

Inhaltsübersicht

	Einleitung	1
1	Grundlagen des Testens der Sicherheit	5
2	Zweck, Ziele und Strategien von Sicherheitstests	65
3	Sicherheitstestprozesse	101
4	Sicherheitstesten im Softwarelebenszyklus	161
5	Testen von Sicherheitsmechanismen	209
6	Menschliche Faktoren beim Test der IT-Sicherheit	289
7	Auswertung von Sicherheitstests und Abschlussberichte	317
8	Sicherheitstestwerkzeuge	331
9	Standards und Branchentrends	341
	Anhang	365
A	Abkürzungen	367
B	Literaturverzeichnis	371
	Index	389

Inhaltsverzeichnis

	Einleitung	1
1	Grundlagen des Testens der Sicherheit	5
1.1	Sicherheitsrisiken	5
1.1.1	Die Rolle der Risikobewertung beim Testen der Sicherheit	5
1.1.1.1	ISO 31000	6
1.1.1.2	Das Risiko im Detail	8
1.1.1.3	Grenzen der Risikobewertung	11
1.1.2	Ermittlung der Assets	12
1.1.2.1	Wert eines Assets	14
1.1.2.2	Der Ort eines Assets	16
1.1.2.3	Der Zugriff auf ein Asset	16
1.1.2.4	Der Schutz von einem Asset	17
1.1.3	Analyse von Verfahren der Risikobewertung	18
1.2	Informationssicherheitsrichtlinien und -verfahren	21
1.2.1	Verstehen von Informationssicherheitsrichtlinien und -verfahren	21
1.2.2	Analyse von Sicherheitsrichtlinien und -verfahren	38
1.3	Sicherheitsaudits und ihre Rolle beim Testen der Sicherheit	45
1.3.1	Zweck und Beispiele eines Sicherheitsaudits	47
1.3.2	Risikomodelle für den praktischen Umgang mit Sicherheitsrisiken	48
1.3.3	Mensch, Prozess und Technik	59
1.4	Was Sie in diesem Kapitel gelernt haben	62

2	Zweck, Ziele und Strategien von Sicherheitstests	65
2.1	Einleitung	65
2.1.1	Unbefugtes Kopieren von Anwendungen oder Dateien	66
2.1.2	Fehler in der Zugangskontrolle	67
2.1.3	Cross-Site Scripting (XSS)	67
2.1.4	Pufferüberläufe	68
2.1.5	Dienstblockade (Denial of Service)	69
2.1.6	Man-in-the-Middle-Angriffe und Brechen von Verschlüsselungen	69
2.1.7	Logische Bombe	71
2.1.8	Code Injection (CI)	71
2.2	Der Zweck von Sicherheitstests	72
2.3	Der Unternehmenskontext	72
2.4	Ziele von Sicherheitstests	74
2.4.1	Informationsschutz und Sicherheitstests	74
2.4.2	Ermittlung von Sicherheitstestzielen	75
2.4.2.1	Betrachtung am Beispiel eines mittelständischen Unternehmens	77
2.5	Der Umfang von Sicherheitstests und die Überdeckung von Sicherheitstestzielen	80
2.5.1	Typische Phasen eines Sicherheitstests	80
2.5.2	Umfang von Sicherheitstests	81
2.6	Vorgehensweisen im Sicherheitstest	83
2.6.1	Bestandteile der Vorgehensweise im Sicherheitstest	84
2.6.2	Ursachen mangelhafter Sicherheitstests	87
2.6.2.1	Mangelndes Engagement der Führungsebene und fehlende Bereitstellung von Ressourcen	88
2.6.2.2	Mangelhafte Implementierung der Sicherheitstestvorgehensweise, fehlende Kompetenzen oder Werkzeuge	89
2.6.2.3	Fehlende Unterstützung seitens des Unternehmens oder der Stakeholder	90
2.6.2.4	Fehlendes Verständnis für Sicherheitsrisiken	90
2.6.2.5	Testvorgehensweise, Teststrategie und übergeordnete Richtlinien passen nicht zusammen	91
2.6.2.6	Fehlendes Verständnis für den Zweck des Systems und fehlende technische Informationen .	91

