
Inhaltsverzeichnis

Teil I White Chapter: Theorie

1	Ursprung und Chroniken des Human Hacking	3
1.1	Socratic Questioning und das Trojanische Pferd	3
1.2	Verschwörung des Catilina im antiken Rom	8
1.3	Von Hofnarren bis hin zur Druckerpresse	9
1.4	Geburtsstunde der globalen intelligenten Services	11
1.5	Beginn des Zeitalters des Internets	14
1.6	Zusammenfassung unserer historischen Reise.	16
	Literatur.	17
2	Definition: Social Engineering	19
2.1	Die vier Seiten einer Nachricht	19
2.2	Anthropologische Dimension des Social Engineering.	20
2.3	Terminologische Dimension des Social Engineering	22
2.4	Defizitäre terminologische Darstellung	24
2.5	Zusammenfassung: Ganzheitliche Definition zum Social Engineering	25
	Literatur.	27
3	Anwendungsgebiet des Social Engineering	29
3.1	Triangulation der Informationssicherheit.	30
3.2	Die Eigenschaften der Triangulation der Informationssicherheit	32
3.3	Zusammenfassung: Holistischer Charakter der Informationssicherheit	32
	Literatur.	33
4	Psychologische Hintergründe zum Social Engineering	35
4.1	Hilfsbereitschaft, Lob und Anerkennung	37
4.2	Rollen, Normen und Werte.	39
4.3	Ehrlichkeit	41
4.4	Integrated Behavior Model im Kontext des Social Engineering	42
4.5	Praktisches Verständnis für IBM	47
4.6	Postbote und Systeme von Kahneman	50

4.7	Emotionale Reiz-Reaktions-Kette	53
4.8	Machtverhältnisse und Autorität	57
4.9	Druck und Dringlichkeit	58
4.10	Ego und unsere Lieblingssünde „Eitelkeit“	59
4.11	Angst	62
4.12	Neugier	63
4.13	Leichtgläubigkeit	63
4.14	Reziprozitätsprinzip – wie du mir, so ich dir	64
	Literatur	66
5	Arten des Social Engineering	67
5.1	Human-based Social Engineering	69
5.2	Computer-based Social Engineering	69
5.3	Reverse Social Engineering	71
	Literatur	72
6	Wie läuft ein Social Engineering-Angriff ab?	73
6.1	Angriffszyklusmodell von Mitnick/Simon	73
6.2	Eingeschränktheit des Angriffszyklusmodells von Mitnick/Simon	75
6.3	Social-Engineering-Angriffszyklusmodell	76
6.4	HUMINT	78
6.5	OSINT	82
6.5.1	Bedeutung von OSINT im Kontext von Social Engineering	83
6.5.2	Ursprung und Entwicklung von OSINT	83
6.5.3	OSINT-Grundlagen	84
	Literatur	88
7	Evolution des Social Engineering	89
7.1	Modifiziertes Catfishing im Kontext des Social Engineering	92
7.2	KI-basierte OSINT und Phishing	93
7.3	KI-basiertes Cross-Site Scripting und Keylogger	94
7.4	KI-basiertes Cybergrooming und Sextortion	95
7.5	KI-basierte Desinformationskampagnen und Deepfakes	97
7.6	Virtuelle HUMINT	98
7.7	Zusammenfassung	99
	Literatur	100
8	Globale Verteidigungskonzepte	103
8.1	Observe-Orient-Decide-Act-Loop (OODA-Loop)	105
8.1.1	Ursprung der OODA-Loop	105
8.1.2	Schlüsselkonzepte der OODA-Loop	108
8.1.3	Anwendungsszenarien der OODA-Loop im Social Engineering	111
8.1.4	Observe und Orient mit Beobachtungsmatrix	112
8.1.5	Decide mit Resilienzplan	117

8.1.6	Act and Information Security Awareness und Training	120
8.1.7	Act mit dem Social-Engineering-Pentest	124
	Literatur	127

