Inhaltsverzeichnis

Geleitwort VII

Vorwort IX

Abkürzungsverzeichnis XIX

Teil 1: Duale Welt 1

A. Jargon und Fachbegriffe 3
B. Zu Teil 1: Duale Welt 5
C. Zu Teil 2: Materielles IuK-Strafrecht 6
I. Quellen des IuK-Strafrechts 7
II. Gesetzlich ausgestaltetes Hacking-Strafrecht 8
III. Betrugsnahes Cybercrime 10
IV. Schweres Cybercrime 11
D. Zu Teil 3: Ermittlungen gegen das Cybercrime 12

Kapitel 1. Cybercrime und IuK-Strafrecht 13

A. Technische Gegenstände des IuK-Strafrechts 14
B. Abgrenzungen zu anderen Begriffssystemen 17
C. Besonderheiten des Cybercrime und des IuK-Strafrechts 18
D. IuK-Strafrecht im engeren Sinne 21
E. Bedeutung des Cybercrime 25
F. BSI, Bedrohungen gegen Anlagensteuerungen 30

Kapitel 2. Geschichte des Cybercrime 33

A. Vor 1900. Technische und wirtschaftliche Anfänge 35
B. Bis 1950. Elektrotechnik und technische Großanlagen 36
C. Bis 1970. Elektronisches Zeitalter 37
D. Bis 1980. Elektronische Gründerzeit 41
E. Bis 1990. Expansion und Missbrauch 42
F. Bis 2000. Internet und Viren 45
I. Adressierung und Internetverwaltung 47
1. Telekommunikation 48
2. Datenkommunikation und Internet 53
3. Domain Name System 56
4. Hierarchische Internetverwaltung 58
II. Informations- und Kommunikationstechnik bis 2000 59
III. Cybercrime und Anfänge der Rechtsprechung zur IuK 60
1. Dialer und Mehrwertdienste 61
2. Grabbing 61
3. Haftung für Links 62
4. Haftung des Providers 64
G. Seit 2000. Kommerzielles Internet und organisiertes Cybercrime 66

Bibliografische Informationen
http://d-nb.info/1066264244

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

I. „Raubkopien“ ... 68
II. Hacking und Malware ... 70
III. Botnetze. Hacktivismus ... 71
H. Cybercrime in der Neuzeit ... 73
I. Klaus Störtebeker ... 74
II. Cardingboards ... 75
III. Botnetze ... 77
IV. Stuxnet ... 80
V. Datenspionage ... 82
1. Operation Shady Rat ... 82
2. Operation Aurora ... 83
3. Night Dragon ... 84
4. Operation High Roller ... 85
5. The Man-in-the-Middle ... 85
VI. Ransomware ... 86
VII. Abofallen ... 87
VIII. Webshops und Betrug ... 89
I. Fazit: Wesentliche Formen des Cybercrime ... 90

Kapitel 3. Formen und Methoden des Cybercrime ... 91

A. Schema eines Hacking-Angriffs ... 94
B. Phishing ... 96
C. Finanzagenten und Beutesicherung ... 98
I. Unfreiwillige und unechte Finanzagenten ... 98
II. Warenagenten, Packstationen und Bezahlsysteme ... 100
D. Skimming ... 101
I. Merkmalstoffe und EMV-Chip ... 104
II. Formenwechsel beim Datenabgriff ... 105
III. Skimming unter Einsatz des Hackings ... 106
E. Malware ... 108
I. Basis-Malware und Infiltration ... 108
1. Präparierte Webseiten ... 112
2. E-Mails und E-Mail-Anhänge ... 114
3. Andere Formen der Anlieferung und Infiltration ... 115
4. Erkundung des Systems und Einnisten der Malware ... 115
II. Produktive Malware ... 116
1. Maliziöse Grundfunktionen ... 117
a) Backdoor ... 117
b) Spyware und Keylogger ... 118
2. Ransomware ... 118
3. Bot Ware ... 119
4. Onlinebanking-Malware ... 119
5. Anlagensteuerungen ... 121
F. Identitätstäuschung und Identitätsdiebstahl ... 122
I. Identitätstäuschung im Rechtssinne ... 124
II. Identitätsmerkmale und Identitätsübernahme ... 126
G. Carding und Kontobetrug ... 127

