

Datensicherung für Betriebe und Verwaltung

Sicherungsmaßnahmen in der
modernen Informationstechnik
– Erfahrungen aus der Praxis –

Dipl.-Ing. Dr. Horst Abel
und
Dipl.-Ing. (FH) Werner Schmölz

TECHNISCHE HOCHSCHULE DARMSTADT	
Fachbereich 1	
<u>Gesamtbibliothek</u>	
<u>Betriebswirtschaftslehre</u>	
Inventar-Nr. :	<u>41.267</u>
Abstell-Nr. :	<u>A18/1938</u>
Sachgebiete :	<u>1.7.7.6</u>



Verlag C. H. Beck München

Inhalt

1.	Vorwort	1
2.	Informationstechnik und Datensicherung	5
2.1	Computergesellschaft	5
2.1.1	Computer auf dem Vormarsch	5
2.1.2	Moderne Technologie versus Datenschutz	7
2.1.3	Zukunftsperspektiven	8
2.2	Risiken der Informationsverarbeitung	9
2.2.1	Ursachen	9
2.2.2	Computerkriminalität	10
2.2.3	Verarbeitung von Personendaten	12
2.3	Gesetze, Verordnungen und Richtlinien	14
2.3.1	Datenschutzgesetzgebung	14
2.3.2	Rechtsvorschriften zur computergestützten Datenverarbeitung	17
2.3.2.1	Handelsgesetzbuch (HGB)	17
2.3.2.2	Abgabenordnung (AO 1977)	18
2.3.2.3	Grundsätze ordnungsgemäßer Speicherbuchführung (GoS)	18
2.3.3	Bereichsspezifische Regelungen	20
2.4	Datensicherung	23
2.4.1	Allgemeine Bemerkungen	23
2.4.2	Definitionen	25
2.4.3	Typologie der Maßnahmen zur Datensicherung	26
2.4.4	Aufwand und Schutzzweck	27
2.4.5	Schutzstufenkonzept	29
2.4.6	Ergonomie der Datensicherung	31
3.	Objektsicherung	33
3.1	Gebäude und Gebäudebereiche	33
3.1.1	Überwachungszonen und -systeme	35
3.1.1.1	Perimetersicherung	36
3.1.1.2	Außenhautsicherung	36
3.1.1.3	Innenraumsicherung	37
3.1.2	Wirksamkeit von Alarmanlagen	39
3.1.3	Schließsysteme	41
3.2	Rechenzentrum	42
3.2.1	Gefahrenarten	43
3.2.2	Sicherungsmaßnahmen	44
3.2.2.1	Bautechnische Maßnahmen	44
3.2.2.2	Definition von Sicherheitsbereichen	46
3.2.2.3	Zugangskontrolle	47
3.2.3	Notfallmaßnahmen	49
3.2.3.1	Magnetbandarchiv	49
3.2.3.2	Ausweichrechenzentrum	50
3.2.4	Dezentrale Systeme	51
3.2.5	Checkliste Notfallmaßnahmen	52
3.2.5.1	Bauliche Maßnahmen	52
3.2.5.2	Gefahrenbegrenzung durch Alarm- und Brandmeldeanlagen	53
3.2.5.3	Organisatorische Maßnahmen	53

