

Inhaltsverzeichnis

Vorwort	V
Verzeichnis der Autorinnen und Autoren	VII
Abkürzungsverzeichnis	XXXIII

A. Einführung

I. Cybercrime – eine Bestandsaufnahme

Claudia Brewi/Georg Royer

1. Was ist Cybercrime?	3
1.1. Das Phänomen „Cybercrime“	3
1.1.1. Cybercrime im engeren Sinn	5
1.1.2. Cybercrime im weiteren Sinn	5
1.2. Herausforderungen für die Strafverfolgungsbehörden	7
2. Relevante Player und Stakeholder im Bereich Cybercrime	8
2.1. Täterseite	8
2.1.1. Cybercrime-Industrie – Crime as a Service (CaaS)	8
2.1.2. Digital Natives	9
2.2. Opferseite	10
2.3. Stakeholder im Bereich Prävention, Bekämpfung und Verfolgung von Cybercrime	11
2.3.1. Cybercrime Competence Center (C4) im Bundes- kriminalamt	11
2.3.2. Kompetenzstelle CYBERCRIME der Staatsanwalt- schaften	13
2.3.3. Die Rolle von Europol und Interpol bei Cyber- kriminalität	13
2.3.4. Zuständige Bundesministerien im Bereich Cybercrime ...	14
2.3.5. Weitere Gremien in der österreichischen Bundes- verwaltung	15
2.3.5.1. Cyber Sicherheit Steuerungsgruppe und Cyber Sicherheit Plattform (CSP)	15
2.3.5.2. Operative Koordinierungsstruktur (OpKoord) und Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)	15
2.3.5.3. Cyberkrisenmanagement-Koordinationsausschuss (CKM-KA)	16

2.3.5.4.	Computer Emergency Response Team (CERT.at)	16
2.3.5.5.	Cyber Diplomacy Toolbox der EU	17
2.3.6.	Abteilung Cybersicherheit in der Direktion Staatsschutz und Nachrichtendienst (DSN)	17

II. Kurzer Abriss der relevantesten IT-Aspekte

Martin Haunschmid

1.	Vorbemerkung	19
1.1.	Eine neue Realität	19
1.2.	Alte Denkmuster, neue Herausforderungen	20
2.	Schutzziele	21
2.1.	Vertraulichkeit	21
2.2.	Integrität	22
2.3.	Verfügbarkeit	22
3.	Was versuchen wir zu schützen?	22
4.	Von wem geht die Gefahr aus?	23
4.1.	Advanced Persistent Threat (APT)	23
4.2.	Ransomware-Gruppen	24
4.3.	Business-E-Mail-Compromise-Gruppierungen	26
4.4.	Databroker und Initial Access Broker	27
4.5.	Hacktivisten (Hacker + Aktivisten)	27
4.6.	Betrüger	28
4.7.	Mitarbeiter	28
5.	Das Gefahrenmodell	28
5.1.	Beispielszenarien im Gefahrenmodell	29
5.1.1.	Diebstahl	29
5.1.2.	Identitätsdiebstahl	29
5.1.3.	Passwort wird öffentlich	30
5.1.4.	Ransomware	30
5.1.5.	Wirtschaftsspionage	30
5.1.6.	Physischer Zugriff	31
5.1.7.	Kompromittierte Lieferkette	31
5.1.8.	Business E-Mail Compromise	31
5.2.	Vom Threat Model zu Maßnahmen	31
6.	Ablauf eines typischen Cyberangriffes	32
6.1.	MITRE ATT&CK Framework	32
7.	Best Practices	34
7.1.	Mehr als eine Stadtmauer: Defense in Depth	35
7.2.	Maximale Sichtbarkeit	35

7.3. Schnelle Reaktionszeit	36
7.4. Schnelle Wiederherstellung	36
7.5. Minimale Privilegien	36
7.6. Nicht die eigene Hausübung bewerten	36

