

---

# Inhaltsverzeichnis

<b>1 Einführung: Warum Daten gesichert werden müssen</b> . . . . .	1
1.1 Relevanz von Daten für Unternehmen. . . . .	1
1.2 Herkunft und Nutzung neuer Datenmengen . . . . .	3
1.3 Motivation für Datensicherung . . . . .	6
1.4 Aufbau dieses Buches . . . . .	8
<b>2 Datenvielfalt, Verlustkosten und Aufbewahrungspflichten</b> . . . . .	11
2.1 Datenkategorien . . . . .	12
2.2 Kosten durch fehlende Daten . . . . .	24
2.3 Rechtliche Verpflichtungen . . . . .	25
<b>3 Ursachen für Datenverluste</b> . . . . .	27
3.1 Technische und räumliche Gefahren . . . . .	29
3.2 Operative Gefahren . . . . .	30
3.3 Gefahren durch technologische Unwissenheit . . . . .	33
3.4 Gefahr bei mobilen Geräten . . . . .	34
3.5 Internetkriminalität/Cybercrime . . . . .	35
<b>4 IT-Sicherheit als Ergänzung zur Datensicherung</b> . . . . .	45
4.1 Organisatorische Risikoaspekte der IT-Sicherheit . . . . .	49
4.1.1 IT-Sicherheitsrichtlinie . . . . .	49
4.1.2 Business Continuity und IT-Notfallmanagement . . . . .	57
4.1.3 User Lifecycle Management . . . . .	60
4.2 Technische Risikoaspekte der IT-Sicherheit . . . . .	65
4.2.1 Network Security . . . . .	66
4.2.2 Endpoint Security . . . . .	69
4.2.3 Update- und Patchmanagement . . . . .	72
4.3 Datensicherheit auf Reisen . . . . .	75
4.4 Kategorien der Schutzmaßnahmen . . . . .	77
4.4.1 Präventiv . . . . .	79
4.4.2 Detektierend . . . . .	84
4.4.3 Reaktiv . . . . .	92

4.5	Zusammenhang zwischen Informationssicherheit und digitaler Forensik . . . . .	95
4.5.1	Bedeutung der Datensicherung für die Forensik . . . . .	96
4.5.2	Lessons Learned aus der forensischen Praxis . . . . .	99
<b>5</b>	<b>Datensicherungsstrategie erstellen . . . . .</b>	103
5.1	Das 3-2-1-Prinzip. . . . .	106
5.2	Arten von Speichermedien/Speicherorten . . . . .	107
5.3	Datensicherungsvarianten . . . . .	108
5.4	Geplante Backups und kontinuierliche Datensicherung . . . . .	109
5.5	Schutzmaßnahmen für Datensicherungen . . . . .	110
5.6	Remote-Backups und Cloud-Strategien. . . . .	111
5.7	Exkurs: Optimierung für die Datensicherung . . . . .	112
5.8	Notfallwiederherstellungsplan/Disaster-Recovery-Plan . . . . .	113
5.9	Leitfaden zur Erstellung der Datensicherungsstrategie . . . . .	114
<b>6</b>	<b>Datensicherungsstrategie umsetzen . . . . .</b>	119
6.1	Technischer Aufbau der Sicherungsarchitektur . . . . .	120
6.2	Organisatorischer Aufbau des Sicherungskonzeptes . . . . .	128
6.3	Abdeckung der Risiken durch Anzahl der Backup-Medien . . . . .	130
<b>7</b>	<b>Sicherungskonzept implementieren . . . . .</b>	131
7.1	Konfiguration . . . . .	132
7.2	Kontrolle . . . . .	133
7.3	Rücksicherung . . . . .	135
7.4	Bordmittel ausgewählter Systeme und Plattformen. . . . .	136
7.4.1	Windows für Desktops und Laptops . . . . .	136
7.4.2	Windows Server . . . . .	138
7.4.3	macOS als Desktop, Laptop oder Server . . . . .	139
7.4.4	Weitere Systeme oder Plattformen. . . . .	140
<b>8</b>	<b>Arbeitshilfen und Vorlagen . . . . .</b>	143
8.1	Orientierungshilfe Erstellung Datensicherungsstrategie . . . . .	145
8.2	Orientierungshilfe Aufbau IT-Sicherheitsrichtlinie . . . . .	148
8.3	Orientierungshilfe Aufbau Business Continuity und IT-Notfallmanagement . . . . .	150
8.4	Orientierungshilfe Aufbau User Lifecycle Management . . . . .	152
8.5	Orientierungshilfe Aufbau Network Security . . . . .	154
8.6	Orientierungshilfe Aufbau Endpoint Security . . . . .	156
8.7	Orientierungshilfe Aufbau Update- und Patchmanagement . . . . .	158
8.8	Orientierungshilfe Aufbau Sicherheitsrichtlinie für Auslandsreisen . . . . .	160
8.9	Orientierungshilfe Einführung konkreter Schutzmaßnahmen . . . . .	162
<b>Literatur- und Quellenverzeichnis . . . . .</b>		165
<b>Stichwortverzeichnis . . . . .</b>		169