Kapitel 4. Gefahren und Hackteure in der dualen Welt 131
A. Gefahren, Typen und Hackteure 131
I. Bedrohungsregister vom BSI 132
II. Typen und Strukturen 134
III. Vorsätzlich handelnde Angreifer laut BSI 138
B. Cyber-Aktivisten (Hacktivisten) 139
I. Hacker und Hacktivismus 140
II. Anonymous und Payback 142
III. Die Zukunft des Hacktivismus 146
C. Subkulturen und Sprachen 147

Teil 2: Materielles IuK-Strafrecht 151

Kapitel 5. Hacking 153
A. Gegenstand und Grenzen des Hacking-Strafrechts 154
B. Ausspähen und Abfangen von Daten 162
I. Kennwortschutz gegen das Ausspähen 164
II. Angriff gegen ein Local Area Network – LAN 165
1. Missbrauch indiskreter Kenntnisse 166
2. Wardriving 167
3. Inhaltlicher Schutzbereich von Daten aus dem LAN 170
4. Datenübermittlung im Internet und Webserver 172
C. Datenveränderung und Computersabotage 174
I. Datenveränderung 174
II. Computersabotage 178
1. Datenverarbeitung von wesentlicher Bedeutung 179
2. Schutz der Datenverarbeitung; DDoS 181
3. Grunddelikt und schwere Computersabotage 187
D. Computerbetrug 189
I. Datenmanipulation 190
II. Geldspielautomaten 191
III. Dreieckscomputerbetrug 193
IV. Manipulierte Sportwetten 194
V. Cashing 195
VI. Systematische Struktur- und Wertgleichheit 195
E. IuK-Straftaten im Vorbereitungsstadium 197
I. Tatphasen 200
II. Computerprogramme 203
III. Einsatz von Hardware 204
IV. Passwörter und Zugangscodes 205
V. Kopierschutz. Warez 206
VI. Verabredung von IuK-Verbrechen 206

Kapitel 6. Malware 209
A. Basis-Malware 212
B. Vorbereitungsstadium 215
I. Distanzdelikte 215
II. Vorbereitende IuK-Straftaten und Beginn des Versuchs 219
III. Strafbarer Versuch 223

C. Anlieferung und Installation 224
D. Einnisten und Tarnung 232
I. Ransomware 233
II. Viren und Würmer 234
III. Backdoors 234
IV. Keylogger und Spyware 235
V. Verzögert und langfristig wirkende Malware 236
VI. Tarnung. Stealth 237
VII. Zusammenfassung 238

Kapitel 7. Botnetze 239

A. Straftaten im Betrieb eines Botnetzes 240
B. Steuerung eines Botnetzes 241
C. Spezialisierte Bot Ware gegen Kritische Infrastrukturen 242

Kapitel 8. Missbräuchliche Datenverwertung und Rechtsverfolgung 245

A. Dienstgeheimnisse 245
B. Privater Missbrauch von Verbindungsdaten 246
C. Geschäfts- und Betriebsgeheimnisse 247
D. Steuerdaten-CDs 248
E. Fallen und Abmahnungen 249
F. TrafficHolder 251
G. Gesetz zur Datenhehlerei 253

Kapitel 9. Bargeldloser Zahlungsverkehr 255

A. Anweisung 255
B. Lastschriftverfahren 257
I. Erklärungen des BGH zum automatisierten Lastschriftverfahren 259
II. Vertragsverhältnisse im Lastschriftverfahren 260
III. Bankkonto und Zahlungsdienste 261
IV. Schadensrisiken und Schadensgemeinschaft 264
1. Inkassostelle 264
2. Kontoinhaber 265
3. Zahlstelle und Zahlungsdiensterahmenvertrag 266
4. Schadensgemeinschaft zwischen Zahlstelle und Kontoinhaber 268
C. Autorisierung bei Zahlungskarten und Clearing 270
D. Sicherheitsmerkmale von Zahlungskarten 273
E. Neue Instrumente im Zahlungsverkehr 275
I. Originäre Zahlungsverfahren 275
II. Abgeleitete Zahlungsverfahren 276
III. Aktuelle Bezahl- und Verrechnungsverfahren 279
1. Virtualisierte Zahlungs- und Bankdienste 279
2. Kontokorrentsysteme 279
3. Kreditäre Abrechnungssysteme 280
4. Gutscheinhändler 280
5. Proprietäre Verrechnungssysteme. BitCoins 280
6. Wechselstuben 281
IV. Fazit 281