4.	Softwaresicherheit	55
4.1	Sicherheitsfunktionen in Betriebssystemen	55
4.1.1	Standardeinrichtungen	57
4.1.2	Forderungen der Revision	61
4.1.3	Beispiele	62
4.1.3.1	Betriebssystem BS 2000 der Siemens AG	62
4.1.3.2	Betriebssysteme der IBM	65
4.1.3.3	Betriebssystem MPE IV von Hewlett Packard	67
4.1.3.4	Betriebssystem DINOS der Philips AG	68
4.1.3.5	Betriebssystem DIPOS der Nixdorf AG	71
4.1.3.6	Betriebssystem für Personal Computer	72
4.1.4	Forderungen an Betriebssysteme	73
4.1.4.1	Mehrbenutzer-Betriebssysteme für Kleinrechner	73
4.1.4.2	Betriebssysteme für Personal Computer	75
4.1.5	Vireninfiizierte Systeme	76
4.2	Paßwort	78
4.2.1	Vergaberegeln	79
4.2.2	Sicherheit	80
4.2.3	Sicherungsmaßnahmen	81
4.3	Sicherheitssoftware	82
4.3.1	Schutzobjekte	83
4.3.2	Schutzfunktionen	84
4.3.3	Maßnahmen zur Verbesserung des Zugriffsschutzes	85
4.3.4	Besonderheiten beim Einsatz von Personal Computern	89
4.4	Datensicherheit bei Online-Übermittlungen	91
4.5	Sicherungsmaßnahmen bei Datenbanken und in Datenbanksystemen	92
4.5.1	Datenbanken und Datenbanksysteme	92
4.5.2	Gefährdungspotential	93
4.5.3	Datensicherungsmaßnahmen	93
4.5.3.1	Ex-ante-Kontrollmaßnahmen	93
4.5.3.2	Ex-post-Kontrollmaßnahmen	94
4.5.4	Erkennen von Unregelmäßigkeiten	96
4.5.5	Bedeutung der Dokumentation	97
4.5.6	Fragen aus der Praxis	98
4.5.7	Zusammenfassung	99
4.6	Teleprocessing – Monitore	100
4.6.1	Grundfunktionen	100
4.6.2	Datensicherheit am Beispiel von UTM	101
4.6.3	Benutzersteuerung	102
5.	Dokumentation und Revision	105
5.1	Verfahrensdokumentation	105
5.1.1	Elemente der Verfahrensdokumentation	106
5.1.2	Programmierung	109
5.1.2.1	Programmierregeln	109
5.1.2.2	Programmstruktur	109
5.1.2.3	K-Schnittstellen	110
5.1.3	Freigabeverfahren	110
5.1.4	Generatoren und Standardsoftware	112
5.1.5	Programmviren	113
5.1.6	Checkliste Dokumentationsunterlagen	114
5.2	Ablaufdokumentation	115
5.2.1	Rechenzentrumshandbuch	115

5.2.2	Systemverwaltung	116
5.2.3	Operating	120
5.2.4	Arbeitsvorbereitung und Arbeitsnachbehandlung	121
5.2.5	Archivverwaltung	122
5.2.6	Produktions-, Planungs-, Steuerungs- und Kontrollsystem	122
5.2.7	Protokollierung von Online-Abfragen	124
5.3	Nachprüfbarkeit von DV-Aktivitäten	126
5.3.1	Groß-EDV	127
5.3.1.1	Typologie der Ablaufdaten	128
5.3.1.2	Auswertemöglichkeiten	129
5.3.1.3	Ansätze in Betriebssystemen und systemnaher Software	130
5.3.2	Datenverarbeitungssysteme mittlerer Größe	131
5.3.2.1	Art und Inhalt der Aufzeichnung von Ablaufdaten	132
5.3.3	Checkliste zur Protokollierung und Auswertung von Ablaufdaten	133
5.3.3.1	Protokollierung	133
5.3.3.2	Auswertung	135
5.4	Aufbewahrungsfristen	136
6.	Datenkommunikation	139
6.1	Stand der Technik	139
6.1.1	Begriffserklärungen	140
6.1.1.1	Übertragungstechnik	140
6.1.1.2	Vermittlungstechnik	141
6.1.1.3	Dienste	142
6.1.2	Öffentliches Fernsprechnet	146
6.1.3	Öffentliches Integriertes Text- und Datennetz (IDN)	147
6.1.4	Breitbandverteilt	147
6.1.5	Verteiltechniken	147
6.1.5.1	Schnittstellenvervielfacher	147
6.1.5.2	Kanalteilung	148
6.1.5.3	Ferndiagnose über Protokollkonverter	148
6.2	Risiken	148
6.2.1	Übertragungstechnik	149
6.2.2	Vermittlungstechnik	150
6.2.3	Datex-L	151
6.2.4	Datex-P	151
6.2.5	Erschleichen von Berechtigungen	152
6.2.6	Mißbrauch einer erteilten Berechtigung	152
6.2.7	Verteiltechnik	152
6.3	Sicherungsmaßnahmen	153
6.3.1	Sicherung der Leitungen und Anschlüsse	153
6.3.2	Physikalische Sicherung des Systemzugangs	156
6.3.3	Logische Sicherung des Systemzugangs	157
6.3.4	Kontrolle der Systemnutzung	157
6.3.5	Anonymes Netz	157
6.3.5.1	Risiken eines diensteintegrierenden Netzes	158
6.3.5.2	Schutzmaßnahmen	158
6.4	Wide Area Network	160
6.4.1	Mehrrechnersystem (MRS) des Siemens AG	160
6.4.2	Netzwerksicherheit in TRANSDATA PDN	162
6.4.2.1	Begriffe	162
6.4.2.2	Sicherheitskomponenten	162
6.4.2.3	Hinweise für die Praxis	164