Teil II Black Chapter: Angriffstechniken

9	Business Email Compromise (BEC)	131
	Literatur	133
10	Ceo-Fraud Geschäftsführerbetrug	135
10.1	Fallbeschreibung: CEO-Fraud Sparkasse Pforzheim Calw	138
10.2	Analyse	139
10.3	Zusammenfassung	142
	Literatur	143
11	Shoulder Surfing	145
11.1	Aktive versus passive Variante	146
11.2	Analyse	146
11.3	Zusammenfassung	148
12	Dumpster Diving	149
12.1	Techniken des Dumpster Diving und ihre Anwendungen	150
12.2	Analyse	152
12.3	Zusammenfassung	154
	Literatur	155
13	Tailgating	157
13.1	Techniken des Tailgating und seine Anwendungen	158
13.2	Analyse	159
13.3	Zusammenfassung	161
14	Vishing	163
14.1	Vishing versus Spear-Vishing	163
14.2	Analyse	165
14.2.1	Unsichtbare Gefahr	166
14.2.2	Verborgene Gefahr	167
14.2.3	Erfolgreiche Gefahr	168
14.3	Zusammenfassung	169
	Literatur	170
15	Enkelkind-Betrug	171
15.1	Formen des Enkelkind-Betrugs	171
15.2	Analyse	176
15.3	Zusammenfassung	178

16	Phishing	179
16.1	Formen des Phishings	179
16.1.1	One-against-many-Taktik	181
16.1.2	One-on-one-Taktik (Spear Phishing)	184
16.2	Analyse	186
16.3	Zusammenfassung	190
	Literatur	191
17	Smishing	193
17.1	Formen des Smishing	193
17.2	Analyse	195
17.3	Zusammenfassung	196
	Literatur	196
 Teil III Yellow Chapter: Anomalieerkennung und Abwehrstrategien		
18	Technisches Basisverteidigungskonzept	199
	Literatur	202
19	Technische Abwehrtaktiken	203
19.1	Technische Abwehrtaktiken gegen BEC	203
19.1.1	Technische Verhaltensanalyse	203
19.1.2	Verschlüsselung von E-Mails	203
19.1.3	E-Mail-Whitelisting	204
19.1.4	E-Mail-Absicherungstechnologie	205
19.1.5	Identitätsprüfung durch technische Verifikationskette	206
19.2	Technische Abwehrtaktiken gegen Shoulder Surfing	207
19.2.1	Blickschutztechnologien	207
19.2.2	Automatische Bildschirmverdunkelung	207
19.2.3	Bewegungssensoren und Gesichtserkennung	208
19.2.4	Verzerrungstechnologien	208
19.2.5	Aktive Bildschirmmaskierung	208
19.3	Technische Abwehrtaktiken gegen Dumpster Diving	209
19.3.1	Daten- und Festplattenverschlüsselung	209
19.3.2	Remote Data Wiping	209
19.3.3	Secure File Deletion	210
19.3.4	Geofencing für digitale Geräte	210
19.3.5	Data-Loss-Prevention-(DLP-)Software	211
19.3.6	Verschlüsselte Kommunikation bei der Entsorgung	211
19.3.7	Überwachung von Geräteaktivitäten	211
19.4	Technische Abwehrtaktiken gegen Tailgating	212
19.4.1	Multifaktorauthentifizierung (MFA) für den Zugang zu sensiblen Bereichen	212
19.4.2	Zugriffsprotokollierung und -überwachung	213