B. Materielles Strafrecht

III. Cybercrime-Delikte im StGB

Pilar Mayer-Koukol/Patricia Grandits

1. Was ist strafbar – und warum?	41
2. Begriffsbestimmungen und Prozessuales	43
2.1. Computersystem	43
2.2. Verfügungsbefugnis	44
2.3. Kritische Infrastruktur	44
2.4. Kriminelle Vereinigung	44
2.5. Vorrichtung	45
2.6. Vor- und Nachteil	45
2.7. Daten	45
2.8. Verfolgungsermächtigung	46
3. Cybercrime-Delikte im engeren Sinn	46
3.1. Widerrechtlicher Zugriff auf ein Computersystem gemäß § 118a StGB	46
3.1.1. Die Tatbestandselemente	48
3.1.1.1. Objektive Tatseite	48
3.1.1.1.1. Sich-Zugang-Verschaffen	48
3.1.1.1.2. Überwindung einer spezifischen Sicherheitsvorkehrung ...	49
3.1.1.2. Subjektive Tatseite	52
3.1.2. Qualifikationen	53
3.1.3. Rechtfertigung	54
3.1.4. Beispiele aus der Praxis	54
3.2. Verletzung des Telekommunikationsgeheimnisses nach § 119 StGB	55
3.2.1. Die Tatbestandselemente	56
3.2.1.1. Objektive Tatseite	56
3.2.1.2. Subjektive Tatseite	57
3.2.1.3. Beispiel und Rechtfertigung	57
3.3. Missbräuchliches Abfangen von Daten gemäß § 119a StGB	57
3.3.1. Die Tatbestandselemente	58
3.3.1.1. Objektive Tatseite	58
3.3.1.2. Subjektive Tatseite	59

3.4.	Datenfälschung gemäß § 225a StGB	59
3.4.1.	Die Tatbestandselemente	60
3.4.1.1.	Objektive Tatseite	60
3.4.1.2.	Subjektive Tatseite	60
3.5.	Datenbeschädigung gemäß § 126a StGB	61
3.5.1.	Die Tatbestandselemente	61
3.5.1.1.	Objektive Tatseite	61
3.5.1.2.	Subjektive Tatseite	62
3.5.2.	Qualifikationen	63
3.5.3.	Privilegierung und Strafaufhebung	63
3.6.	Störung der Funktionsfähigkeit eines Computersystems gemäß § 126b StGB	63
3.6.1.	Die Tatbestandselemente	64
3.6.1.1.	Objektive Tatseite	64
3.6.1.2.	Subjektive Tatseite	65
3.6.2.	Qualifikationen	65
3.6.3.	Privilegierung und Strafaufhebung	66
3.7.	Missbrauch von Computerprogrammen oder Zugangsdaten gemäß § 126c StGB	66
3.7.1.	Die Tatbestandselemente	66
3.7.1.1.	Objektive Tatseite	66
3.7.1.2.	Subjektive Tatseite	67
3.7.2.	Qualifikationen	67
3.7.3.	Strafaufhebung	67

IV. Online- und Krypto-Betrug

Claudia Brewi

1.	Vorbemerkung	71
2.	Erscheinungsformen von Online- und Krypto-Betrug	72
2.1.	Phishing	72
2.2.	Fake President Fraud	73
2.3.	Authority Scam	74
2.4.	Fake Invoice und Overpayment Fraud	75
2.5.	Fake Shops	75
2.6.	Bestellbetrug, Bezahldienst- und Transportdienst-Trick	76
2.7.	Pig Butchering – Liebes- und Investmentbetrug	77
2.8.	Krypto-Betrug	78
3.	Einschlägige Strafbestimmungen	79
3.1.	Betrug gemäß § 146 StGB	79
3.1.1.	Tatbestandselemente	79
3.1.2.	Qualifikation nach § 147 StGB	82

3.2. Betrügerischer Datenverarbeitungsmissbrauch gemäß § 148a StGB	83
3.2.1. Tatbestandselemente	83
3.2.2. Qualifikation nach Abs 2 leg cit	85
3.3. Exkurs: Erpressung gemäß § 144 StGB	85
3.4. Sonderprobleme iZm Krypto-Assets	87
3.4.1. Technische Rahmenbedingungen – Blockchain	87
3.4.2. Inländische Gerichtsbarkeit	89
3.4.3. Vermögensbefriedigung von Geschädigten	90
4. Was tun bei Online- oder Krypto-Betrug?	91

