Inhaltsverzeichnis

Vorwort V
Literaturverzeichnis XIII
Onlinemedien XIV
Abbildungsverzeichnis XVII

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 13
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 22
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 32
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 43
   2.2 Browserunterstützte Techniken 44
3. Authentifizierung 45
   3.1 Nachweis der Kenntnis einer Information 45
   3.2 Verwendung eines Besitztums 45
   3.3 Gegenwart des Benutzers selbst 48
   3.4 Zwei-Faktoren-Authentifizierung 49
4. Die wichtigsten Onlinebanking-Verfahren im Überblick 49
   4.1 HBCI/FinTS 49
   4.2 HBCI+ 51
   4.3 TAN 52
   4.4 iTAN – indizierte TAN 52
   4.5 iTANplus 53
   4.6 mTAN – mobile Tan 53
   4.7 Portierung der Mobilfunkrufnummer/ Neue SIM-Karte 57
   4.8 sm@rt-TAN, chip-TAN, optic-TAN 58
   4.9 photoTAN 59
   4.10 qrTAN (Quick-Response-Code-TAN) 60
   4.11 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 67
8. Präventionsmaßnahmen 68

VI. Skimming 71

1. Phänomenbeschreibung 71
2. Straftaten, die ebenfalls in Zusammenhang mit einem Geldautomaten stehen 74
   2.1 Cash Trapping 74
   2.2 Loop-Trick 74

3. Strafrechtliche Relevanz 75
4. Zivilrechtliche Relevanz 80
5. Checkliste für die Ermittlungspraxis 81
6. Präventionsmaßnahmen 82

VII. Ransomware (Online-Erpressungen) 84

1. Phänomenbeschreibung 84
2. Die Infizierung erfolgt derzeit über zwei verschiedene Wege 85
   2.1 Drive-by-Download 85
   2.2 .zip-Trojaner 86
3. Strafrechtliche Relevanz 89
4. Zivilrechtliche Relevanz 91
5. Checkliste für die Ermittlungspraxis 91
6. Präventionsmaßnahmen 92

VIII. Telefonanlagen- und Router-Hacking 95

1. Phänomenbeschreibung 95
2. Möglichkeiten der Bereicherung 96
   2.1 Kostenersparnis 96
   2.2 Mehrwertdienste 97
   2.3 Bereicherung durch Transit- und Terminierungsentgelte 97
      2.3.1 Der betrügerische Provider kassiert doppelt 98
      2.3.2 Cold Stop 98
3. Strafrechtliche Relevanz 99
4. Zivilrechtliche Relevanz 100
5. Checkliste für die Ermittlungspraxis 100
6. Präventionsmaßnahmen 100

IX. Finanzagent, Warenagent 102

1. Phänomenbeschreibung 102
2. Strafrechtliche Relevanz 103
3. Zivilrechtliche Relevanz 105
4. Checkliste für die Ermittlungspraxis 105
5. Präventionsmaßnahmen 106

X. Urheberrecht 107

1. Phänomenbeschreibung 107

1.1 Kopieren von Texten, Bildern, Musik-, Filmdateien oder Computerprogrammen 108
1.2 Tauschbörsen für Musikstücke, Filme oder Computerdateien, filesharing 109
1.3 Streaming 110
2. Strafrechtliche Relevanz 112
3. Zivilrechtliche Relevanz 113
4. Checkliste für die Ermittlungspraxis 115
5. Präventionsmaßnahmen 117

XI. Kinderpornographie 118

1. Phänomenbeschreibung 118
2. Strafrechtliche Relevanz 121
3. Zivilrechtliche Relevanz 124
4. Checkliste für die Ermittlungspraxis 125
5. Präventionsmaßnahmen 126

XII. Cybermobbing, Cyber-Bullying 128

1. Phänomenbeschreibung 128
2. Strafrechtliche Relevanz 134
3. Zivilrechtliche Relevanz 135
4. Checkliste für die Ermittlungspraxis 136
5. Präventionsmaßnahmen 138

XIII. Passwortsicherheit 141

1. Beschreibung 141
2. Hintergrundwissen 142
3. MD5-Hash 145
4. Salt 147

XIV. Computerforensik 148

1. Die Rolle der Forensik 148
2. Postmortale vs. Live-Forensik 149
3. Sicherstellung 152

XV. Organisationen und Gremien der IT-Sicherheit 154

1. Europäische Union 154
1.1 Agentur für Netz- und Informationssicherheit – ENISA 154

1.2 Task Force Computer Security Incident Response Teams – TF-CSIRT 154
1.3 Trusted Introducer für CERTs in Europa – TI . . 154
2. Deutschland – Bund und Länder 155
2.1 Bundesamt für Sicherheit in der Informationstechnik – BSI 155
2.2 Bundesamt für Verfassungsschutz – BfV und Landesämter für Verfassungsschutz – LfV 155
2.3 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit – BfDI 156
2.4 Landeskriminalämter – LKÄ 156
2.5 Zentralstelle für anlassunabhängige Recherchen in Datennetzen – ZaRD 156
2.6 Technisches Servicezentrum des Bundeskriminalamtes – TeSIT 157
2.7 Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz – BMELV 157
2.8 Bundesnachrichtendienst – BND 157
2.9 Bürger-CERT 157
2.10 Cyber-Abwehrzentrum (früher Nationales Cyber-Abwehrzentrum – NCAZ) 158
2.11 Nationaler Cyber-Sicherheitsrat – NCS 158
2.12 Datenzentralen der Länder 158
2.13 Gemeinsames Internetzentrum – GIZ 158
2.14 Task Force IT-Sicherheit in der Wirtschaft 159
2.15 Netzwerk Elektronischer Geschäftsverkehr – NEG 159
3. Organisationen der Wirtschaft 159
3.1 Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e. V. – ASW e. V. 159
3.2 Deutschland sicher im Netz e. V. – DsiN e. V. . . . 160
3.3 Nationale Initiative für Information- und Internet-Sicherheit e. V. – NIFIS e. V. 160
3.4 Verband der deutschen Internetwirtschaft e. V. – eco e. V. 160

Stichwortverzeichnis 161