19.4.3	Biometrische Authentifizierung für IT-Räume.....	214
19.4.4	Videoanalyse und KI-Überwachung	214
19.4.5	Automatische Zutrittskontrolle	215
19.4.6	RFID-Zugangskarten mit Zeitzonebeschränkungen	216
19.5	Technische Abwehrtaktiken gegen Vishing	216
19.5.1	Anrufauthentifizierungssysteme.....	216
19.5.2	Whitelisting für legitime Anrufquellen	217
19.5.3	Call-Filtering-Technologien.....	217
19.6	Technische Abwehrtaktiken gegen Phishing	218
19.6.1	E-Mail-Authentifizierung auf Anwendungsebene	218
19.6.2	Identifikation von gespoofen E-Mails.....	219
19.6.3	Verstärkte Identitätsprüfung.....	219
19.6.4	Technische Lösungen für Schadsoftwareprüfung	219
19.6.5	Phishing-Alert-Button	220
19.7	Technische Abwehrtaktiken gegen Smishing.....	220
19.7.1	Containerisierung durch Mobile Device Management (MDM)	220
19.7.2	Zugriffskontrollen und Berechtigungen.....	221
19.7.3	Virtuelle Umgebung für Apps	221
19.7.4	Verschlüsselung auf Containerebene	221
19.7.5	Mobile App Reputation Services	221
20	Organisatorisches Basisverteidigungskonzept.....	223
	Literatur.....	229
21	Organisatorische Abwehrtechniken	231
21.1	Organisatorische Abwehrtaktiken gegen BEC und Phishingarten.....	231
21.1.1	Konzeption und Integration eines Verifizierungsprozesses (Vishing)	232
21.2	Organisatorische Abwehrtaktiken gegen Shoulder Surfing	233
21.2.1	Telearbeitrichtlinien	233
21.2.2	Sichtschutzfilter für Bildschirme	234
21.2.3	Schulungen und Training	234
21.2.4	Regelungen zum Umgang mit IT-Assets	234
21.2.5	Clear-Screen-Richtlinien	234
21.3	Organisatorische Abwehrtaktiken gegen Dumpster Diving.....	235
21.3.1	Richtlinie zur sicheren Entsorgung von Wechseldatenträgern	235
21.3.2	Schulungen und Training	235
21.3.3	Nutzung von Aktenvernichtern	236
21.3.4	Zutrittskontrolle zu Müllbereichen	237
21.3.5	Einsatz von Sicherheitsbehältern	237
21.3.6	Kennzeichnung und Klassifizierung.....	238
21.3.7	Vertragspartnermanagement und Lieferantensicherheit	238

21.4	Organisatorische Abwehrtaktiken gegen Tailgating.	239
21.4.1	Einsatz von Sicherheitspersonal.	239
21.4.2	Sensibilisierung, Schulung und Training der Mitarbeiter	240
	Literatur.	240
22	Human-based Basisverteidigungskonzept	241
22.1	Sicherheits- und Fehlerkultur.	241
22.2	Sicherheitstraining und -übung	242
22.3	Mensch als Stütze der Informationssicherheit	244
	Literatur.	246
23	Human-based Abwehrtaktiken	249
23.1	Anti-Social-Engineering-Mindset	249
23.1.1	Mindset-Typen	250
23.1.2	Persönlichkeitsmerkmale	251
23.1.3	Emotionale Reiz-Reaktions-Kette in der Praxis.	253
23.1.4	Strategie 1: Kennen und Reagieren auf Stressoren	256
23.1.5	Strategie 2: Achtsamkeit durch Innehalten.	258
23.1.6	Strategie 3: Reflexion	261
23.1.7	Strategie 4: Soziale Auslöser identifizieren	264
23.1.8	Strategie 5: Trainiere „Neinsagen“	266
23.1.9	Strategie 6: Kontinuität durch Training	267
23.1.10	Strategie 7: Reziprozität verstehen.	268
23.1.11	Strategie 8: Haloeffekt vermeiden	268
23.2	Human-based Abwehrtaktiken gegen BEC und Phishingarten ...	270
23.3	Human-based Abwehrtaktiken gegen Shoulder Surfing	274
23.4	Human-based Abwehrtaktiken gegen Tailgating	277
	Literatur.	280
 Teil IV Red Chapter: Design an Attack		
24	Szenariobasiertes Red Teaming	285
24.1	Testszenario	286
24.2	Probelauf	292
24.3	Design an Attack	302
 Teil V Green Chapter: Die Kunst der holistischen Verteidigung		
25	Die Hölle, das Sind die anderen	311
26	CISOs und ISBs müssen Kommunikation können	313
	Literatur.	315
27	Erfolgsschlüssel 1: „Sicherheitskultur“	317

28	Erfolgsschlüssel 2: Holistik	319
29	A Day in the Life of a Hacker	321
30	Fazit des Buches	323
	Stichwortverzeichnis	325