V. Online-Suchtgifthandel

Noah McElheney

1. Allgemeines	93
1.1. Vorbemerkung	93
1.2. Erscheinungsformen und Besonderheiten des Online-Suchtgifthandels	93
1.2.1. Soziale Medien	94
1.2.2. Mobile Datenträger und Kryptohandys	94
1.3. Darknet im Besonderen	97
1.4. Ausblick	98
2. Überblick der relevanten SMG-Bestimmungen	99
2.1. Der Grundtatbestand nach § 27 Abs 1 SMG	100
2.1.1. Tatobjekt Suchtgift	100
2.1.2. Die im Zusammenhang mit Online-Handel typischen Tathandlungen	101
2.1.3. Privilegierung zum persönlichen Gebrauch nach § 27 Abs 2 SMG	103
2.1.4. Vorläufiger Rücktritt von der Verfolgung nach § 35 Abs 1 SMG	104
2.2. Unterschreiten der Grenzmenge	105
2.3. § 28 SMG und § 28a SMG	106
2.3.1. Aufteilung der Tathandlungen	106
2.3.2. Überschreiten der Grenzmenge	107
2.3.3. Die Qualifikationen	108
2.3.4. Die Privilegierungen	109
2.3.5. Therapie statt Strafe (§ 39 SMG)	110
3. Das Neue-Psychoaktive-Substanzen-Gesetz (NPSG)	112
4. Besonderheiten zur inländischen Gerichtsbarkeit und Auslieferung	113

VI. Cyberterrorismus

Samuel Benedik/Victoria Demal

1. Einleitung	117
2. Begriff des Terrorismus	117
3. Begriff und Abgrenzung Cyberterrorismus	118
4. Gesetzgeberische Bestrebungen der letzten Jahre im Zusammenhang mit der Bekämpfung von Cyberterrorismus	119
4.1. Strafrechtsänderungsgesetz 2018 – Bekämpfung des Cyberterrorismus ieS	119
4.2. Terrorinhalte-Bekämpfungsgesetz – Bekämpfung des Cyberterrorismus iwS	120
5. Cyberterrorismus ieS	120
5.1. Überblick	121
5.2. Sockeltatbestände des § 278c Abs 1 Z 6 2. und 3. Fall StGB	122
5.2.1. Objektive Tatseite des Grunddelikts des § 126a Abs 1 StGB	122
5.2.2. Objektive Tatseite des Grunddelikts des § 126b Abs 1 StGB	124
5.2.3. Weitere Voraussetzungen für die Erfüllung der Sockeltatbestände	125
5.2.3.1. Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß	126
5.2.3.2. Beeinträchtigung vieler Computersysteme	127
5.2.3.3. Beeinträchtigung wesentlicher Bestandteile der kritischen Infrastruktur	128
5.3. Terroristische Eignung	129
5.4. Vorsatz	130
5.4.1. Vorsatz auf die Erfüllung der Sockeltatbestände	130
5.4.2. Vorsatz auf die terroristische Eignung	131
5.4.3. Erweiterter Vorsatz der terroristischen Zielsetzung	131
5.5. Ausschlussgrund des Abs 3	131
5.6. Strafraumen	132
5.7. Konkurrenzen	133
5.8. Beispiele von Cyberterrorismus ieS in der Vergangenheit	133
5.8.1. Stuxnet	133
5.8.2. Ukrainische Stromausfälle 2015	134
6. Cyberterrorismus iwS	134

VII. Cybercrime und Geldwäsche – eine Bestandsaufnahme

Holger Bielez

1. Einleitung	137
2. Cybercrime und Geldwäsche	137
3. Was ist Cyber-Geldwäsche (Cyber-Laundering)?	139
4. Praktische Erscheinungsformen der Cyber-Geldwäsche	142
4.1. Überblick	142
4.2. Virtuelle Währungen und Krypto-Assets	145
4.2.1. Bitcoin und seine zentralen Eigenschaften	146
4.2.2. Eignung von Bitcoin zur Geldwäsche	148
4.2.3. Weitere Arten von Krypto-Assets	150
4.2.4. Stablecoins	150
4.2.5. Zwischenergebnis	151
4.3. Geldwäsche im Kryptobereich in der Praxis	152
4.3.1. Allgemein	152
4.3.2. NFT und Geldwäsche	155
5. Jüngere unionsrechtliche Maßnahmen zur Eindämmung der Geldwäsche	156
5.1. Allgemeines	156
5.2. Besondere Regelungen für Krypto-Dienstleistungen	159
6. Ausblick	164

VIII. Hass im Netz

Georg Royer

1. Einleitung	167
2. Relevante Straftatbestände	168
2.1. Nötigung (§ 105 StGB)	168
2.2. Gefährliche Drohung (§ 107 StGB)	168
2.3. Beharrliche Verfolgung (§ 107a StGB)	170
2.4. Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems („Cybermobbing“, § 107c StGB)	172
2.4.1. Einmaliges Tätigwerden ausreichend	173
2.4.2. Im Wege der Telekommunikation oder unter Verwendung eines Computersystems	174
2.4.3. Verletzung der Ehre (Z 1)	174
2.4.4. Tatsache des höchstpersönlichen Lebensbereichs (Z 2)	175