2.6.3	Der Sicherheitstest als Business Case aus Sicht der Stakeholder	92
2.6.3.1	Sicherheitstest als Business Case	93
2.6.3.2	Stakeholder	94
2.7	Optimierung der Sicherheitstestpraktiken	96
2.7.1	Überdeckungsgrade für Sicherheitsrisiken	97
2.7.2	Überdeckungsgrade von Sicherheitsrichtlinien und Strategien für den Test	98
2.7.3	Überdeckungsgrade von Sicherheitsanforderungen für den Test	98
2.7.4	KPIs für die Wirksamkeit von Sicherheitstests	98
2.8	Was Sie in diesem Kapitel gelernt haben	99
3	Sicherheitstestprozesse	101
3.1	Einleitung	101
3.1.1	Der Sicherheitstestprozess basierend auf dem Testprozess nach ISTQB®	102
3.1.2	Ausrichtung des Sicherheitstestprozesses an einem bestimmten Entwicklungslebenszyklusmodell	109
3.2	Planung von Sicherheitstests	118
3.2.1	Ziele der Sicherheitstestplanung	119
3.2.2	Das Sicherheitstestkonzept	120
3.3	Entwurf von Sicherheitstests	123
3.3.1	Entwurf von Sicherheitstests für Anwendungen	124
3.3.1.1	Sicherheitsmechanismen, -risiken und Schwachstellen	128
3.3.1.2	Dokumentation von Sicherheitstests	147
3.3.2	Entwurf von Sicherheitstests gestützt auf Richtlinien und Verfahren	148
3.4	Ausführung von Sicherheitstests	152
3.4.1	Schlüsselemente und Merkmale einer effektiven Sicherheitstestumgebung	152
3.4.2	Bedeutung von Planung und Genehmigungen für Sicherheitstests	155
3.5	Bewertung von Sicherheitstests	157
3.6	Wartung von Sicherheitstests	159
3.7	Was Sie in diesem Kapitel gelernt haben	159

4	Sicherheitstesten im Softwarelebenszyklus	161
4.1	Die Rolle der Sicherheit im Softwarelebenszyklus	161
4.1.1	Der Softwarelebenszyklus und Lebenszyklusmodelle	162
4.1.2	Sicherheit in den Phasen des Softwarelebenszyklus	165
4.1.3	Die Ermittlung von Sicherheitsanforderungen	166
4.1.4	Der Entwurf sicherer Software	168
4.1.5	Die Implementierung sicherer Software	169
4.1.6	Die Integration und Verifikation sicherer Software	171
4.1.7	Die Transition sicherer Software	172
4.1.8	Die Aufrechterhaltung der Sicherheit während des Betriebs	172
4.1.9	Sicherheitstesten im Softwarelebenszyklus	174
4.2	Die Rolle des Sicherheitstestens in der Anforderungsermittlung . . .	177
4.3	Die Rolle des Sicherheitstestens beim Entwurf	180
4.4	Die Rolle des Sicherheitstestens während der Implementierung . . .	184
4.4.1	Der statische Test von Softwarekomponenten	185
4.4.2	Der dynamische Test von Softwarekomponenten	186
4.4.2.1	Whitebox- und Glassbox-Sicherheitstests	187
4.4.2.2	Anforderungsbasierte und risikobasierte Sicherheitstests	188
4.4.2.3	Abdeckungsmaße zur Bewertung von Sicherheitstests	189
4.5	Die Rolle des Sicherheitstestens während der Integration & Verifikation	193
4.5.1	Sicherheitstests während der Komponentenintegration . . .	193
4.5.2	Sicherheitstesten während des Systemtests	195
4.6	Die Rolle des Sicherheitstestens in der Transitionsphase	197
4.6.1	Sicherheitstesten im Abnahmetest	197
4.6.2	Definition und Pflege sicherheitsbezogener Abnahmekriterien	198
4.6.3	Zusätzliche Umfänge betrieblicher Abnahmetests	201
4.7	Die Rolle des Sicherheitstestens während Betrieb & Wartung	202
4.7.1	Sicherheitstesten als Regressions- und Fehlernachtest	202
4.7.2	Penetrationstest	205
4.8	Was Sie in diesem Kapitel gelernt haben	206

5	Testen von Sicherheitsmechanismen	209
5.1	Systemhärtung	209
5.1.1	Das Konzept der Systemhärtung	209
5.1.2	Testen der Wirksamkeit der Mechanismen der Systemhärtung	215
5.2	Authentifizierung und Autorisierung	217
5.2.1	Authentizität und Authentisierung	217
5.2.2	Der Zusammenhang zwischen Authentifizierung und Autorisierung	219
5.2.3	Testen der Wirksamkeit von Authentifizierungs- und Autorisierungsmechanismen	221
5.3	Verschlüsselung	225
5.3.1	Das Konzept der Verschlüsselung	225
5.3.1.1	Kryptografische Grundprinzipien	226
5.3.1.2	Symmetrische Verschlüsselungen	228
5.3.1.3	Asymmetrische Verschlüsselungen	231
5.3.1.4	Hashverfahren	232
5.3.1.5	Transport Layer Security (TLS)	233
5.3.2	Testen der Wirksamkeit gängiger Verschlüsselungsmechanismen	233
5.3.2.1	Tests auf Designschwächen der Verschlüsselung	233
5.3.2.2	Tests auf Schwachstellen in der Implementierung	236
5.3.2.3	Prüfung auf Schwachstellen in der Konfiguration von Verschlüsselungssystemen	237
5.4	Firewalls und Netzwerkzonen	238
5.4.1	Konzepte von Firewalls	239
5.4.1.1	Paketfilterung	240
5.4.1.2	Proxy-Firewall (Vermittler)	244
5.4.1.3	Applikationsfilter	245
5.4.1.4	Dual-Homed Bastion	246
5.4.2	Testen der Wirksamkeit von Firewalls	247
5.4.2.1	Testen der Konfiguration einer Firewall	247
5.4.2.2	Portscans	249
5.4.2.3	Fehlerhafte Netzwerkpakete und Netzwerk-Fuzzing	250
5.4.2.4	Fragmentierungsangriffe	251
5.4.2.5	IT-Grundschutz einer Firewall	252

