

Egbert Wald

Backup & Disaster Recovery

Inhaltsverzeichnis

I	Einleitung	II
I.1	„Wie sicher sind meine Daten?“	15
2	Grundlagen und Definitionen	19
2.1	Vision der möglichen Schäden: Katastrophenszenario	19
2.2	Was ist Ausfallzeit („downtime“)?	23
2.3	Was kostet Ausfallzeit?	23
2.4	Wie lange und wie oft kann ich es aushalten „down“ zu sein?	28
2.5	Wovor muss ich mich schützen?	30
2.6	Wie viel Schutz brauche ich?	33
3	Projekt „Aufstellung eines Plans zur Vermeidung bzw. Beseitigung einer IT-Störung“	35
3.1	Vorbereitende Schritte	37
3.2	Sammlung und Dokumentation von relevanten Daten	43
3.3	Risikoanalyse	55
4	Schaffung eines zuverlässigen Systems	63
4.1	Datenbackup	63
4.1.1	Speicher(-Storage)-Management-Definition	64
4.1.2	Netzwerkspeicherarchitektur	64
4.1.3	Die Entwicklung der Datensicherung (Backup)	66
4.1.4	Einzelplatz-Backup	66
4.1.5	Automatisches Backup	68
4.1.6	LAN-Backup	70

4.1.7	Storage-Area-Network(-SAN)-Backup	73
4.1.8	Zukunft der Network-Backup-Software	75
4.1.9	Zukunft der Tape-Drive- & Automation-Hardware	75
4.1.10	Networking-Trends	83
4.1.11	Das neue Modell der Netzwerktypisierung	83
4.1.12	Die externe Datenspeicherung	85
4.1.13	Die NAS(-Network-Attached-Storage)-Architektur	85
4.1.14	Die SAN(-Storage-Area-Network)-Architektur	87
4.1.15	SAN-Vorteile	93
4.1.16	SAN-Weiterentwicklung	94
4.1.17	Das zu speichernde Datenvolumen	95
4.1.18	Netzwerkbackupsoftware	95
4.1.19	Netzwerkbackup-Hardware	121
4.1.20	Tape-Technologie-Übersicht	121
4.1.21	SLR/MLR-Technologie	121
4.1.22	DLT-Technologie	124
4.1.23	Ausblick Tape-Automation	127
4.1.24	Das Medium Band (Tape)	133
4.1.25	Die Bandanzahl	134
4.1.26	Vorschriften zum Umgang mit Medien	135
4.1.27	Checkliste	138
4.1.28	Backup-Praktiken	139
4.1.29	Austauschschema der Bänder	145
4.1.30	Einzelplatzbackup-Umgebung	148
4.1.31	Arbeitsgruppenbackup-Umgebung	149
4.1.32	Zentraladministrierte Backup-Umgebung	150
4.1.33	Backup oder Archive	150
4.1.34	Netzwerkbackup-Trends	151
4.1.35	Backupsoftware-Trends	152
4.1.36	Backuphardware-Trends	152
4.1.37	Rettungstechnologien	152

4.2	Sicherung der Spannungsversorgung	154
4.2.1	Anatomie einer Stromstörung	155
4.2.2	Offline-USV-Anlagen (Mittlaufbetrieb)	160
4.2.3	Line-interactive-USV-Anlage (Netzüberwachungsbetrieb)	161
4.2.4	Online-USV-Anlage (Dauerbetrieb)	162
4.2.5	Richtige Dimensionierung von USVs	164
5	Störschutzplanung	167
5.0.1	Störschutzplan für das „kleine“ Rechenzentrum	168
5.0.2	Störschutzplan für das Netzwerk (LAN – WAN)	176
5.0.3	Störschutzplan für den Endbenutzer	180
5.1	Präsentation der Pläne	189
6	Notfallhandbuch	193
6.1	Inhaltliche Gliederung eines Notfallhandbuches	194
6.2	Sofortmaßnahmen	196
6.2.1	Alarmierung im Notfall	196
6.2.2	Alarmierungsplan und Meldewege	197
6.2.3	Adresslisten betroffener Mitarbeiter	197
6.2.4	Festlegung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall	199
6.2.5	Notrufnummern (z.B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger, Ausweichrechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)	199
6.2.6	Handlungsanweisung für spezielle Ereignisse	201
6.3	Organisatorische Festlegungen	201
6.3.1	Allgemeine Regelungen	201
6.3.2	Notfall-Verantwortliche	201
6.3.3	Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten, Kompetenzverteilung	201
6.3.4	Organisationsrichtlinien, Verhaltensregeln	202
6.3.5	Tabelle der Verfügbarkeitsanforderungen	205
6.3.6	Wiederanlaufpläne für kritische Komponenten	205

6.3.7	Wiederanlaufplan für Komponenten erster Ordnung (z.B. Host)	205
6.3.8	Wiederbeschaffungsmöglichkeiten	206
6.3.9	Interne / externe Ausweichmöglichkeiten	206
6.3.10	DFÜ-Versorgung	207
6.3.11	Eingeschränkter IT-Betrieb	207
6.3.12	Wiederanlaufreihenfolge	207
6.3.13	Wiederanlaufplan für Komponenten zweiter Ordnung (z.B. Drucker)	208
6.4	Dokumentation	209
6.4.1	Wiederanlaufverfahren der IT-Anwendungen	210
6.4.2	Sonstige Unterlagen (Handbücher etc.)	211
6.4.3	Ersatzbeschaffungsplan	212
6.4.4	Verzeichnis der Dienstleistungsunternehmen, Hersteller und Lieferanten	212
7	Erstmaßnahmen im Schadensfall	213
7.1	Checklisten	213
7.2	Grundregeln	221
7.3	Notbetrieb	224
7.3.1	Ausweichsysteme	224
7.3.2	Hilfe durch Dritte	225
7.3.3	Notbetrieb im Netzwerk	226
7.4	Normalbetrieb	226
8	Wiederherstellungstraining (Notfallübungen)	229
8.1	Trainingsprogramm	230
8.2	Beispielformulare für Notfallübungen	244

A	Anhang: Herstellung des Normalbetriebes nach einem Virenbefall	251
A.1	Was ist passiert?	252
A.2	Warum sich Sorgen machen?	254
A.3	Vorgeschichte der Viren	256
A.4	Viren und die Revolution des PCs	257
A.5	Wohin als Nächstes?	260
A.6	Typen von Computerviren	261
A.6.1	Dateiviren	262
A.6.2	Bootsekturviren	263
A.6.3	MBR-(Master-Boot-Record-)Viren	263
A.6.4	Mehrteilige Viren	264
A.6.5	Makroviren	264
A.6.6	Hoax	265
A.7	Was Viren anrichten können	265
A.8	Ausbreitung von Viren	266
A.9	So schützen Sie sich selbst	266
A.10	Entfernen von Viren von Ihrem Computer	269
A.10.1	Erstellen einer Erste-Hilfe-Diskette	270
A.10.2	Reagieren auf Viren oder böswillige Software	271
A.10.3	Reaktion bei Entdeckung eines Virus durch den Online-Scanner	271
A.10.4	Reaktion bei Entdeckung eines Virus durch VirusScan	272
A.11	Was ist ein falscher Alarm?	274
A.12	Virenbeispiele einsenden	276
	Glossar	281
	Stichwortverzeichnis	315