2.4.5.	Wahrnehmbarkeit für eine größere Zahl von Personen ...	175
2.4.6.	Eignung	176
2.4.7.	Sonstiges	177
2.5.	Üble Nachrede (§ 111 StGB)	177
2.6.	Beleidigung (§ 115 StGB)	178
2.7.	Unbefugte Bildaufnahmen (§ 120a StGB)	179
2.7.1.	Geschützter Bereich	180
2.7.2.	Subjektive Tatseite	181
2.7.3.	Zugänglichmachen bzw Veröffentlichen (§ 120a Abs 2 StGB)	181
2.8.	Kreditschädigung (§ 152 StGB)	182
2.9.	Verhetzung (§ 283 StGB)	183
2.10.	Datenverarbeitung in Gewinn- oder Schädigungsabsicht (§ 63 DSGVO)	187
2.10.1.	Widerrechtliches Verschaffen	187
2.10.2.	Tathandlung	188
2.10.3.	Verbotsgesetz 1947	189

IX. Identitätsdiebstahl

Angelika Lange

1.	Definition und Bedeutung von Identitätsdiebstahl	191
2.	Wie gelangen Cyberkriminelle an die Daten?	192
2.1.	Häufigste Methoden zur Datenbeschaffung	192
2.2.	Neue Möglichkeiten durch künstliche Intelligenz	194
3.	Konsequenzen von Identitätsdiebstahl	196
3.1.	Strafbarkeit wegen des Beschaffens der Daten	196
3.2.	Strafbarkeit wegen der Verwendung der Daten	198
3.2.1.	Strafbarkeit nach dem StGB	198
3.2.2.	Strafbarkeit nach dem DSGVO	198
3.3.	Identitätsdiebstahl als Erschwerungsgrund bei Strafzumessung ...	199
3.4.	Exkurs: Strafanwendungsrecht	200
3.5.	Möglichkeiten und Grenzen des Strafrechts	201
4.	Strategien für die Prävention von Identitätsdiebstahl	201
4.1.	Strategien für Unternehmen	201
4.2.	Strategien für Einzelpersonen	203
5.	Was können Betroffene tun?	203
6.	Conclusio	204

C. Strafverfahren und Ermittlungen

X. (Internationale) Zuständigkeitsfragen

Simone Marxer

1. Einleitung	209
1.1. Allgemeines zum internationalen Strafrecht	209
1.2. Prinzipien des internationalen Strafrechts	209
2. Inländische Zuständigkeit bei inländischem Tatort gemäß §§ 62, 67 StGB	210
3. Inländische Zuständigkeit bei ausländischem Tatort gemäß §§ 64, 65 StGB	211
3.1. Anknüpfung nach § 64 StGB	211
3.2. Anknüpfung nach § 65 StGB	212
4. Zuständigkeit bei ausgewählten Cybercrime-Delikten	213
4.1. Erfolgsdelikte im Allgemeinen (Betrug, Erpressung)	213
4.2. Äußerungsdelikte/Hass im Netz	215
4.2.1. Allgemeines	215
4.2.2. Üble Nachrede	215
4.2.3. Beleidigung	216
4.2.4. Cybermobbing	216
4.3. Delikte betreffend Verletzungen der Privatsphäre	217
4.3.1. Allgemeines	217
4.3.2. Widerrechtlicher Zugriff auf ein Computersystem	217
4.3.3. Verletzung des Telekommunikationsgeheimnisses	218
4.3.4. Missbräuchliches Abfangen von Daten	218
4.4. Delikte betreffend Daten, Computersysteme und Computerprogramme	219
4.4.1. Allgemeines	219
4.4.2. Datenbeschädigung	219
4.4.3. Störung der Funktionsfähigkeit eines Computersystems	219
4.4.4. Missbrauch von Computerprogrammen oder Zugangsdaten	219
4.5. Kriminelle Organisation (§ 64 Abs 1 Z 4 StGB)	220
4.6. Suchtmitteldelikte (§ 64 Abs 1 Z 4 StGB)	220
4.7. Pornographische Darstellung Minderjähriger (§ 64 Abs 1 Z 4a StGB)	221
4.8. Geldwäscherei (§ 64 Abs 1 Z 8 StGB)	222
4.9. Terroristische Straftaten (§ 64 Abs 1 Z 9 StGB)	223

