

Inhalt

8	Abkürzungsverzeichnis
12	Vorwort
22	Vom Hacker zum Cyberkrieger
34	1 Strategie 1: Den Hacker kennen
35	1.1 Wer greift uns an?
36	1.1.1 Kein Angriff ohne Motiv
38	1.1.2 Kein Angriff ohne die notwendige Fähigkeit
39	1.1.3 Erst die Angriffsfläche ermöglicht den Angriff
41	1.2 Sind wir vor dem Angreifer sicher?
44	2 Strategie 2: Security ist Chefsache
45	2.1 Commitment
46	2.2 Vorbildwirkung
48	2.3 Planung und Lenkung
48	2.3.1 Sicherheitsziele & Risikopolitik
49	2.3.2 Management-Review und Reporting
50	2.3.3 Rollen und Ressourcen
52	3 Strategie 3: Schutz der Kronjuwelen
54	3.1 Übersicht zur Vorgangsweise
55	3.2 Identifikation von Informationswerten
55	3.2.1 Herangehensweise: Top-down und Bottom-up
57	3.2.2 Gruppieren von Informationswerten
58	3.2.3 Erhebung der Systeme
59	3.3 Identifikation des Schutzbedarfs
59	3.3.1 Definition von Schutzzielen
61	3.3.2 Bewertung des Schutzbedarfs
63	3.3.3 Klassifizierung von Informationswerten
63	3.4 Schutzmaßnahmen zur Sicherung der Informationswerte
65	3.4.1 Risikoanalyse
67	3.4.2 Auswahl von Schutzmaßnahmen
68	3.4.3 Effektivitätsprüfung und Überwachung von Risiken
70	3.5 Grundhygiene in der Cybersecurity
72	4 Strategie 4: Das Projekt aufsetzen
73	4.1 Warum ein Projekt?
75	4.2 Wie plane ich das Projekt?
75	4.2.1 Projektziele festlegen
75	4.2.2 Das Projekt abgrenzen
76	4.2.3 Darstellung des Projektkontextes

77		4 2 4	Die Tätigkeiten strukturieren
79		4.2.5	Die Projektorganisation einsetzen
79	4.3		Die Projektarbeit
79		4.3 1	Zusammenarbeit fördern
81		4 3 2	Projektmarketing gestalten
82		4.3.3	Projektfortschritt messen und Risiken aufzeigen
86	5		Strategie 5: Organisationsstruktur aufbauen
87	5.1		Informationssicherheits-Managementsystem
87	5 2		Die wichtigsten Rollen im ISMS
88		5.2 1	Die Leitung
88		5 2 2	Informationssicherheitsbeauftragter
89		5 2 3	Schlüsselpersonal
90	5.3		Strukturen schaffen
90		5 3 1	Logging- und Monitoring-Konzept
91		5 3 2	Verwaltung von Werten
92		5.3.3	Compliance-Management
92	5.4		Auf den Ernstfall vorbereitet sein
93	5.5		Was ist notwendig, um richtig reagieren zu können?
93		5 5 1	Notfallmanagement
94		5 5 2	Krisenmanagement
95		5 5 3	Üben und Testen
95	5.6		Integrierter Ansatz der Bewältigung
98	6		Strategie 6: IT-Betrieb sichern
99	6 1		Einleitung
99	6 2		WerteManagement
99		6.2.1	Informationswert
100		6.2.2	Physischer Wert
100		6 2 3	Personen
100	6 3		Backups und Datensicherung
104	6.4		Cloud Security
104		6.4.1	Risiken der Cloud
104		6 4 2	Sicherheit in der Cloud
105	6.5		Systemwartung und sichere Konfiguration
107	6.6		Patch-Management
108		6 6 1	Planen der Patches
109		6 6 2	Testen der Patches
109		6.6.3	Ausrollen der Patches
109	6 7		Netzwerksicherheit
111	6 8		Schutz vor Schadsoftware
112	6.9		Regelmäßige Überprüfungen und Übungen
113		6 9 1	Awareness-Trainings
113		6.9.2	Schwachstellen-Scans
113		6 9 3	Penetration-Tests
114		6 9 4	Red-Team-Assessments

INHALT

116 7 Strategie 7: Physische Sicherheit etablieren

117	7.1	Einleitung
118	7.2	Sicherheitszonen
119	7.2.1	Firmengelände
120	7.2.2	Besprechungsraume
120	7.2.3	Verteilerschranke/-raume
120	7.2.4	Buros
121	7.2.5	Kritische Bereiche
121	7.3	Übergreifende Sicherheitsmaßnahmen
121	7.3.1	Bauliche Maßnahmen
122	7.3.2	Zutrittskontrolle
123	7.3.3	Brandschutz
123	7.3.4	Stromversorgung
123	7.3.5	Weitere Schutzmaßnahmen
125	7.4	Agieren statt reagieren

128 8 Strategie 8: Mitarbeiter begeistern

129	8.1	Einleitung
131	8.2	Training
131	8.2.1	Inhalte
132	8.2.2	Methoden
133	8.2.3	Herausforderung
133	8.3	Motivation
134	8.3.1	Updates
134	8.3.2	Personalisierung
134	8.3.3	Gamification und Serious-Gaming
135	8.3.4	Belohnungssystem

136 9 Strategie 9: Sicher im Homeoffice

137	9.1	Einleitung
137	9.2	Governance
138	9.3	IT-Security
138	9.3.1	Device-Management
139	9.3.2	Bring-Your-Own-Device
141	9.3.3	Verschlüsselung bei Mobile Computing
142	9.3.4	Zugriffsschutz
143	9.3.5	Netzwerksicherheit
144	9.3.6	IT-Operations & Technology
147	9.4	Physische Sicherheit
149	9.5	Awareness
149	9.5.1	Sichere Kommunikation
150	9.5.2	Phishing-Attacken
150	9.6	Datenschutz
151	9.7	Kommunikation im Homeoffice
152	9.8	Zukunft im Homeoffice

154 10 Strategie 10: Qualität steigern

156	10.1	Der KVP-Prozess
158	10.2	Messen der Informationssicherheit
159	10.2.1	KPIs entwickeln

160	10.2.2	Daten sammeln und analysieren
164	10.2.3	Maßnahmen identifizieren und umsetzen
164	10.3	Reporting

166 Ausblick

170 Literatur- und Normenverzeichnis

176 DIE AUTOREN