7.	Lokale Netze	167
7.1	Aufbau	167
7.2	Standards	168
7.2.1	Aufgaben der Übertragungsprotokolle	170
7.2.2	Physikalisch mögliche Anordnung von Datenverbindungen	171
7.3	Risiken und Sicherungsaspekte	172
7.3.1	Medium-Ebene (Schicht 0)	172
7.3.2	Physikalische Ebene (Schicht 1)	173
7.3.2.1	Stern-System	173
7.3.2.2	Ring-System	173
7.3.2.3	Bus-System	174
7.3.2.4	Baumförmige Systeme	174
7.3.3	Verbindungsebene (Schicht 2)	175
7.3.4	Netzwerkebene (Schicht 3)	177
7.3.5	Transportebene (Schicht 4)	177
7.3.6	Schicht 5 bis Schicht 7	177
7.3.7	Organisatorische Maßnahmen	178
7.3.8	Zusammenfassung	178
7.4	Normierung der LAN-Managementdienste	179
8.	Personal Computer	181
8.1	Ausgangslage	181
8.2	Einsatzmöglichkeiten	182
✓ 8.3	Risiken und Mängel	183
✓ 8.3.1	Systembedingte Mängel	185
✓ 8.3.2	Organisationsbedingte Mängel	186
✓ 8.4	Sicherungsmaßnahmen	187
✓ 8.4.1	Technische Sicherungsmaßnahmen	188
✓ 8.4.2	Organisatorische Sicherungsmaßnahmen	189
✓ 8.4.3	Sicherungsmaßnahmen bei der Vernetzung von Personal Computern	190
8.4.4	Tele-Heimarbeit	192
✓ 8.4.5	Allgemeine Feststellungen	193
8.5	Anregungen für die Praxis	195
8.6	Sicherheitskomponenten	196
8.6.1	HETROLOCK-HS 210, das elektronische Sicherheitsschloß	197
8.6.2	Zugriffsschutz mit Elkey Nr. 1	197
8.6.3	Verschlüsselung mit ULTRA-LOCK	198
8.6.4	Kryptographie mit ABATON	199
8.6.5	Sperren und Verriegeln mit SAFEGUARD	199
8.6.6	Zugriffsschutz mit pc + softlock	200
8.6.7	Festplattenschutz und Revisionsfähigkeit mit CLAVIS und OCULIS	200
8.6.8	Zugriffsschutz mit WATCHDOG	202
8.6.9	Paßwortschutz mit C.P.	202
9.	Bürokommunikation	203
9.1	Büroorganisation heute	203
9.2	Eigenschaften und Komponenten	204
9.3	Wege zur Bürokommunikation	207
9.4	Das Büro von morgen	208
9.5	Chancen	210
9.6	Risiken	212
9.6.1	Nebenstellenanlage	212
9.6.2	Elektronisches Archiv	213

