

Vorwort der ersten Auflage	17
Vorwort	19
1 Ein Sicherheitsprogramm anlegen	29
Die Voraussetzungen schaffen	29
Teams aufstellen	30
Ihre grundlegende Sicherheitslage ermitteln	32
Gefahren und Risiken beurteilen	32
Aufgabenbereich, Assets und Gefahren identifizieren	33
Risiken und Auswirkungen abschätzen	34
Mindern	34
Überwachen	35
Regeln	35
Priorisieren	37
Meilensteine setzen	38
Use-Cases, Tabletop-Übungen und Übungsalarme	39
Ihr Team und Ihre Fähigkeiten erweitern	46
Fazit	47
2 Asset-Management und Dokumentation	49
Was ist Asset-Management?	51
Dokumentation	52
Das Schema einrichten	53
Optionen zur Datenspeicherung	53

	Datenklassifikation	55
	Ihr Inventarisierungsschema verstehen	60
	Schritte zur Implementierung des Asset-Managements	70
	Definieren des Lebenszyklus	70
	Sammeln von Informationen	72
	Das Verfolgen von Änderungen	76
	Überwachung und Berichterstattung	78
	Asset-Management-Richtlinien	78
	Automatisieren	78
	Etablieren einer »Single Source of Truth«	79
	Organisieren eines unternehmensweiten Teams	79
	Suchen Sie Fürsprecher im Management	80
	Bleiben Sie bei der Softwarelizenzierung am Ball	80
	Fazit	81
3	Richtlinien	83
	Sprache und Formulierungen	84
	Dokumentinhalte	85
	Themen	87
	Speicherung und Kommunikation	91
	Fazit	91
4	Standards und Prozeduren	93
	Standards	95
	Prozeduren	97
	Dokumentinhalte	98
	Fazit	99
5	Anwenderschulung	101
	Gestörte Prozesse	102
	Die Lücke schließen	103
	Ihr eigenes Programm aufbauen	103
	Ziele festlegen	104
	Die Ausgangslage feststellen	104
	Umfang und Erstellung von Programmregeln und Richtlinien ...	105

	Positive Verstärkung bieten	105
	Prozesse zur Reaktion auf Sicherheitsvorfälle definieren	106
	Sinnvolle Metriken erhalten	107
	Messungen	107
	Erfolgsrate und Fortschritt verfolgen	107
	Wichtige Metriken	108
	Fazit	108
6	Incident Response – die Reaktion auf Sicherheitsvorfälle	109
	Prozesse	109
	Prozesse, die man vor einem Zwischenfall haben sollte	110
	Incident-Prozesse	111
	Prozesse nach einem Zwischenfall	114
	Werkzeuge und Technologien	114
	Protokollanalyse	115
	EDR/XDR/MDR – alle diese »Rs«	116
	Festplatten- und Dateianalyse	117
	Speicheranalyse	118
	PCAP-Analyse	119
	All-in-one-Werkzeuge	120
	Fazit	120
7	Disaster Recovery	121
	Ziele setzen	122
	Recovery Point Objective	122
	Recovery Time Objective	122
	Wiederherstellungsstrategien	123
	Herkömmliche physische Backups	123
	Warm Standby	124
	Hochverfügbarkeit	125
	Alternatives System	126
	Neuzuweisung von Systemfunktionen	126
	Cloud-natives Disaster Recovery	127
	Abhängigkeiten	128
	Szenarien	129
	Ein Failover auslösen ... und wieder zurück	130

Testen	131
Sicherheitsüberlegungen	131
Fazit	133
8 Industrie-Compliance-Standards und Frameworks	135
Industrie-Compliance-Standards	136
Family Educational Rights and Privacy Act (FERPA)	137
Gramm-Leach-Bliley Act (GLBA)	138
Health Insurance Portability and Accountability Act (HIPAA)	139
Payment Card Industry Data Security Standard (PCI DSS)	140
Sarbanes-Oxley (SOX) Act	141
Frameworks	141
Center for Internet Security (CIS)	142
Cloud Control Matrix (CCM)	142
Das Committee of Sponsoring Organizations of the Treadway Commission (COSO)	142
Control Objectives for Information and Related Technologies (COBIT)	142
Die ISO-27000-Reihe	143
MITRE ATT&CK	144
NIST Cybersecurity Framework (CSF)	144
Regulierte Branchen	144
Die Finanzbranche	145
Die Regierung	145
Gesundheitswesen	147
Fazit	148
9 Physische Sicherheit	149
Physisch	150
Beschränkter Zugriff	150
Videoüberwachung	151
Wartung der Authentifizierungsmaßnahmen	152
Sichere Medien	152
Rechenzentren	153

