

Inhaltsverzeichnis

<i>Vorwort zur 3. Auflage</i>	V
<i>Vorwort zur 1. Auflage</i>	VII
<i>Literaturverzeichnis</i>	XV
<i>Abbildungsverzeichnis</i>	XXIII
I. Einleitung	1
1. Definition Internetkriminalität	3
2. Computerkriminalität in der PKS	6
II. Identitätsdiebstahl	8
1. Phänomenbeschreibung	8
2. Strafrechtliche Relevanz	14
3. Zivilrechtliche Relevanz	16
4. Checkliste für die Ermittlungspraxis	16
5. Präventionsmaßnahmen	17
III. Social Engineering, Social Hacking	19
1. Phänomenbeschreibung	19
2. Strafrechtliche Relevanz	23
3. Zivilrechtliche Relevanz	25
4. Checkliste für die Ermittlungspraxis	26
5. Präventionsmaßnahmen	27
IV. Phishing	30
1. Phänomenbeschreibung	30
1.1 Wie läuft ein Phishing-Angriff ab?	30
1.2 Beispiel für den Inhalt einer Phishingmail	31
1.3 Phishing unter Ausnutzung mobiler Endgeräte	34
1.4 Mishing – Phishing über mobile Kommunikations- geräte	35
1.4.1 Smishing – Phishing über Kurznachrichten	36
1.4.2 Quishing – Phishing mittels QR-Codes	37
2. Strafrechtliche Relevanz	38
3. Zivilrechtliche Relevanz	40

4.	Ermittlungsmöglichkeiten	40
4.1	E-Mail	40
4.2	Phishingseite (www.)	44
5.	Checkliste für die Ermittlungspraxis	48
6.	Präventionsmaßnahmen	49
V.	Internetbanking, Onlinebanking	52
1.	Phänomenbeschreibung	52
2.	Verwendete Techniken im Onlinebanking	52
2.1	Banksoftware	53
2.2	Browserunterstützte Techniken	53
3.	Authentifizierung	54
3.1	Nachweis der Kenntnis einer Information (Wissen)	54
3.2	Verwendung eines Besitzums (Besitz)	55
3.3	Gegenwart des Benutzers selbst (Inhärenz)	57
3.4	Zwei-Faktoren-Authentifizierung	58
4.	Die wichtigsten Onlinebanking-Verfahren im Überblick	59
4.1	FinTS/HBCI	59
4.2	HBCI+	61
4.3	TAN, iTAN, iTANplus	61
4.4	mTAN – mobile TAN	61
4.5	Portierung der Mobilfunkrufnummer/Neue SIM-Karte/ SIM-Swapping-Angriff	64
4.6	Handy-Apps/Push-TANs	66
4.7	sm@rt-TAN, chip-TAN, optic-TAN	67
4.8	photoTAN	68
4.9	qrTAN (Quick-Response-Code-TAN)	70
4.10	NFC-TAN	71
5.	Weitere Manipulationsmöglichkeiten	71
5.1	Man-in-the-middle-Attacke, Man-in-the-browser- Attacke	71
5.2	ARP-Spoofing	73
5.3	DNS-Spoofing, Pharming	73
6.	Strafrechtliche Relevanz	74
7.	Zivilrechtliche Relevanz	77
8.	Checkliste für die Ermittlungspraxis	77
9.	Präventionsmaßnahmen	78

VI. Ransomware (Online-Erpressungen)	84
1. Phänomenbeschreibung	84
2. Wege der Infizierung und Kompromittierung von Netzwerken	86
2.1 Initialzugang über kompromittierte Zugangsdaten	86
2.2 Phishing und Social Engineering	86
2.3 Ausnutzung von Sicherheitslücken	86
2.4 Laterale Bewegung und Vorbereitung	86
2.5 Gezielte Verschlüsselung	87
2.5.1 Aktuelle Verschlüsselungsprogramme	87
2.6 Sexpression als Sonderform digitaler Erpressung	89
3. Strafrechtliche Relevanz	92
4. Zivilrechtliche Relevanz	94
5. Checkliste für die Ermittlungspraxis	94
6. Präventionsmaßnahmen	96
VII. Telefonanlagen- und Router-Hacking	99
1. Phänomenbeschreibung	99
2. Möglichkeiten der Bereicherung	101
2.1 Kostenersparnis	101
2.2 Mehrwertdienste und „International Revenue Share Fraud“	101
2.3 Bereicherung durch Transit- und Terminierungs-entgelte	102
3. Strafrechtliche Relevanz	104
4. Zivilrechtliche Relevanz	104
5. Checkliste für die Ermittlungspraxis	105
6. Präventionsmaßnahmen	105
VIII. Finanzagent, Warenagent	107
1. Phänomenbeschreibung	107
2. Strafrechtliche Relevanz	111
3. Zivilrechtliche Relevanz	112
4. Checkliste für die Ermittlungspraxis	113
5. Präventionsmaßnahmen	113
IX. Onlineshopping/Fakeshop	115
1. Phänomenbeschreibung	115
2. Strafrechtliche Relevanz	117

