

---

# Inhaltsverzeichnis

---

1	Ausgangssituation und Zielsetzung .....	1
1.1	Ausgangssituation .....	2
1.1.1	Bedrohungen.....	2
1.1.2	Schwachstellen .....	2
1.1.3	Schutzbedarf.....	5
1.2	Zielsetzung.....	6
1.3	Lösung.....	7
1.4	Zusammenfassung .....	8
2	Kurzfassung und Überblick für Eilige .....	9
3	Definitionen zum Sicherheitsmanagement.....	13
3.1	Sicherheitsmanagement.....	13
3.2	IuK-Sicherheitsmanagement.....	14
3.3	Sicherheit im Lebenszyklus .....	14
3.4	Sicherheitspyramide.....	15
3.5	Sicherheitspolitik.....	15
3.5.1	... nach IT-Grundschutzhandbuch .....	15
3.5.2	... nach ITSEC.....	16
3.5.3	... nach ISO/IEC TR 13335-1, Part 1.....	16
3.5.4	... nach ISO 15408 (Common Criteria).....	17
3.5.5	... nach ISO/IEC 17799:2000.....	17
3.5.6	... nach Dr.-Ing. Müller .....	18
3.5.7	Vergleich.....	18

3.6	Sicherheitsziele.....	19
3.7	Sicherheitstransformation .....	19
3.8	Sicherheitsarchitektur .....	19
3.9	Sicherheitsrichtlinien - Generische Sicherheitskonzepte .....	20
3.10	Spezifische Sicherheitskonzepte .....	20
3.11	Sicherheitsmaßnahmen.....	20
3.12	ProTOPSi.....	20
3.13	Lebenszyklus.....	21
3.14	Sicherheitskriterien .....	21
3.15	Sicherheit.....	21
3.16	Risiko.....	22
3.17	Risikomanagement.....	22
3.18	Zusammenfassung .....	22

## 4

	Die Sicherheitspyramide - Strategie und Vorgehensmodell.....	25
4.1	Überblick.....	25
4.2	Sicherheitshierarchie.....	28
4.2.1	Sicherheitspolitik.....	28
4.2.2	Sicherheitsziele.....	28
4.2.3	Sicherheitstransformation.....	29
4.2.4	Sicherheitsarchitektur.....	29
4.2.5	Sicherheitsrichtlinien.....	29
4.2.6	Spezifische Sicherheitskonzepte.....	29
4.2.7	Sicherheitsmaßnahmen.....	30
4.3	ProTOPSi.....	30
4.4	Prozess- und Systemlebenszyklus.....	30
4.4.1	Geschäfts- und Supportprozess-Lebenszyklus .....	30
4.4.2	Systemlebenszyklus.....	31
4.5	Sicherheitsregelkreis .....	31
4.6	Zusammenfassung .....	32

---

# 5

Sicherheitspolitik.....	33
5.1 Zielsetzung.....	33
5.2 Umsetzung.....	34
5.3 Inhalte.....	34
5.4 Checkliste.....	36
5.5 Praxisbeispiele.....	37
5.5.1 Sicherheitspolitischer Leitsatz Versicherung.....	38
5.5.2 Sicherheitspolitik.....	38
5.6 Zusammenfassung.....	41

# 6

Sicherheitsziele.....	43
6.1 Schutzbedarfsanalyse.....	43
6.2 Schutzbedarfsklassen.....	46
6.3 Tabelle Schadensszenarien.....	47
6.4 Praxisbeispiele.....	50
6.4.1 Schutzbedarf der Geschäftsprozesse.....	51
6.4.2 IuK-Schutzbedarfsanalyse.....	51
6.4.3 Schutzbedarfsklassen.....	54
6.5 Zusammenfassung.....	56

# 7

Sicherheitstransformation.....	57
7.1 Haus der Sicherheit "House of Safety and Security" (HoSS).....	58
7.2 "Safety and Security Function Deployment" (SSFD).....	59
7.2.1 Transformation der Anforderungen auf Sicherheitscharakteristika.....	59
7.2.2 Detaillierung der Sicherheitscharakteristika.....	61
7.2.3 Abbildung der Charakteristika auf den Lebenszyklus.....	61
7.3 Schutzbedarfsklassen.....	61
7.4 Praxisbeispiel.....	62
7.5 Zusammenfassung.....	62

# 8

Sicherheitsarchitektur .....	65
8.1 Überblick.....	65
8.2 Prinzipielle Sicherheitsanforderungen .....	67
8.3 Prinzipielle Bedrohungen.....	67
8.4 Sicherheitsprinzipien und –strategien.....	69
8.4.1 Prinzip der Wirtschaftlichkeit .....	70
8.4.2 Risikostrategie .....	70
8.4.3 Sicherheitsstrategie.....	71
8.4.4 Prinzip der Abstraktion.....	72
8.4.5 Prinzip der Klassenbildung .....	73
8.4.6 Poka-Yoke-Prinzip .....	74
8.4.7 Prinzip der Namenskonventionen .....	75
8.4.8 Prinzip der Redundanz .....	75
8.4.9 Prinzip des "aufgeräumten" Arbeitsplatzes.....	77
8.4.10 Vier-Augen-Prinzip.....	77
8.4.11 Prinzip der Funktionstrennung .....	78
8.4.12 Prinzip der Sicherheitsschalen.....	78
8.4.13 Prinzip der Pfadanalyse .....	78
8.4.14 Prinzip der minimalen Rechte .....	79
8.4.15 Prinzip der minimalen Dienste.....	79
8.4.16 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit.....	79
8.4.17 Prinzip des Closed-Shop-Betriebs und der Sicherheitszonen.....	79
8.4.18 Prinzip der Prozess- und Lebenszyklusimmanenz.....	80
8.4.19 Prinzip der Konsolidierung .....	80
8.4.20 Prinzip der Standardisierung .....	81
8.5 Sicherheitselemente .....	81
8.5.1 Betriebs- (Safety) und Angriffssicherheit (security) .....	82
8.5.2 Managementdisziplinen (Prozesse) im Überblick .....	83
8.5.3 Leistungsmanagement.....	87
8.5.4 Finanzmanagement.....	88
8.5.5 Projektmanagement .....	89