9.7	Sicherungsmaßnahmen	215
9.7.1	Nebenstellenanlagen	215
9.7.2	Bürosysteme	215
9.7.3	Anschluß an den Host	217
9.8	Realisierungen	217
9.8.1	Isolierte Textverarbeitung	218
9.8.2	HICOM der Siemens AG	219
9.8.3	DISOSS der IBM	219
9.8.4	Bürokommunikation mit Mannesmann-Kienzle	220
9.8.5	Sophomation der Philips AG	221
9.8.6	GEI-Konzept	222
10.	Bildschirmtext	223
10.1	Systembeschreibung	223
10.1.1	Allgemeine Bemerkungen	223
10.1.2	Verbindungsaufbau und Sicherung des Benutzerzugangs	226
10.1.3	Freizügigkeit und öffentliche Terminals	229
10.1.4	Persönliches Kennwort	229
10.1.5	Anschlußsperre	230
10.1.6	Editieren	231
10.1.7	Betreiberbezogene Teilnehmerverwaltung (BTV)	232
10.1.8	Dialog	232
10.1.8.1	Mitbenutzer	232
10.1.8.2	Geschlossene Benutzergruppe (GBG)	234
10.1.8.3	Benutzerbezogene Teilnehmerverwaltung (BBTV)	234
10.1.8.4	Mitteilungsdienst	235
10.1.9	Abruf von Anbieterseiten	236
10.1.9.1	Btx-Seitentypen	236
10.1.9.2	Btx-Seitenarten	237
10.1.10	Kennzeichnung von Seiten mit personenbezogenen Daten	238
10.1.11	Dialog mit dem externen Rechner	239
10.1.12	Abrufstatistik	242
10.1.13	Störfall	242
10.1.14	Betriebskonzept der Btx-Leitzentrale	243
10.1.15	Regionale Btx-Vermittlungsstelle	243
10.1.16	Abrechnungsverfahren	244
10.1.17	Datensätze	246
10.1.17.1	Anschlußsatz	246
10.1.17.2	Teilnehmer- und Mitbenutzersatz	246
10.1.17.3	Datensatz für geschlossene Benutzergruppen	247
10.1.17.4	Session-Satz	247
10.1.17.5	Session-Abschlußsatz	247
10.1.17.6	Gebühren- und Entgeltsatz	248
10.2	Sicherheit, Risiken und Sicherungsmaßnahmen	248
10.2.1	Vorhandene Sicherungsmaßnahmen	248
10.2.2	Technische Risiken und Sicherheitsaspekte	250
10.2.2.1	Grundsätzliche Ausführungen	250
10.2.2.2	Risiken für Anbieter	252
10.2.3	Ausblick	253
10.3	Dokumentation von Bildschirmtextanwendungen	254
10.4	Tendenzen von Bildschirmtext	254
10.5	Bildschirmtext als Kommunikationsmedium	256