XI. Strafverfahren und Ermittlungsbefugnisse

Elias Schönborn/Shirin Ghazanfari/Jan Thiel

1. Ermittlungsbefugnisse der Strafverfolgungsbehörden	225
1.1. Verhältnismäßigkeitsgrundsatz (§ 5 StPO)	225
1.2. Sicherstellung und Beschlagnahme	226
1.2.1. Sicherstellung (§ 109 Z 1, §§ 110 ff StPO)	226
1.2.2. Besonderheiten bei (kommunikationsfähigen) Datenträgern	228
1.2.3. Beschlagnahme von Datenträgern und Daten (§ 109 Z 2a–2e, §§ 115f–115l StPO)	229
1.2.3.1. Beschlagnahme von Datenträgern und Daten (§ 115f StPO)	230
1.2.3.2. Mitwirkungspflicht (§ 115g StPO) und Aufbereitung von Daten (§ 115h StPO)	232
1.2.3.3. Auswertung von Daten (§ 115i StPO)	233
1.2.3.4. Rechtsschutz (§ 115l StPO)	235
1.2.3.5. Übergangsregelung (§ 516 Abs 13 StPO) und Fazit	237
1.2.4. Beschlagnahme (§ 109 Z 2, § 115 StPO)	238
1.2.5. Sonderfall: Sicherung von Vermögenswerten	238
1.3. Durchsuchung von Orten und Gegenständen (§§ 119 ff StPO) ...	240
1.4. Verdeckte Ermittlung und Scheingeschäft (§§ 129 ff StPO)	242
1.4.1. Verdeckte Ermittlung (§ 131 StPO)	242
1.4.2. Scheingeschäft (§ 132 StPO)	243
1.5. Beschlagnahme von Briefen, Auskunft über Stamm- und Zugangs- daten, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdaten- speicherung und Überwachung von Nachrichten (§§ 134, 135 StPO)	244
1.5.1. Beschlagnahme von Briefen (§ 134 Z 1, § 135 Abs 1 StPO)	244
1.5.2. Auskunft über Stamm- und Zugangsdaten (§ 134 Z 1a und 1b, § 135 Abs 1a StPO)	245
1.5.2.1. Stammdaten (§ 134 Z 1a StPO)	246
1.5.2.2. Zugangsdaten (§ 134 Z 1b StPO)	247
1.5.3. Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2, § 135 Abs 2 StPO)	247
1.5.4. Lokalisierung der technischen Einrichtung (§ 134 Z 2a, § 135 Abs 2a StPO)	248
1.5.5. Anlassdatenspeicherung (§ 134 Z 2b, § 135 Abs 2b StPO)	249
1.5.6. Überwachung von Nachrichten (§ 134 Z 3, § 135 Abs 3 StPO)	250

2. Datenschutz im Strafverfahren	254
2.1. Rechtsgrundlagen	254
2.1.1. Datenschutzgesetz	254
2.1.2. Art 8 EMRK	255
2.2. Teilaspekte des Grundrechts auf Datenschutz	257
2.2.1. Geheimhaltung	257
2.2.2. Auskunft	258
2.2.3. Löschung	259
2.2.4. Richtigstellung	260
2.3. Einfachgesetzlicher Schutz in der StPO	261
2.3.1. Allgemeines	261
2.3.2. Einschränkung der Verarbeitung personenbezogener Daten in Strafverfahren	261
2.3.3. Datenlöschung	264
2.3.4. Akteneinsicht	265
2.3.5. Einspruch wegen Rechtsverletzung (§ 106 StPO)	266

XII. Cyberkriminalität im Bereich der Polizei

Christian Baumgartner

1. Cybercrime und die Polizei	275
1.1. Vorbemerkung	275
1.2. Begrifflichkeiten	276
1.2.1. Cybercrime	276
1.2.2. Cybersecurity	277
1.2.3. Cyberprevention	277
1.3. Bekämpfung von Cybercrime	278
1.3.1. Rechtliche Komponente	278
1.3.2. Technische Komponenten	279
1.3.3. Organisatorische Komponenten	279
2. Angriffsvektoren	280
2.1. Technische und organisatorische Schwachstellen	281
2.2. Menschliche Schwachstellen	282
3. Lessons learned in technischer Hinsicht	282
3.1. Fehlende Sicherheitssoftware oder Updates	283
3.2. Schlechtes Passwortmanagement	283
3.3. Fehlende Backupstrategie	284
3.4. Falsches Rechtemanagement	284
4. Lessons learned in menschlicher Hinsicht	285
4.1. Betrug und Täuschung	285
4.2. Cyber-Competence	285

5. Was tut die Polizei und wie kann man die Polizei dabei unterstützen? ...	286
5.1. Die Werkzeuge der Polizei	286
5.2. Unterstützung der Polizei bei der Bekämpfung von Cyber- kriminalität	287
5.3. Verantwortlichkeiten im Bereich der Betroffenen	288
6. Fazit	288

