

Inhaltsverzeichnis

Vorwort	5
Autorenverzeichnis	11
Abbildungsverzeichnis	13
Abkürzungsverzeichnis	15
1 Eine etwas andere Einleitung (<i>Dirk Drechsler</i>)	19
1.1 Schokolade und Manipulation	19
1.2 Kritischer Buchhalter	19
1.3 Neue Realitäten, bekannte Techniken und frische Kombinationen	20
1.4 Literaturverzeichnis	23
2 Digitalwirtschaftliche Ökosysteme – das neue Organisa- tionsparadigma (<i>Dirk Drechsler</i>)	25
2.1 Einleitung	25
2.2 Wirtschaftliche Ökosysteme (Business Ecosystems)	26
2.2.1 Anfänge	26
2.2.2 Weiterentwicklung	26
2.2.3 Netzwerkgedanke	29
2.2.4 Schlüsselunternehmen als Kern des Ganzen	30
2.3 Digitalwirtschaftliche Ökosysteme (Digital Business Ecosystems)	31
2.3.1 Ideen haben einen langen Vorlauf	31
2.3.2 Silicon Valley Sichtweise	32
2.3.3 Organisation der Dinge	35
2.3.4 Vormals Figurationszusammenhänge, heute Hyperkonnektivität	36
2.4 Digitale Plattformen	38
2.4.1 Geschäftsmodell und Binnenkontext	38
2.4.2 Einheitliche Begriffe?	40
2.4.3 Vergrößerung der Oberfläche – verstehen das alle?	42
2.5 Cyber-physische Systeme	42
2.5.1 Business rules, but technology moves	42
2.5.2 IIoT-Plattformen	43
2.5.3 Viel Technologie, aber auch viele Menschen	45
2.6 Zusammenfassung und Fazit	47
2.6.1 Herausforderungen für das Management, Risiken für die Anderen	47
2.6.2 Innovationen, Innovationen ... aber bitte mit Sicherheit	48
2.6.3 So geht es weiter	49
2.7 Literaturverzeichnis	49

3 Risiken digitalwirtschaftlicher Ökosysteme	
(<i>Dirk Drechsler</i>)	55
3.1 Risikolandschaft	55
3.1.1 Risikobericht des World Economic Forums 2019	56
3.1.2 „Tech Trends Report 2019“ des Future Today Institute	58
3.2 Vertiefung der globalen Sichtweise	60
3.2.1 Bericht der ENISA 2018	60
3.2.2 ISACA-Studie „State of Cybersecurity 2018“	65
3.3 Systemischer Charakter der digitalwirtschaftlichen Risiken	65
3.3.1 Interdependente Cyber-Herausforderungen	65
3.3.2 Generische Betrachtung von (Inter-)Dependenz	66
3.4 Herausforderungen der smarten Geschäftswelt	69
3.4.1 Auswahl von Risiko- und Sicherheitsmodellen	69
3.4.2 Einbettung für eine durchgängige Systematik	72
3.4.3 Intensivierung der Portfolio-Sicht ist notwendig	73
3.4.4 Einbettung einer zweiten Systematik	76
3.5 Menschliche Schwachstelle im Angriffsszenario	78
3.5.1 Angriffsziele im digitalwirtschaftlichen Ökosystem	78
3.5.2 Informationen, Informationen, Informationen!	79
3.5.3 Rolle und Zielprofil	80
3.5.4 Aufeinandertreffen in der Situation	80
3.5.5 Konkrete Situation	81
3.6 Zusammenfassung und Fazit	82
3.6.1 Big Picture und Top-Down Ansatz	82
3.6.2 Details zur Ergänzung	82
3.6.3 Effekte aus der Hyperkonnektivität	82
3.6.4 Antworten der smarten Geschäftswelt	83
3.6.5 Menschen im Gesamtgefüge	83
3.6.6 Fazit und Ausblick	83
3.7 Literaturverzeichnis	83
4 Social Engineering aus Sicht der Polizei (<i>Otmar Hertwig, Dirk Drechsler</i>)	89
4.1 Einleitung	89
4.2 Polizei im Wandel	91
4.3 Personelle Umsetzung in Baden-Württemberg	91
4.4 Polizeiliche Kriminalstatistik	92
4.4.1 Allgemeine Erfassungsmodalitäten der Polizeilichen Kriminalstatistik	92
4.4.2 Besonderheiten bei der Erfassung von Delikten aus dem Bereich der Cyber-Kriminalität	93
4.4.3 Versuch einer cyber-kriminologischen Einordnung	93
4.5 Fallstudien mit dem Modus Operandi Social Engineering	97
4.5.1 Fallstudie 1: Ransomware-Angriff	97
4.5.2 Fallstudie 2: Falscher Microsoft-Mitarbeiter	99
4.5.3 Fallstudie 3: Warenbetrug	101