11.	Neue Kommunikationsdienste	259
11.1	Fernwirkdienst TEMEX der Deutschen Bundespost	260
11.1.1	Leistungsspektrum	260
11.1.2	Technisches Konzept von TEMEX	262
11.1.2.1	TEMEX-Netzabschluß (TNA)	262
11.1.2.2	TEMEX-Unterzentrale (TUZ)	263
11.1.2.3	TEMEX-Hauptzentrale (THZ)	264
11.1.2.4	Service-Anbieter	264
11.1.3	Fernwirkanwendungsmöglichkeiten und Datensicherungs- maßnahmen	265
11.1.4	System- und Betriebsversuche	267
11.1.5	Fernwirkanwendungen außerhalb von TEMEX	267
11.2	Teletex	268
11.3	Telebox	271
11.4	Kabledienste	274
11.5	Bargeldlose Zahlungsmittel	276
11.6	Funk-Dienste	278
11.6.1	Datenfunk	278
11.6.2	Funkfernsprechen	279
12.	Technische Einzelprobleme	281
12.1	Wartung von DV-Systemen	281
12.1.1	Herkömmliche Wartung	283
12.1.2	Fernwartung	283
12.1.3	Maßnahmenkatalog für den Anwender	287
12.1.4	Fragen an den Hersteller	289
12.2	Mikroverfilmung	291
12.2.1	COM-Verfilmung	292
12.2.1.1	Wirtschaftlichkeit	293
12.2.1.2	Datensicherheit	293
12.2.2	Verfilmung von Schriftgut	294
12.2.2.1	Technik der Schriftgutverfilmung	295
12.2.2.2	Auftragsdatenverarbeitung	298
12.2.2.3	Empfehlungen für die Praxis	298
12.2.3	Orientierungshilfe für die Organisation bei der Verfilmung von Schriftgut und bei der Außerhausverfilmung	303
12.2.3.1	Klassifizierung des zu verfilmenden Schriftgutes	303
12.2.3.2	Allgemeine Grundsätze	303
12.2.3.3	Arbeitsschritte der Schriftgutverfilmung und deren Organisation	304
12.2.3.4	Grundsätze bei der Vertragsgestaltung	306
12.3	Kompromittierende Abstrahlung	306
12.3.1	Ausgangslage	306
12.3.2	Physikalische Grundlagen	308
12.3.3	Abhörmethoden	309
12.3.4	Risiken	310
12.3.5	Schutzmaßnahmen	311
12.4	Kryptographische Verfahren	314
12.4.1	Ausgangslage	314
12.4.2	Verschlüsselungstechniken	315
12.4.3	Anwendungen und Bewertung	317
12.4.4	Beispiele für Verschlüsselungstechniken	319
12.4.4.1	Hardwarelösung	319
12.4.4.2	Softwarelösung	320

12.4.5	Problemfälle	321
12.5	Chip-Karten-Technik	322
12.5.1	Einsatzbeispiele für Chip-Karten	324
12.5.1.1	Bankdienstleistungen	324
12.5.1.2	Computerdienstleistungen	326
12.5.1.3	OSIS – Projekt	326
12.5.2	Weitere Einsatzmöglichkeiten	326
12.5.3	Echtheitsprüfung	327
12.5.4	Datenschutz versus Umweltschutz	327
13.	Verarbeitung von Personendaten	329
13.1	Typologie der automatisierten Datenverarbeitung	330
13.1.1	Zur Entwicklung der Datenverarbeitung	330
13.1.2	Arten der Datenverarbeitung	332
13.1.2.1	Stapelanwendungen	332
13.1.2.2	Quasi-Online-Anwendungen	332
13.1.2.3	Dialog-Anwendungen	333
13.1.2.4	Fachinformationszentren und zentrale Auskunftsbanken	334
13.1.2.5	Dedizierte Systeme	334
13.1.2.6	Künftiges DV-Konzept	335
13.1.3	Klassifizierung der Datenbestände	335
13.2	Personenbezogene Daten	336
13.3	Dateienregister	338
13.3.1	Zweck	339
13.3.2	Dateibegriff	340
13.3.3	Meldepflichtige Dateien	341
13.3.4	Grenzfälle	342
13.3.5	Karteierfassung	343
13.4	Personalinformationssysteme	344
13.4.1	Personaldaten	345
13.4.2	Rechtliche Gesichtspunkte	347
13.4.3	Risiken	349
13.4.4	Sicherungsmaßnahmen	351
13.4.5	Standardsysteme	353
13.5	Anonymisierung	355
13.5.1	Grundlagen	355
13.5.2	Risiken großer Datensammlungen	357
13.5.3	Meldungen zum Dateienregister	358
14.	Organisatorische Maßnahmen	361
14.1	Organisation	361
14.1.1	Organisation der Datensicherung	361
14.1.2	Datenschutzbeauftragter	362
14.1.3	Verpflichtung	365
14.1.4	Dateistatut	366
14.2	Versand- und Transportmaßnahmen	368
14.2.1	Versandarten	370
14.2.1.1	Deutsche Bundespost	370
14.2.1.2	Kurier oder Boten	374
14.2.2	Ordnungsgemäßer Transport	375
14.3	Datenverarbeitung im Auftrag	376
14.3.1	Einzelprobleme	377
14.3.2	Grundsätze für Vertragsregelungen	380