D. Schutz vor und Abwehr von Cybercrime

XIII. Der Schutz vor Cybercrime als Staatsaufgabe

Célia Royer/Georg Royer

1. (Cyber-)Sicherheit als Staatsaufgabe	293
2. Sicherheitsstrategien (auch) zum Schutz vor Cybercrime	294
2.1. Strategien auf Unionsebene	295
2.1.1. Globale Strategie für die Außen- und Sicherheitspolitik der EU	295
2.1.2. Strategie für die innere Sicherheit der EU (ISS)	295
2.1.3. EU-Strategie für die Sicherheitsunion	296
2.1.4. EU-Cybersicherheitsstrategie	297
2.2. Österreichische Strategien	298
2.2.1. Österreichische Sicherheitsstrategie (ÖSS)	298
2.2.2. Teilstrategie Innere Sicherheit (TIS)	299
2.2.3. Strategie INNEN.SICHER	301
2.2.4. Österreichische Strategie für Cybersicherheit 2021 (ÖSCS 2021)	301
3. Der Schutz der kritischen Infrastruktur vor Cybercrime	304
3.1. NIS-2-Richtlinie und NISG	305
3.2. Investitionskontrolle	305
3.2.1. Prüfung von Risiken iZm Cybersicherheit im Rahmen des investitionskontrollrechtlichen Verfahrens	307

XIV. NIS-2-Richtlinie – Neue Anforderungen an die Cybersicherheit

Beatrice Blümel

1. Einleitung	311
2. Anwendungsbereich	312
2.1. Voraussetzungen	312
2.1.1. Sektoren mit hoher Kritikalität und sonstige kritische Sektoren	313

2.1.2.	Unternehmensgröße	315
2.1.3.	Örtlicher Anwendungsbereich	316
2.2.	Wesentliche und wichtige Einrichtungen	316
2.3.	Ausnahmen	318
3.	Pflichten für Unternehmen	318
3.1.	Registrierung, Selbstdeklaration und Nachweispflicht	318
3.2.	Governance und Risikomanagement	318
3.3.	Sicherheit der Lieferkette	320
3.4.	Mehrstufige Meldepflichten bei Sicherheitsvorfällen an das CSIRT	321
3.4.1.	Erheblicher Sicherheitsvorfall	321
3.4.2.	CSIRT	322
3.4.3.	Abfolge der Meldungen	322
4.	Sanktionen und weitere Befugnisse der Aufsichtsbehörde	323
4.1.	Sanktionen	323
4.2.	Haftung der Leitungsorgane	324
4.3.	Befugnisse der Aufsichtsbehörde	324
5.	Fazit	325

XV. Technischer Schutz vor und bei Cybercrime

Martin Haunschmid

1.	Warum fällt es so schwer, sich vor Cyberangriffen zu schützen?	327
2.	Einordnung der Maßnahmen	327
3.	IT-Hygiene	328
3.1.	Passwörter	328
3.1.1.	Passwortmanager	329
3.1.2.	Die Wahl des Passwortmanagers	330
3.1.3.	Passwortlose Authentifizierung	330
3.1.4.	Mehrfaktor-Authentifizierung	331
3.2.	Sichtbarkeit	331
3.2.1.	EDR/XDR/SIEM	332
3.2.2.	Security Operations Center	333
3.2.3.	Honeypots: Tarnen und Täuschen	333
3.2.4.	Threat Intelligence	333
3.3.	Identitäten	334
3.3.1.	Nachvollziehbarkeit der Nutzer einer Identität	334
3.3.2.	Lebenszyklus von Accounts	334
3.3.3.	Berechtigungsmanagement	335

3.4. E-Mail und Browser	335
3.4.1. E-Mail-Filter	336
3.4.2. Die „EXTERN“-Warnung	336
3.4.3. Technische Sicherheitsmaßnahmen	336
3.4.4. Werbeblocker	336
3.5. Netzwerksegmentierung und Zero-Trust	337
3.5.1. Remote-Arbeit	337
3.5.2. Zero-Trust	337
3.6. Asset- und Patchmanagement	338
3.7. Backup-Konzept	339
3.8. Bewusstsein	339
3.9. Unternehmenskultur	340
3.10. Datenschutz	340
3.11. Cyberversicherung	340
4. Proaktiv für den Ernstfall planen	340
4.1. Notfallplan	341
4.2. Kontakte zur Incident Response	341
4.3. Parallelinfrastruktur für den Notfall	341
5. Den Ernstfall testen	342
5.1. Backup-Test	343
5.2. Tabletop-Simulationen	343
5.3. Penetrationstests	343
5.4. Red-Teaming	343
6. Fazit	344

