Inhaltsverzeichnis

Vorwort V
Vorwort zur 1. Auflage VII
Literaturverzeichnis XV
Abbildungsverzeichnis XIX

I. Einleitung 1
1. Definition Internetkriminalität 3
2. Computerkriminalität in der PKS 6

II. Identitätsdiebstahl 8
1. Phänomenbeschreibung 8
2. Strafrechtliche Relevanz 12
3. Zivilrechtliche Relevanz 13
4. Checkliste für die Ermittlungspraxis 14
5. Präventionsmaßnahmen 14

III. Social Engineering, Social Hacking 17
1. Phänomenbeschreibung 17
2. Strafrechtliche Relevanz 20
3. Zivilrechtliche Relevanz 22
4. Checkliste für die Ermittlungspraxis 23
5. Präventionsmaßnahmen 23

IV. Phishing 26
1. Phänomenbeschreibung 26
1.1 Wie läuft ein Phishing-Angriff ab? 26
1.2 Beispiel für den Inhalt einer Phishingmail 27
2. Strafrechtliche Relevanz 30
3. Zivilrechtliche Relevanz 31
4. Ermittlungsmöglichkeiten 32

4.1 E-Mail ... 32
4.2 Phishingseite (www.) ... 36
5. Checkliste für die Ermittlungspraxis ... 40
6. Präventionsmaßnahmen ... 40

V. Internetbanking, Onlinebanking ... 43
1. Phänomenbeschreibung ... 43
2. Verwendete Techniken im Onlinebanking ... 43
2.1 Banksoftware ... 44
2.2 Browserunterstützte Techniken ... 44
3. Authentifizierung ... 45
3.1 Nachweis der Kenntnis einer Information (Wissen) ... 45
3.2 Verwendung eines Besitztums (Besitz) ... 46
3.3 Gegenwart des Benutzers selbst (Inhärenz) ... 48
3.4 Zwei-Faktoren-Authentifizierung ... 49
4. Die wichtigsten Onlinebanking-Verfahren im Überblick ... 50
4.1 FinTS/HBCI ... 50
4.2 HBCI+ ... 52
4.3 TAN, iTAN, iTANplus ... 52
4.4 mTAN – mobile TAN ... 52
4.5 Portierung der Mobilfunkrufnummer/Neue SIM-Karte/SIM-Swapping-Angriff ... 55
4.6 Handy-Apps/Push-TANs ... 57
4.7 sm@rt-TAN, chip-TAN, optic-TAN ... 58
4.8 photoTAN ... 59
4.9 qrTAN (Quick-Response-Code-TAN) ... 60
4.10 NFC-TAN ... 61
5. Weitere Manipulationsmöglichkeiten ... 62
5.1 Man-in-the-middle-Attacke, Man-in-the-browser-Attacke ... 62
5.2 ARP-Spoofing ... 63
5.3 DNS-Spoofing, Pharming ... 63
6. Strafrechtliche Relevanz ... 64
7. Zivilrechtliche Relevanz ... 67

8. Checkliste für die Ermittlungspraxis 68
9. Präventionsmaßnahmen 68

VI. Skimming 72
1. Phänomenbeschreibung 72
2. Straftaten, die ebenfalls in Zusammenhang mit einem Geldautomaten stehen 75
2.1 Jackpotting 75
2.2 Cash Trapping 76
2.3 Loop-Trick 76
3. Strafrechtliche Relevanz 76
4. Zivilrechtliche Relevanz 82
5. Checkliste für die Ermittlungspraxis 83
6. Präventionsmaßnahmen 84

VII. Ransomware (Online-Erpressungen) 87
1. Phänomenbeschreibung 87
2. Die Infizierung und Möglichkeiten zur Hilfe 88
2.1 Drive-by-Download 88
2.2 .zip-Trojaner 89
2.3 Weitere Hilfen bei einem Befall 92
2.4 Die aktuellen Verschlüsselungsprogramme 93
2.5 „Sonderfall" Sexpressung 94
3. Strafrechtliche Relevanz 96
4. Zivilrechtliche Relevanz 97
5. Checkliste für die Ermittlungspraxis 98
6. Präventionsmaßnahmen 99