3.	Zivilrechtliche Relevanz	117
4.	Wie können Fakeshops erkannt werden?	119
5.	Checkliste für die Ermittlungspraxis	124
6.	Präventionsmaßnahmen	124
X.	Cybertrading	125
1.	Phänomenbeschreibung	125
2.	Strafrechtliche Relevanz	129
3.	Zivilrechtliche Relevanz	130
4.	Checkliste für die Ermittlungspraxis	131
5.	Präventionsmaßnahmen	132
XI.	Urheberrecht	133
1.	Phänomenbeschreibung	133
1.1	Kopieren von Texten, Bildern, Musik-, Filmdateien oder Computerprogrammen	134
1.2	Tauschbörsen für Musikstücke, Filme oder Computer- dateien, filesharing	135
1.3	Streaming	137
1.4	KI-generierte Inhalte	138
1.5	Memes, Social-Media-Sharing	138
1.6	Uploadfilter, Plattformhaftung und EU-Urheberrechts- richtlinie 2019	139
2.	Strafrechtliche Relevanz	139
3.	Zivilrechtliche Relevanz	141
4.	Checkliste für die Ermittlungspraxis	143
5.	Präventionsmaßnahmen	145
XII.	Kinderpornographie	146
1.	Phänomenbeschreibung	146
2.	Strafrechtliche Relevanz	152
3.	Zivilrechtliche Relevanz	158
4.	Checkliste für die Ermittlungspraxis	159
5.	Präventionsmaßnahmen	161
XIII.	Cybermobbing, Cyber-Bullying	163
1.	Phänomenbeschreibung	163
2.	Strafrechtliche Relevanz	171
3.	Zivilrechtliche Relevanz	172

4.	Checkliste für die Ermittlungspraxis	175
5.	Präventionsmaßnahmen	179
XIV.	Passwortsicherheit	182
1.	Beschreibung	182
2.	Hintergrundwissen	186
3.	MD5-Hash	188
4.	Salt	191
XV.	Computerforensik	192
1.	Die Rolle der Forensik	192
2.	Postmortale vs. Live-Forensik	193
3.	Sicherstellung	196
4.	Mobile Forensik	197
XVI.	Organisationen und Gremien der IT-Sicherheit	199
1.	Europäische Union	199
1.1	Agentur der Europäischen Union für Cybersicherheit – ENISA	199
1.2	Task Force Computer Security Incident Response Teams – TF-CSIRT	199
1.3	Trusted Introducer für CERTs in Europa – TI	200
2.	Deutschland – Bund und Länder	200
2.1	Bundesamt für Sicherheit in der Informationstechnik – BSI	200
2.2	Bundesamt für Verfassungsschutz – BfV – und Landes- ämter für Verfassungsschutz – LfV	200
2.3	Bundesbeauftragter für den Datenschutz und die Infor- mationsfreiheit – BfDI	201
2.4	Landeskriminalämter – LKÄ	201
2.5	Bundesministerium der Justiz und für Verbraucherschutz – BMJV	202
2.6	Bundesnachrichtendienst – BND	202
2.7	Bürger-CERT	202
2.8	Nationales Cyber-Abwehrzentrum – NCAZ (ugs. Cyber-Abwehrzentrum)	202
2.9	Nationaler Cyber-Sicherheitsrat – NCS	203
2.10	Datenzentralen der Länder	203
2.11	Gemeinsames Internetzentrum – GIZ	203

2.12	IT-Sicherheit in der Wirtschaft	203
2.13	Netzwerk Elektronischer Geschäftsverkehr – NEG	204
2.14	Zentrale Stelle für Informationstechnik im Sicherheits- bereich – ZITiS	204
3.	Organisationen der Wirtschaft	205
3.1	Allianz für Sicherheit in der Wirtschaft e. V.	205
3.2	Deutschland sicher im Netz e.V. – DsiN e.V.	205
3.3	Nationale Initiative für Information- und Internet-Sicher- heit e.V. – NIFIS e.V.	205
3.4	Verband der deutschen Internetwirtschaft e.V. – eco e.V.	205
	<i>Sachverzeichnis</i>	207