

ESV ERICH
SCHMIDT
VERLAG

Schutz vor Social Engineering

Angriffspunkte und Abwehrmöglichkeiten
in digitalwirtschaftlichen Ökosystemen

Herausgegeben von

Prof. Dr. Dirk Drechsler

Mit Beiträgen von

Prof. Dr. Dirk Drechsler

Dirk Haag

Otmar Hertwig

Anselm Rohrer

Marco Dennis Schmid

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

<http://ESV.info/978-3-503-18859-8>

ISBN 978-3-503-18859-8 (gedrucktes Werk)

ISBN 978-3-503-18860-4 (eBook)

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2019

www.ESV.info

Druck: Hubert & Co., Göttingen

Vorwort

Social Engineering stellt aus Sicht der Unternehmen und auch anderer, nicht-wirtschaftlicher Organisationen ein Problem dar, obwohl dessen Angriffsmuster aufgrund gängiger Publikationen durchaus bekannt sind. Jedoch beobachtet der Verfasser seit einigen Jahren, dass die verzeichneten Angriffe weder wirklich zurückgehen noch an Wirksamkeit verlieren. Das ist bedenklich, da die aktuellen Entwicklungen auf dem Gebiet der Digitalisierung sowohl eine höhere Komplexität und Dynamik für die Geschäftstätigkeit mit sich bringen als auch die Angriffsflächen sich durch das dominante Organisationsparadigma der digitalwirtschaftlichen Ökosysteme erheblich vergrößern.

Aus diesem Grund und nach einer etwas längeren Zeit des Nachdenkens hat sich der Herausgeber dieses Sammelbands dazu entschlossen, das Thema zusammen mit verschiedenen Autoren aus diversen Blickwinkeln erneut zu beleuchten. Das Buch ist dabei modular aufgebaut, so dass jedes Kapitel unabhängig von den anderen gelesen werden kann. Es ist auch nicht als Lehrbuch gedacht, da alle Autoren der einzelnen Kapitel jeweils individuell ihre eigenen Ansichten zu dem Thema ausdrücken.¹ Mögliche Widersprüche oder Redundanzen sind der jeweiligen Struktur des Beitrags geschuldet und auch so gewollt.

Der Herausgeber möchte noch einigen Personen danken, die am Herstellungsprozess des Buchs beteiligt waren:

- **Philip Schelske** und **Ulrike Weiss** vom Erich Schmidt Verlag haben den Herausgeber jederzeit konstruktiv bezüglich der Umsetzung begleitet und standen für sämtliche Fragen Rede und Antwort. Das Vertrauen, das der *ESV* dem Herausgeber entgegengebracht hat, bedeutet eine besondere Herausforderung. Eine Publikation in einem führenden Verlag auf dem Gebiet des Risikomanagements ist eine Chance, sich als Autorengruppe darstellen zu können.
- Die **Autoren** haben sich als Team und Personen als angenehme und verlässliche Partner gezeigt. Der Herausgeber hofft, dass die Leser auch inhaltlich zu einem positiven Resultat kommen.
- Sämtliche Korrekturarbeiten wurden von **Elaine Kohler** (B.A. Medienwirtschaft und cand. M.Sc. Medien und Kommunikation) und Dipl.-Pädagogin **Simone Drechsler** durchgeführt. Beiden gilt ein tiefempfundener Dank für die akribische Durchsicht sämtlicher Beiträge. Die verbleibenden Fehler gehen natürlich zu Lasten des Herausgebers.

1 Sämtliche Beiträge sind nicht Gender-neutral geschrieben. Alle männlichen Bezeichnungen umfassen bei fehlender Konkretisierung auch weibliche Personen. Das geschieht rein aus Gründen der Lesbarkeit und der Herausgeber entschuldigt sich vorab, sofern diese Vorgehensweise nicht im Sinne aller ist.

Vorwort

Das Social Engineering ist und bleibt eine erhebliche Bedrohung. Der Herausgeber hofft, mit dem Sammelband einen Beitrag zu einer neuen Perspektive und verstärkten Wahrnehmung geliefert zu haben.

Offenburg, im Juli 2019

Prof. Dr. rer. soc. HSG Dirk Drechsler
(CIA CCSA CRMA CFE)

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

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 (Dirk Haag, Anselm Rohrer)	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 (Dirk Haag, Anselm Rohrer)	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