VIII. Telefonanlagen- und Router-Hacking 103
1. Phänomenbeschreibung 103
2. Möglichkeiten der Bereicherung 104
2.1 Kostenersparnis 104
2.2 Mehrwertdienste 105
2.3 Bereicherung durch Transit- und Terminierungsentgelte 105

2.3.1 Der betrügerische Provider kassiert doppelt 106
2.3.2 Cold Stop 106
3. Strafrechtliche Relevanz 107
4. Zivilrechtliche Relevanz 107
5. Checkliste für die Ermittlungspraxis 108
6. Präventionsmaßnahmen 108

IX. Finanzagent, Warenagent 110
1. Phänomenbeschreibung 110
2. Strafrechtliche Relevanz 112
3. Zivilrechtliche Relevanz 114
4. Checkliste für die Ermittlungspraxis 114
5. Präventionsmaßnahmen 115

X. Urheberrecht 116
1. Phänomenbeschreibung 116
1.1 Kopieren von Texten, Bildern, Musik-, Filmdateien oder Computerprogrammen 117
1.2 Tauschbörsen für Musikstücke, Filme oder Computerdateien, filesharing 118
1.3 Streaming 119
2. Strafrechtliche Relevanz 121
3. Zivilrechtliche Relevanz 122
4. Checkliste für die Ermittlungspraxis 124
5. Präventionsmaßnahmen 126

XI. Kinderpornographie 127
1. Phänomenbeschreibung 127
2. Strafrechtliche Relevanz 131
3. Zivilrechtliche Relevanz 134
4. Checkliste für die Ermittlungspraxis 136
5. Präventionsmaßnahmen 137

XII. Cybermobbing, Cyber-Bullying 139
1. Phänomenbeschreibung 139
2. Strafrechtliche Relevanz 146
3. Zivilrechtliche Relevanz 147
4. Checkliste für die Ermittlungspraxis 148
5. Präventionsmaßnahmen 150

XIII. Passwortsicherheit 154
1. Beschreibung 154
2. Hintergrundwissen 157
3. MD5-Hash 159
4. Salt 162

XIV. Computerforensik 163
1. Die Rolle der Forensik 163
2. Postmortale vs. Live-Forensik 163
3. Sicherstellung 167
4. Mobile Forensik 168

XV. Organisationen und Gremien der IT-Sicherheit 170
1. Europäische Union 170
1.1 Agentur der Europäischen Union für Cybersicherheit – ENISA 170
1.2 Task Force Computer Security Incident Response Teams – TF-CSIRT 170
1.3 Trusted Introducer für CERTs in Europa – TI 171
2. Deutschland – Bund und Länder 171
2.1 Bundesamt für Sicherheit in der Informationstechnik – BSI 171
2.2 Bundesamt für Verfassungsschutz – BfV – und Landesämter für Verfassungsschutz – LfV 171
2.3 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit – BfDI 172
2.4 Landeskriminalämter – LKÄ 172

2.5 Bundesministerium für Justiz und Verbraucherschutz – BMJV ... 173
2.6 Bundesnachrichtendienst – BND ... 173
2.7 Bürger-CERT ... 173
2.8 Cyber-Abwehrzentrum (früher Nationales Cyber-Abwehrzentrum – NCAZ) ... 173
2.9 Nationaler Cyber-Sicherheitsrat – NCS ... 174
2.10 Datenzentralen der Länder ... 174
2.11 Gemeinsames Internetzentrum – GIZ ... 174
2.12 IT-Sicherheit in der Wirtschaft ... 174
2.13 Netzwerk Elektronischer Geschäftsverkehr – NEG ... 175
2.14 Zentrale Stelle für Informationstechnik im Sicherheitsbereich – ZITiS ... 175
3. Organisationen der Wirtschaft ... 175
3.1 Allianz für Sicherheit in der Wirtschaft e. V. ... 175
3.2 Deutschland sicher im Netz e.V. – DsiN e.V. ... 176
3.3 Nationale Initiative für Information- und Internet-Sicherheit e.V. – NIFIS e.V. ... 176
3.4 Verband der deutschen Internetwirtschaft e.V. – eco e.V. ... 176

Sachverzeichnis ... 177