte durch die Einführung der EDV	91
2. Merkmale bisher realisierter Sicherheitskonzepte	92
2.1 Alles oder nichts-Prinzip	93
2.2 Vertrauen ist gut — Kontrolle notwendig — Mißtrauen schlecht	93
2.3 Methoden der Maßnahmenauswahl und -installation oft überformalisiert	93
3. Neue Probleme für eine „sichere EDV“	95
3.1 Dezentralisierung der EDV	95
3.2 Zunehmende Vernetzung/Datenfernverkehr	95
3.3 Einführung von Bildschirmtextsystemen	96
3.4 Gesellschaftliche Ablehnung des Computers	96
4. Begriffserklärungen: Datenschutz und Datensicherheit	98
5. Fallstudien	100
5.1 Manipulationen	103
5.2 Datendiebstahl	107
5.3 Sabotage	111
6. Allgemeine Sicherungsgrundsätze	115
6.1 Die Rolle der EDV im Unternehmen	115
6.2 Sensitive Bereiche	116
6.3 Allgemeine Grundsätze	118

7.	Aufbau eines Sicherheitssystems	123
7.1	Erstellen einer Analyse des gesamten EDV-Bereiches .	123
7.2	Umsetzen der allgemeinen Sicherungsgrundsätze	129
7.3	Schwachstellenanalyse	130
7.4	Auswahl der Maßnahmen	137
7.5	Unterstützung durch Software	154
7.6	Unterstützung durch Hardware	161
8.	Besondere Sicherungsmöglichkeiten	167
8.1	Chiffriertechniken	167
8.2	Das Chipkartensystem	177
8.3	Das AIDA Sicherungsverfahren	184
8.4	Security Software: Zugriffskontrollsysteme	187

Teil IV: Physische EDV-Sicherheit

	von Robert Droux	195
1.	Risikobeurteilung im EDV-Bereich	200
1.1	Einführung	200
1.2	Probleme der Sicherung gegen vorsätzliche Handlungen.....	203
1.3	Risikofaktoren	205
2.	Sicherheitsaspekte einer EDV-Gesamtkonzeption	214
2.1	Bedeutung der EDV-Gesamtkonzeption (EGK)	214
2.2	Vorgehen und Organisation	216
2.3	Sicherheitszonen	219
2.4	Raumprogramm, Funktionen und Sicherheit	222

2.5	Hardware-Architektur als Sicherheitsfaktor	229
2.6	Datensicherung	233
3.	Grundlagen der Sicherungsplanung im EDV-Bereich ..	238
3.1	Allgemeines	238
3.2	Risikostellen	238
3.3	Übergeordnete Sicherungsmaßnahmen	239
4.	Sicherheitsaspekte der Bau- und Installationsplanung	248
4.1	Ausgangslage	248
4.2	Gebäude	248
4.3	Elektromagnetische Störeinträge	257
4.4	Elektrostatische Aufladungen	258
4.5	EDV-Klimatisierung	259
4.6	Elektroversorgung	267
5.	Sicherungsmaßnahmen	275
5.1	Grundsätzliche Überlegungen	275
5.2	Mechanische Widerstände und Barrieren	276
5.3	Brandschutz	281
5.4	Wertschutz- bzw. Gefahrenmeldeanlagen	284
5.5	Zutrittskontrolle	288
5.6	Video-Anlagen	296
5.7	Datensicherung in Räumen und Behältnissen	298
6.	Der nukleare elektromagnetische Impuls/NEMP	303
6.1	Ursache und Wirkungen	303
6.2	Mögliche Schutzmaßnahmen	305

Teil V: Die externe Revision als Teil der Abwehrmaßnahmen

von Kaspar Hofmann	307
1. Aufdeckung strafbarer Handlungen	310
1.1 Strafanzeige	310
1.2 Konkreter Tatverdacht	310
1.3 Aufdeckung durch die Revision	311
2. Die Revision — ein systematisch arbeitendes Kontrollorgan	312
2.1 Gesetzlicher Auftrag der externen Revision	312
2.2 Die Arbeitsweise der Revision	314
2.3 Aufgaben der Unternehmensführung	315
2.4 Die EDV als besondere Herausforderung	316
2.5 Präventivwirkung der Revision	317
3. Revisionsmethoden und -techniken, die zur Erzielung einer Präventivwirkung besonders geeignet sind	318
3.1 Analyse der betriebsintern ausgeführten Kontrollmaßnahmen	318
3.2 Einsatz der EDV für die Revision	325
4. Schlußbemerkung	332

Teil VI: Die Aufdeckung von Computerdelikten

von Dr. Erwin Zimmerli und Ernst Angst	333
1. Strafrechtlicher Schutz vor Computerkriminalität in der Schweiz	336
1.1 Zum geltenden Recht	336
1.2 Zur geplanten Revision des StGB (Computerbetrug) ..	338

2.	Strafrechtlicher Schutz vor Computerkriminalität in der Bundesrepublik Deutschland	340
3.	Schwierigkeit der Sachverhaltsabklärung	342
4.	Aufdeckung der verschiedenen Mißbrauchsformen ...	344
4.1	Allgemeine Bemerkungen zur Methode und zum Vorgehen	344
4.2	Computermanipulation	349
4.3	Zeitdiebstahl	365
4.4	Spionage, insbesondere Softwarediebstahl	369
4.5	Sabotage.....	375
5.	Zusammenfassung	379
6.	Checkliste für Schwachstellenanalysen	380
6.1	Risikobereich A Systemsoftware	380
6.2	Risikobereich B Hardware.....	381
6.3	Risikobereich C Organisation	381
6.4	Risikobereich D Verfahren	384
6.5	Risikobereich E Physische Sicherheit	384
Teil VII: Anhang		387
1.	Literaturverzeichnis	389
2.	Sachregister	391