Operative Aspekte	154
Besucher und Fremdfirmen identifizieren	154
Schulungen zur physischen Sicherheit	156
Fazit	158
10 Microsoft-Windows-Infrastruktur	159
Schnelle Erfolge	159
Upgrade	160
Drittanbieter-Patches	161
Offene Shares	162
Active Directory Domain Services	162
Forests	163
Domänen	164
Domänencontroller	165
Organisationseinheiten	166
Gruppen	166
Accounts	167
Group Policy Objects (GPOs)	168
Fazit	169
11 Unix-Anwendungsserver	171
Auf dem neuesten Stand bleiben	172
Software-Updates von Drittanbietern	172
Updates des eigentlichen Betriebssystems	175
Einen Unix-Anwendungsserver härten	176
Dienste deaktivieren	177
Dateiberechtigungen einstellen	178
Hostbasierte Firewalls benutzen	180
Die Dateintegrität verwalten	181
Separate Festplattenpartitionen konfigurieren	181
chroot benutzen	183
Richten Sie eine Mandatory Access Control ein	184
Fazit	185

12	Endpunkte	187
	Auf dem neuesten Stand bleiben	188
	Microsoft Windows	188
	macOS	189
	Unix-Desktops	190
	Drittanbieter-Updates	190
	Endpunkte härten	191
	Dienste deaktivieren	191
	Desktop-Firewalls benutzen	193
	Die komplette Festplatte verschlüsseln	194
	Schutzwerkzeuge für Endpunkte benutzen	196
	Mobile Device Management	197
	Sichtbarkeit der Endpunkte	197
	Zentralisierung	199
	Fazit	199
13	Datenbanken	201
	Einführung in Datenbanken und deren Bedeutung für die Informationssicherheit	202
	Datenbankimplementierungen	202
	Verbreitete Datenbankmanagementsysteme	203
	Eine Fallstudie aus dem richtigen Leben: der Marriott- Datendiebstahl	204
	Gefahren und Schwachstellen der Datenbanksicherheit	206
	Unberechtigter Zugriff	206
	SQL-Injection	207
	Datenlecks	209
	Bedrohungen von innen	210
	Die Verteidigung umgehen	211
	Best Practices der Datenbanksicherheit	211
	Datenverschlüsselung	212
	Authentifizierungs- und Autorisierungsmechanismen	215
	Konfigurieren und Härten einer sicheren Datenbank	216
	Datenbankmanagement in der Cloud	218
	Praktische Übung: Implementieren einer Verschlüsselung in einer MySQL-Datenbank (Operation Lockdown)	219
	Fazit	221

14	Cloud-Infrastruktur	223
	Arten von Cloud-Diensten und die Implikationen für deren Sicherheit	224
	Software as a Service (SaaS)	224
	Platform as a Service (PaaS)	225
	Infrastructure as a Service (IaaS)	225
	Das Modell der gemeinsamen Verantwortung	225
	Verbreitete Fehler bei der Cloud-Sicherheit und wie Sie diese vermeiden können	226
	Fehlkonfigurationen	227
	Unzulängliche Verwaltung von Zugangsdaten und Geheimnissen	229
	Cloud-Ressourcen mit zu vielen Berechtigungen	232
	Schlechte Sicherheitshygiene	233
	Mangelndes Verständnis für das Modell der gemeinsamen Verantwortung	236
	Best Practices der Cloud-Sicherheit	237
	Beginnen Sie mit sicheren architektonischen Mustern	237
	Geheimnisse richtig verwalten	240
	Setzen Sie auf gut gestaltete Frameworks	241
	Befolgen Sie weiterhin die Best Practices zur Sicherheit	242
	Übung: Einblick in die Sicherheit einer AWS-Umgebung gewinnen	243
	Konfigurieren einer SNS-E-Mail-Benachrichtigung	243
	GuardDuty aktivieren	245
	EventBridge einrichten, um Warnmeldungen an E-Mail umzuleiten	245
	Testen	248
	Fazit	250
15	Authentifizierung	251
	Identity and Access Management	251
	Passwörter	253
	Passwortgrundlagen	253
	Verschlüsselung, Hashing und Salting	257
	Passwortmanagement	260
	Zusätzliche Passwortsicherheit	264