5.5	Angriffserkennung	253
5.5.1	Verstehen des Konzepts von Werkzeugen zur Angriffserkennung	253
5.5.2	Testen der Wirksamkeit von Werkzeugen der Angriffserkennung	257
5.5.3	Verfahren für die Anomalieerkennung zur Identifikation von Angriffen	260
5.6	Schadprogrammsscans	261
5.6.1	Konzepte der Schadprogrammscanner	264
5.6.2	Testen der Wirksamkeit von Schadprogrammscannern ..	265
5.7	Datenmaskierung	267
5.7.1	Konzept der Datenmaskierung	268
5.7.1.1	Techniken der Datenmaskierung	270
5.7.1.2	Diskussion ausgewählter Techniken der Datenmaskierung	274
5.7.2	Testen der Wirksamkeit von Datenmaskierungs- verfahren sowie maskierter Daten	275
5.8	Schulungen	277
5.8.1	Bedeutung von Sicherheitsschulungen	278
5.8.2	Testen der Wirksamkeit von Sicherheitsschulungen	280
5.8.2.1	Der Schulungsprozess	280
5.8.2.2	Szenarien während der Schulung	282
5.8.2.3	Wirksamkeit von Übungen und Prüfungen im Sicherheitstesten	284
5.9	Was Sie in diesem Kapitel gelernt haben	285
6	Menschliche Faktoren beim Test der IT-Sicherheit	289
6.1	Motivation	289
6.2	Kommunikationsmodelle für Social Engineers	291
6.2.1	Kanalmodell nach Berlo	291
6.2.2	Kommunikationsquadrat nach Friedemann Schulz von Thun	292
6.2.3	Feedback nach den logischen Ebenen nach Dilts	293
6.2.4	Wertemodell nach Graves/Falter/Mottok	294

6.3	Verstehen der Angreifer	296
6.3.1	Der Einfluss des menschlichen Verhaltens auf Sicherheitsrisiken	296
6.3.2	Verstehen der Mentalität von Angreifern	298
6.3.3	Allgemeine Motive und Quellen für Angriffe auf Computersysteme	300
6.3.4	Angriffsszenarien und -motive	303
6.3.4.1	Erfassung und Authentifizierung	303
6.3.4.2	Reaktion bei Sicherheitsstörfällen	304
6.3.4.3	Analyse und Beweissicherung	304
6.4	Social Engineering	306
6.5	Sicherheitsbewusstsein	308
6.5.1	Die Bedeutung des Sicherheitsbewusstseins	308
6.5.2	Schärfung des Sicherheitsbewusstseins	310
6.6	Zwei Fallbeispiele	311
6.7	Reverse Social Engineering	313
6.8	Social Engineering Pentests	314
6.9	Was Sie in diesem Kapitel gelernt haben	314
7	Auswertung von Sicherheitstests und Abschlussberichte	317
7.1	Auswertung von Sicherheitstests	317
7.2	Berichterstattung für Sicherheitstests	322
7.2.1	Abschlussbericht für Sicherheitstests	323
7.2.2	Sicherheitstestzwischenberichte	326
7.3	Wirksamkeit von Sicherheitstestberichten	327
7.4	Vertraulichkeit von Sicherheitstestergebnissen	329
7.5	Was Sie in diesem Kapitel gelernt haben	330
8	Sicherheitstestwerkzeuge	331
8.1	Typen und Funktionen von Sicherheitstestwerkzeugen	331
8.1.1	Werkzeuge für dynamische Sicherheitstests	331
8.1.2	Statische und dynamische Sicherheitstestwerkzeuge	333

8.2	Werkzeugauswahl	335
8.2.1	Analysieren und Dokumentieren von Sicherheits- testerfordernissen	335
8.2.2	Open-Source-Werkzeuge und kommerzielle Produkte ...	337
8.3	Was Sie in diesem Kapitel gelernt haben	339
9	Standards und Branchentrends	341
9.1	Sicherheitsteststandards und Sicherheitsnormen	341
9.1.1	Die Vor- und Nachteile der Verwendung von Standards und Normen	344
9.1.2	Anwendungsszenarien von Standards und Normen	348
9.1.2.1	BSI-Gesetz	349
9.1.2.2	DSGVO	350
9.1.2.3	BAIT/VAIT	354
9.1.3	Auswahl von Sicherheitsstandards und -normen	355
9.2	Anwenden von Sicherheitsstandards	357
9.3	Branchen- und andere Trends	359
9.4	Was Sie in diesem Kapitel gelernt haben	364
Anhang		365
A	Abkürzungen	367
B	Literaturverzeichnis	371
	Index	389