XVI. Schutzmaßnahmen als Haftungsminimierung für Unternehmen und ihre Organe

Paul Krepil

1. Einleitung	347
2. Gesetzliche Grundlagen für Organisationspflichten	347
2.1. Internes Kontrollsystem	348
2.2. Compliance-Organisation	349
2.3. Organisatorische und technische Maßnahmen iSd DSGVO	352
3. Spezifische gesetzliche Grundlagen auch für IT-Organisation?	355
3.1. IT-Pflichten für „regulierte Unternehmen“	355
3.1.1. „NIS 2“	355
3.1.2. Sondergesetzliche Vorschriften	356
3.2. IT-Pflichten für „nicht-regulierte“ Unternehmen	356
3.2.1. Pflicht zur Digitalisierung?	356
3.2.2. Pflicht zur Sicherung der IT-Infrastruktur	357
3.2.3. Verletzung der „Business Judgement Rule“?	359

4. Cyber-Versicherungen als sinnvolle Ergänzung	361
5. Fazit	362

XVII. IT-Maßnahmen im Krisenfall

Martin Haunschmid

1. IT-Maßnahmen im Krisenfall	365
2. Erkennen	366
3. Handlungsfähigkeit herstellen	367
3.1. Personen versammeln	367
3.2. War-Room	367
3.3. Kommunikationsfähigkeit	367
4. Eindämmung	367
4.1. Sichtbarkeit nutzen oder herstellen	368
4.2. Kompromittierte Netzwerke isolieren	368
4.3. Kompromittierte Systeme isolieren	368
4.4. Kompromittierte User deaktivieren oder zurücksetzen	369
4.5. Internet kappen?	369
4.6. Stecker ziehen?	369
4.7. Die Hacker merken, wenn man loslegt	369
5. Schadenserhebung	369
5.1. Sichtbarkeit	369
5.2. Was ist passiert?	370
5.3. Gibt es noch Backups?	370
5.4. Brauchen wir externe Hilfe?	370
6. Wiederherstellung und Bereinigung	371
6.1. Alle Zugangsdaten zurücksetzen	371
6.2. Artefakte entfernen	371
6.3. Die grüne Wiese	371
7. Forensik	371
8. Der lange Weg zurück	372
9. Die mentale Komponente	372
10. Lessons Learned	373
11. Das Lösegeld	373
12. Fazit	374

XVIII. Krisen-PR im Falle von Cybercrime

Gregor Schütze

1. Die Wichtigkeit von PR	375
2. In der Krise – Was passiert, wenn was passiert?	376
2.1. Phasen der Krise	378
2.2. Während der Krise – Verhalten im Krisenfall	381
2.2.1. C.A.T.C.H. the Situation!	381
2.2.2. Hackerangriffe	382
2.2.3. Verhalten bei einer Cyberkrise	383
2.3. Grundregeln der Krisenkommunikation	385
3. Vor der Krise	386
3.1. Issues Management	386
3.2. Checkliste mit Vorbereitungsmaßnahmen	387
3.3. Krisenvorbereitung – Maßnahmen	388
3.3.1. Fokus Cyberkrise	390
4. Nach der Krise	390
4.1. Die Post-Incident-Analyse	390
4.2. Künftig Cyberkrisen ganz vermeiden?	391

XIX. Krisenfall Cybercrime im Unternehmen – datenschutzrechtliche Aspekte

Johannes Sekanina/Phillip Wrabetz

1. Einleitung	395
1.1. Datenschutzrechtliche Relevanz von Cybercrime	395
1.2. Krisenfall Cybercrime als „Data Breach“ iSd Art 4 Z 12 DSGVO	395
1.3. Die Normadressaten	398
2. Datenschutzrechtliche Pflichten im Krisenfall Data Breach	399
2.1. Interne Dokumentationspflicht	399
2.2. Meldepflicht an die Datenschutzbehörde (Art 33 DSGVO)	400
2.2.1. Beurteilung der Meldepflicht: Risikobewertung	400
2.2.2. Meldefrist	402
2.2.3. Inhalt der Meldung	403
2.3. Benachrichtigung der betroffenen Personen (Art 34 DSGVO)	405
2.3.1. Bewertung der Benachrichtigungspflicht: Risikobewertung	405
2.3.2. Ausnahmen von der Benachrichtigungspflicht	406