8.5.6	Qualitätsmanagement .....	89
8.5.7	Problemmanagement .....	90
8.5.8	Änderungsmanagement .....	91
8.5.9	Konfigurationsmanagement.....	92
8.5.10	Releasemanagement.....	92
8.5.11	Lizenzmanagement .....	93
8.5.12	Datenschutzmanagement.....	93
8.5.13	Kapazitätsmanagement .....	94
8.5.14	Kontinuitätsmanagement .....	103
8.5.15	Securitymanagement.....	119
8.5.16	Personalmanagement.....	150
8.5.17	Technologie im Überblick .....	153
8.5.18	Organisation im Überblick .....	155
8.5.19	Personal im Überblick .....	155
8.5.20	Lebenszyklus .....	155
8.6	Hilfsmittel Sicherheitsarchitekturmatrix .....	156
8.7	Zusammenfassung .....	157

## 9

	Sicherheitsrichtlinien /-standards- Generische Sicherheitskonzepte.....	159
9.1	Übergreifende Richtlinien.....	160
9.1.1	Sicherheitsregeln .....	160
9.1.2	Prozessvorlagen .....	161
9.1.3	Benutzerordnung .....	163
9.1.4	E-Mail-Nutzung.....	164
9.2	Managementdisziplinen.....	164
9.2.1	Kapazitätsmanagement .....	165
9.2.2	Kontinuitätsmanagement .....	166
9.2.3	Securitymanagement.....	172
9.3	Organisation.....	182
9.4	Zusammenfassung .....	184

---

10	Spezifische Sicherheitskonzepte.....	185
10.1	Kontinuitätsmanagement.....	186
10.1.1	Datensicherung.....	186
10.2	Securitymanagement.....	187
10.2.1	Systemspezifische Passworteinstellungen.....	187
10.3	Zusammenfassung.....	188
11	Sicherheitsmaßnahmen.....	189
11.1	Securitymanagement.....	189
11.1.1	Protokoll Passworteinstellungen.....	189
11.2	Zusammenfassung.....	190
12	Systemlebenszyklus.....	191
12.1	Beantragung.....	192
12.2	Planung.....	192
12.3	Fachkonzept, Anforderungsspezifikation.....	193
12.4	Technisches Grobkonzept.....	193
12.5	Technisches Feinkonzept.....	194
12.6	Entwicklung.....	195
12.7	Integrations- und Systemtest.....	196
12.8	Freigabe.....	196
12.9	Software-Evaluation.....	196
12.10	Auslieferung.....	197
12.11	Abnahmetest und Abnahme.....	197
12.12	Software-Verteilung.....	198
12.13	Inbetriebnahme.....	198
12.14	Betrieb.....	199
12.15	Außerbetriebnahme.....	199
12.16	Hilfsmittel.....	200

---

12.17	Zusammenfassung .....	201
-------	-----------------------	-----

# 13

	Sicherheitsregelkreis .....	203
13.1	Sicherheitsprüfungen .....	203
13.1.1	Sicherheitsstudie/Risikoanalyse .....	203
13.1.2	Penetrationstests .....	205
13.1.3	Security-Scans .....	207
13.2	Sicherheitscontrolling .....	207
13.3	Berichtswesen (Safety-/Security-Reporting) .....	209
13.3.1	Anforderungen .....	209
13.3.2	Inhalte .....	212
13.4	Safety-/Security-Benchmarks .....	214
13.5	Hilfsmittel .....	214
13.6	Zusammenfassung .....	215

# 14

	Reifegradmodell des Sicherheitsmanagements – Safety/Security Management Maturity Model .....	217
14.1	Maturity-Modell .....	217
14.2	Reifegradmodell nach Dr.-Ing. Müller .....	217
14.2.1	Stufe 0: unbekannt .....	218
14.2.2	Stufe 1: begonnen .....	219
14.2.3	Stufe 2: konzipiert .....	219
14.2.4	Stufe 3: standardisiert .....	219
14.2.5	Stufe 4: integriert .....	219
14.2.6	Stufe 5: gesteuert .....	219
14.2.7	Stufe 6: selbst lernend .....	220
14.3	Checkliste .....	220
14.4	Praxisbeispiel .....	222
14.5	Zusammenfassung .....	222

---

# 15

Glossar .....	223
Verzeichnis über Gesetze, Vorschriften, Standards, Normen .....	237
Gesetze, Verordnungen .....	237
Ausführungsbestimmungen, Grundsätze, Vorschriften .....	238
Standards und Normen .....	239
Literatur- und Quellenverzeichnis .....	241
Abbildungsverzeichnis .....	245
Stichwortverzeichnis .....	247
Markenverzeichnis .....	255
Über den Autor .....	257