Kapitel 10. Betrug, Irrtum und Schaden 283

A. Kaufvertrag und Irrtum 285
B. Besondere Formen des Betruges 288
C. Täuschung über die Zahlungsfähigkeit 290
D. Risikogeschäfte und Schaden 291
E. Schadenseintritt und Vermögensgefährdung 293
F. Kreditbetrug und Rückzahlungsanspruch 295
G. Debitkonto und Kartenmissbrauch 296
H. Kontoeröffnungsbetrug 298
I. Gefälschte Schecks 303
J. Manipulationen mit Bankkonten 304
K. Fazit 307

Kapitel 11. Zahlungs- und Warenverkehr 309

A. Beschaffung von Daten 310
B. Beschaffung von Tatausführungsmitteln 312
C. Tatausführung 314
D. Beuteerlös und -sicherung 316

Kapitel 12. Skimming 321

A. Skimming als mehrgliedriges Delikt 321
I. Cashing als finales Tatziel 323
II. Fälschungsdelikte 324
III. Zahlungskarten 326
IV. Grundlagen zum Skimming 327
B. Tatphasen, Versuch und Vorbereitung 329
I. Beteiligung am Versuch 331
II. Umgangsdelikte in der Vorbereitungsphase 336
III. Skimming im engeren Sinne 339
IV. Datenbeschaffung per Hacking 343
V. Verabredung zum Skimming 345
1. Gewerbsmäßiges Handeln 346
2. Bande 346
3. Beteiligung an einer Straftat 348
4. Täter hinter dem Täter 349
5. Zwischenergebnisse 350
6. Tatvarianten bei der Beteiligung am Skimming 351
VI. Deliktische Einheiten und Konkurrenzen 353

Kapitel 13. Urkunden und beweiserhebliche Daten 357

A. Urkunde und Abbild 360
B. Amtliche Ausweise und Persobuilder 365
C. Identitätstäuschung 367
I. Anonymität, Pseudonym und Identität 367
II. Datenlüge und Identitätstäuschung 370
1. Strafbare Täuschung: Kammergericht Berlin. 370
2. Straflose Datenlüge: OLG Hamm. 371
3. Offene und verdeckte Pseudonyme; Lehnnamen. 372

D. Falsche beweiserhebliche Daten ... 373
E. Fakes, falsche und Lehnnamen ... 377
I. Fake Account und Fake-Identität ... 377
II. Lehnnamen ... 377
III. Bankdrops ... 379
IV. Fazit ... 381
F. Virtuelle Kommunikation und Abbilder ... 381
I. Quasiurkunden ... 382
II. Spam-Mails und Schutzrechte ... 383
III. Technische Stempel und Adressen ... 384
IV. Namens- und Identitätstäuschung ... 385
G. Urkunde und Quasiurkunde ... 388
I. Abbild und Verkörperung ... 389
II. Lüge oder Identitätstäuschung ... 391

Kapitel 14. Phishing ... 395

A. Finanzagenten ... 397
I. Vollendung und Beendigung ... 398
II. Doppelter Gehilfenvorsatz ... 399
III. Begünstigung ... 400
IV. Geldwäsche und Hehlerei ... 401
B. Klassisches Phishing ... 401
I. Tatphasen beim Kontohacking ... 403
II. Werbung von Finanzagenten ... 405
III. Webdesign und Werbetexte ... 406
C. Nachgemachte Webseiten ... 408
D. Direkter Eingriff in das Onlinebanking ... 410
E. Vollautomatisches Phishing ... 414
F. Fazit: Phishing in verschiedenen Phasen ... 418

Kapitel 15. Onlinehandel und Underground Economy ... 423

A. Webshops ... 423
B. Abofallen ... 427
I. Kompakte Handlungsmodelle ... 430
II. Göttinger Abofalle ... 433
III. Gewinnspieleintragungsdienste ... 433
IV. Fazit ... 434
C. Nummerntricks ... 435
I. Klassische Nummerntricks (Spoofing) ... 435
II. Erfolgreiche Regulierung ... 436
III. Rückruftrick. Ping-Anrufe ... 437
D. Carding- und andere Boards ... 439
I. Cardingboards ... 441
II. Kriminelle Geschäfte ... 442
1. Eigene kriminelle Geschäfte ... 442
2. Öffentliche Aufforderung zu Straftaten ... 444
III. Kriminelle Vereinigung ... 444
1. Mitgliedschaft ... 445
2. Gründung und Beteiligung ... 446