2.3.3. Frist	407
2.3.4. Inhalt der Benachrichtigung	408
2.4. Data-Breach-Response-Plan	408
3. Sanktionen und Rechtsschutz	409

XX. Opfer von Cybercrime – Rechte und Vorgehen in der Praxis

Wolfgang Gappmayer/Diana Seeber-Grimm

1. Einleitung	411
2. Opferbegriff	412
3. Opfererfahrungen	414
3.1. Ransomware	414
3.2. Internetbetrug	416
3.3. Phishing	416
4. Rechtliche Überlegungen	418
4.1. Sorgfaltspflichten	418
4.2. Melde- und Anzeigepflichten	419
4.3. Strafanzeige	419
4.3.1. Zwangsmaßnahmen	421
4.3.1.1. Auskunft über Stamm- und Zugangsdaten	421
4.3.1.2. Auskunft über Bankkonten und Bankgeschäfte	421
4.3.1.3. Sicherstellung und Beschlagnahme	422
4.3.1.4. Privatbeteiligung und Beweisantragsrecht	422
4.3.2. Lösegeldforderung	423
4.3.2.1. Strafrecht	424
4.3.2.2. Embargos und Sanktionen	424
4.3.2.3. Steuerrecht	426
4.3.3. Lösegeldverhandlung	426
5. Öffentlichkeitsarbeit	427
6. Zusammenfassung und Ausblick	427

XXI. Digitale Forensik und Cybercrime

Kerstin Farkas/Dominik Fuss/Alexander Schneider

1. Datenforensik bei forensischen Sonderuntersuchungen	430
2. Digitale Spurensicherung in der Datenforensik	433
2.1. Sammlung digitaler Spuren	433
2.2. Aufbewahrung digitaler Beweise	433
2.3. Analyse digitaler Spuren	434

3. Forensische Datenquellen und Artefakte	434
3.1. IT-Landscaping	434
3.2. Relevante Datenquellen	435
3.2.1. Datenträger, Computer und Laptops	435
3.2.2. Mobiltelefone	436
3.2.3. Arbeitsspeicher/RAM	436
3.2.4. Serverdaten	437
3.2.5. Log-Daten	437
3.3. Forensische Artefakte	437
3.3.1. Ausgeführte Programme/geöffnete Dateien	438
3.3.2. Netzwerkverbindungen	438
3.3.3. Benutzeranmeldungen	438
3.3.4. Persistenzmechanismen/Auto-Start	439
3.3.5. Angeschlossene USB-Geräte	439
4. Forensische Analysemethoden	439
4.1. Das Datenmosaik	439
4.2. Datenwiederherstellung und der Umgang mit korrupten Daten	441
4.3. Timeline	442
4.4. Grenzen der Datenforensik	444
5. Fallbeispiele aus der Praxis	445
5.1. Ransomware	445
5.2. Unautorisierter Zugriff/unautorisierte Aktivitäten/Datendiebstahl	447
5.3. Phishing/Social Engineering	448

E. Aktuelle Entwicklungen und Ausblick

XXII. Aktuelle Entwicklungen und Ausblick

Claudia Brewi/Georg Royer

1. Entwicklungen und Trends	453
1.1. Zunahme von Cybercrime-Fällen	453
1.2. Innovationen und Herausforderungen im Bereich der Strafverfolgung	455
1.3. Aktuelle Trends	457
1.3.1. Crime as a Service (CaaS)	458
1.3.2. Künstliche Intelligenz (KI)	458
1.3.3. Blockchain und Krypto-Assets	460
2. Ausblick	461
2.1. Österreich	461
2.1.1. Quellen-TKÜ vs Bundestrojaner	461
2.1.2. Handysicherstellung	462

2.1.3.	Vorrats- bzw Anlassdatenspeicherung	463
2.1.4.	RTR-Anti-Spoofing-Verordnung	463
2.1.5.	Herausforderungen iZm Krypto-Assets	464
2.1.6.	Reformvorschläge der StAV	466
2.2.	Europäische und internationale Ebene	467
2.2.1.	E-Evidence-VO	467
2.2.2.	EU-Empfehlungen zur Datenent- und verschlüsselung ...	468
2.2.3.	EU-Sanktionen gegen Cyberangriffe	468
2.2.4.	KI-Verordnung der EU	469
2.2.5.	2. Zusatzprotokoll zum Übereinkommen über Computerkriminalität	469
2.2.6.	Verhandlungen zu UN-Cybercrime-Convention	470
	Stichwortverzeichnis	471