4.5.4	Fallstudie 4: Romance Scamming oder moderne Form des Heiratsschwindels	103
4.5.5	Fallstudie 5: Warenagentin als leichtfertige Geldwäscherin	106
4.5.6	Fallstudie 6: Ausspähen von Daten mittels „Keylogger“	107
4.5.7	Fallstudie 7: Erpressung auf sexueller Grundlage	108
4.5.8	Fallstudie 8: Falscher BKA-Beamter	109
4.5.9	Fallstudie 9: Strafunmündiges Kind als Hacker und Erpresser	110
4.5.10	Fallstudie 10: Missbrauch von Firmendaten bei Fakeshops	112
4.5.11	Fallstudie 11: CEO Fraud	113
4.6	Fazit	115
4.7	Literaturverzeichnis	116
5	Manipulationstechniken (<i>Dirk Haag, Anselm Rohrer</i>)	119
5.1	Definition eines Social Engineers	119
5.2	Bewusste und unbewusste Manipulation	121
5.3	Motivation eines Social Engineers	122
5.3.1	Initiierung durch den Angreifer	122
5.3.2	Initiierung durch den Angegriffenen	123
5.4	Soziale Aspekte und psychologische Einflussfaktoren	124
5.4.1	Nonverbale Kommunikation	125
5.4.2	Rapport	131
5.4.3	Pretexting vs. Impersonation	132
5.4.4	Elizitieren	133
5.4.5	Vertrauenswürdigkeit	135
5.4.6	Autorität	135
5.4.7	Hilfsbereitschaft	137
5.4.8	Mangelndes Gefahrenbewusstsein	137
5.4.9	Framing	138
5.4.10	Aspekte der Beeinflussung	139
5.4.11	Zuschauereffekt	143
5.5	Geschlechterrolle	144
5.6	Zusammenfassung und Fazit	147
5.7	Literaturverzeichnis	148
6	Technische Seite des Social Engineerings (<i>Dirk Haag, Anselm Rohrer</i>)	151
6.1	Kategorisierung von Social-Engineering-Angriffen	151
6.1.1	Human Based Social Engineering	151
6.1.2	Computer Based Social Engineering	151
6.1.3	Reverse Social Engineering	152
6.2	Technische Hilfsmittel	152
6.3	Verkleidungen	152
6.4	Öffnungswerkzeuge	153

6.5	Spionagewerkzeuge	153
6.6	Data-Mining-Tools	154
6.7	Social-Engineering-Toolkit	155
6.8	Strukturierung eines Angriffs	155
6.8.1	Planung	156
6.8.2	Aufklärung und Informationsbeschaffung	158
6.8.3	Entwicklung eines Szenarios	161
6.8.4	Durchführung	164
6.8.5	Berichterstattung	164
6.9	Auswirkungen eines Angriffs	165
6.9.1	Materielle Auswirkungen	166
6.9.2	Immaterielle Auswirkungen	167
6.9.3	Personelle Auswirkungen	168
6.10	Literaturverzeichnis	169
7	Social Engineering Kill Chain (<i>Dirk Drechsler, Marco Dennis Schmid</i>)	171
7.1	Einleitung	171
7.2	Entwicklung langfristiger Resilienz	172
7.2.1	Rückgriff auf das neue Organisationsparadigma	172
7.2.2	Zeitliche Verteilung von Resilienz	173
7.2.3	Threat Intelligence mit Strategic Foresight Management	174
7.3	Social Engineering Kill Chain	181
7.3.1	Einleitung	181
7.3.2	Aufbau der Social Engineering Kill Chain	182
7.3.3	Phase 1: Planung und Zielbestimmung	183
7.3.4	Phase 2: Aufklärung und Informationsbeschaffung	188
7.3.5	Phase 3: Entwicklung des Szenarios	200
7.3.6	Phase 4: Durchführung	202
7.4	Fazit	203
7.5	Literaturverzeichnis	205
8	Zusammenfassung und Fazit (<i>Dirk Drechsler</i>)	211
8.1	Zusammenfassung	211
8.2	Fazit	212
8.3	Literaturverzeichnis	217