Verbreitete Authentifizierungsprotokolle	265
NTLM	265
Kerberos	267
LDAP	268
RADIUS	269
Unterschiede zwischen Protokollen	270
Protokollsicherheit	272
Das beste Protokoll für Ihre Organisation auswählen	272
Multi-Faktor-Authentifizierung	273
MFA-Schwächen	275
Wo sie implementiert werden sollte	276
Fazit	276
16 Sichere Netzwerkinfrastruktur	279
Geräte härten	280
Firmware-/Software-Patching	280
Dienste	282
SNMP	284
Verschlüsselte Protokolle	286
Managementnetzwerk	286
Hardwaregeräte	287
Bastion-Hosts	288
Router	288
Switches	289
Drahtlosgeräte	290
Design	292
Egress-Filterung	293
IPv6: Ein Hinweis zur Warnung	293
TACACS+	295
Netzwerkangriffe	295
ARP-Cache-Poisoning und MAC-Spoofing	296
DDoS-Amplification	296
VPN-Angriffe	297
Der Drahtlosbereich	297
Fazit	299

17 Segmentierung 301

Netzwerksegmentierung 301

 Physisch 301

 Logisch 303

 Ein Beispiel für ein physisches und logisches Netzwerk 310

 Software-defined Networking 312

Anwendungssegmentierung 312

Segmentierung von Rollen und Verantwortlichkeiten 314

Fazit 316

18 Schwachstellenmanagement 317

Authentifizierte versus nicht authentifizierte Scans 318

Werkzeuge zur Schwachstellenbewertung 321

Open-Source-Werkzeuge 323

Schwachstellenmanagementprogramm 323

 Die Programminitialisierung 324

 Business as Usual 325

Die Priorisierung der Verbesserungen 326

Risikoduldung 328

Fazit 329

19 Entwicklung 331

Die Sprachauswahl 331

 Assembler 332

 C und C++ 333

 Go 333

 Rust 334

 Python/Ruby/Perl 334

 PHP 335

Richtlinien zum sicheren Programmieren 336

Testen 337

 Automatisiertes statisches Testen 337

 Automatisiertes dynamisches Testen 338

 Peer Review 339

Der Software Development Lifecycle 339

Fazit 341

20	OSINT und das Purple Team	343
	Open Source Intelligence	344
	Informations- und Zugriffstypen	344
	Moderne OSINT-Werkzeuge	352
	Purple Teaming	359
	Ein Purple-Teaming-Beispiel	360
	Fazit	363
21	Intrusion-Detection- und Intrusion-Prevention-Systeme verstehen	365
	Rollen in der Informationssicherheit	366
	IDS- und IPS-Typen erkunden	368
	Netzwerkbasierte IDS	368
	Hostbasierte IDS	370
	IPS	374
	NGFWs	375
	IDS und IPS in der Cloud	376
	AWS	378
	Azure	378
	GCP	379
	Mit IDS und IPS arbeiten	380
	Falsch-Positive verwalten	381
	Ihre eigenen Signaturen schreiben	382
	IDS/IPS-Positionierung	384
	Verschlüsselte Protokolle	385
	Fazit	387
22	Protokollierung und Überwachung	389
	SIEM – Security Information and Event Management	389
	Wieso sollte man ein SIEM benutzen?	390
	Der Umfang der Abdeckung	391
	Das SIEM entwerfen	392
	Protokollanalyse und -anreicherung	394
	Sysmon	394
	Gruppenrichtlinie	399

Beispiele für Warnungen und Protokollierungsquellen, auf die Sie sich konzentrieren sollten	400
Authentifizierungssysteme	400
Anwendungsprotokolle	401
Cloud-Dienste	401
Datenbanken	404
DNS	404
Lösungen zum Schutz von Endpunkten	405
IDS/IPS	405
Betriebssysteme	406
Proxy- und Firewall-Protokolle	406
Benutzer-Accounts, Gruppen und Berechtigungen	407
Die Konfiguration testen und fortsetzen	408
An Detection-Frameworks, Compliance-Mandaten und Use-Cases ausrichten	409
MITRE ATT&CK	409
Sigma	410
Compliance	411
Use-Case-Analyse	411
Fazit	413
23 Und noch einen Schritt weiter!	415
E-Mail-Server	415
DNS-Server	418
Security through Obscurity	421
Nützliche Ressourcen	421
Bücher	422
Blogs	422
Podcasts	423
Websites	423
Index	425