14.4	Entsorgung von Datenträgern	381
14.4.1	Ausgangslage	381
14.4.2	Deutsche Sicherheitsnorm DIN 32757	382
14.4.3	Entsorgung vor Ort	384
14.4.4	Sichere Vernichtung außer Haus	386
14.4.5	Wirtschaftlichkeit	387
14.5	Hinweise für Dienstanweisungen zur Datensicherung	388
14.5.1	Grundsätze	388
14.5.2	Stoffsammlung	389
15.	Manuelle Datenverarbeitung	393
15.1	Gewährleistung des Persönlichkeitsschutzes	393
15.1.1	Bauliche Maßnahmen	394
15.1.2	Organisatorische Maßnahmen	395
15.2	Kopierschutz von Schriftstücken und Sicherheitskopierer	396
15.3	Sicherung von Karteien	397
15.3.1	Zugang	399
15.3.2	Aufbewahrung	401
15.4	Orientierungshilfe für technische und organisatorische Maßnahmen bei der Verarbeitung von Dateien in nichtautomatisierten Verfahren	403
15.4.1	Zugang	404
15.4.2	Anlegen und Bearbeiten von Dateien	405
15.4.3	Weitergabe von Daten und Transport von Datenträgern	405
15.4.4	Aufbewahren von Dateien	406
15.4.5	Vernichten von Datenträgern	407
15.4.6	Organisation	408
X 16.	Anhang	409
16.1	Orientierungshilfen	409
16.1.1	Orientierungshilfe für technische und organisatorische Maßnahmen beim Einsatz dezentraler Systeme	410
16.1.1.1	Zugangskontrolle	411
16.1.1.2	Abgangskontrolle	412
16.1.1.3	Speicherkontrolle	413
16.1.1.4	Benutzerkontrolle	414
16.1.1.5	Zugriffskontrolle	415
16.1.1.6	Übermittlungskontrolle	415
16.1.1.7	Eingabekontrolle	415
16.1.1.8	Auftragskontrolle	416
16.1.1.9	Transportkontrolle	416
16.1.1.10	Organisationskontrolle	417
X 16.1.2	Orientierungshilfe für Baumaßnahmen	418
U 16.1.2.1	Feuer	421
16.1.2.2	Wasser	423
16.1.2.3	Versorgungsausfall	423
16.1.2.4	Physikalische und chemische Einwirkungen	423
16.1.2.5	Einwirkungen durch Personen	423
16.1.2.6	Katastrophen- und Notfallplan	424
16.1.2.7	Erläuterungen	424
16.1.3	Orientierungshilfe für bauliche und technisch-organisatorische Maßnahmen zur Datensicherheit für die Installation und den Betrieb von DV-Systemen mittlerer Größe	424
16.1.3.1	Raumauswahl	425

16.1.3.2	Außenhautsicherung	426
16.1.3.3	Zugangssicherung	426
16.1.3.4	Innenraumsicherung	427
16.1.3.5	Brandschutz	427
16.1.3.6	Klimaanlage	427
16.1.3.7	Sicherung der Datenträger	427
16.1.3.8	Sonstiges	428
16.2	Katalog zur Prüfung der technischen und organisatorischen Datensicherungsmaßnahmen	428
16.3	Normen und Richtlinien	444
16.4	Abkürzungen und Erläuterungen	449
16.5	Literaturverzeichnis	461
16.6	Stichwortverzeichnis	465