3. Unterstützung und Werbung 446
4. Rädelsführer und Hintermänner 446
IV. Kriminelle Vereinigung im IuK-Strafrecht 447
E. Bullet Proof-Dienste 448
F. Anonymisierungsdienste 451
G. Zahlungsdienste und Geldwäsche 459

Kapitel 16. Äußerungsdelikte 463

Kapitel 17. Pornografische Abbildungen 469

A. Nacktheit. Posing. Pornografie 470
B. Schutzzwecke 472
C. Herstellungs-, Verschaffungs- und Verbreitungsverbote 473
D. Zwischenspeicher 474
E. Zugänglichmachen. Besitzverschaffung 476

Teil 3: Ermittlungen gegen das Cybercrime 479

Kapitel 18. Strafverfolgung, Verdacht und Ermittlungen 481

A. Aufgaben der Strafverfolgung 482
B. Ermittlungshandlungen 486
I. Auskunftsersuchen oder Rasterfahndung? 486
II. Klassische Erkenntnisquellen 487
III. Verdeckte Ermittlungen 488
C. Anhaltspunkte und Verdacht 490
I. Spurenkritik und zulässige Eingriffsmaßahme 491
II. Anfangsverdacht 494
III. Geltung von Tatsachen und Erfahrungen 496
IV. Eignung, Erfolgserwartung und Ermittlungsplan 498
V. Gefahr im Verzug 501
D. Verwertungsgrenzen und -verbote 502
I. Erhebungs- und Verwertungsverbote 502
1. Kernbereich der persönlichen Lebensgestaltung 504
2. Beweisverwertungsverbote 505
3. Zusammenfassung 506
II. Hypothetischer Ersatzeingriff 509
III. Kollidierende Verfahrensordnungen 511
E. Ermittlungsmaßnahmen im Überblick 514
I. Polizeiliche Eingriffsmaßnahmen 514
II. Beschränkte Eingriffsmaßnahmen ohne Katalogbindung 515
III. Personale Ermittlungen gegen die erhebliche Kriminalität 516
IV. Technische Eingriffsmaßnahmen 516

Kapitel 19. Das Internet und die IuK-Technik als Informationsquellen 519

A. BVerfG zur Onlinedurchsuchung 519
B. Persönlichkeitsschutz durch Grundrechte 521
I. Telekommunikationsgeheimnis und Verkehrsdaten 524
II. Informationelle Selbstbestimmung 526
III. Vertraulichkeit und Integrität informationstechnischer Systeme 526

IV. Unverletzlichkeit der Wohnung 527
V. Eingriffstiefe und additive Grundrechtseingriffe 528
C. Dokumentationsermächtigung und Akten 529
D. Ergebnisse 531

Kapitel 20. Informationsquellen und Sachbeweise 533

A. Öffentliche Quellen und behördliche Auskünfte 534
I. Öffentliche Quellen und Kommunikation 535
II. Behördliche Auskünfte 536
III. Registerauskünfte 537
B. Auskünfte und Zwangsmittel 538
C. Bestandsdaten 539
D. Verkehrsdaten 541
E. Durchsuchung 543
I. Durchsicht und Sicherstellung 544
II. Ferndurchsicht 546
F. Beschlagnahme von E-Mail-Konten 548

Kapitel 21. Personale Ermittlungen 551

A. Informanten und Vertrauenspersonen 552
B. NoeB und Verdeckte Ermittler 555
I. Verdeckte Ermittler 555
II. Nicht offen ermittelnde Polizeibeamte 556
III. Abgrenzung zwischen NoeB und VE 558
IV. Verdeckte personale Ermittlungen gegen das Cybercrime 560
C. Zugangsverschaffung 562
I. Nutzung fremder Zugangsdaten 562
II. Zugangsbeschränkungen und Keuschheitsproben 563
III. Scheinkauf 564

Kapitel 22. Technische Maßnahmen 565

A. Observation und technische Mittel 565
B. TKÜ und Serverüberwachung 567
I. Überwachung der Telekommunikation 567
II. Auslandskopfüberwachung 569
III. IMSI-Catcher 569
C. Onlinedurchsuchung und Quellen-TKÜ 570
D. Spyware und Crawler 572

Glossar 573

Rechtsprechungsübersicht 651

Stichwortverzeichnis 663