

# #Cybercrime

## Handbuch für die Praxis

- Ransomware & Co als Bedrohung
- Prävention und Krisenplan
- Richtiges Verhalten im Anlassfall
- Post Incident Analyse

HERAUSGEGEBEN VON

Dr. Axel Anderl, LL.M.

# Inhaltsverzeichnis

Vorwort .....	V
Autor:innenverzeichnis .....	XVII
Abkürzungsverzeichnis .....	XXI
<b>A. Haftungsfalle Cybercrime .....</b>	<b>1</b>
<b>A.1. Einleitung – Haftungsfalle Cybercrime (Axel Anderl/Nino Tlapak) .....</b>	<b>3</b>
A.1.1. Problemaufriss .....	3
A.1.2. Zunahme und Konsequenzen der Gefahr an Cyberbedrohungen .....	3
A.1.2.1. Weltweiter Anstieg an Cyberangriffen .....	3
A.1.2.2. Ursachen und Auswirkungen .....	5
A.1.2.3. Handlungsbedarf als Konsequenz .....	5
A.1.3. Wichtigkeit der (unterschätzten) Präventionsarbeit .....	7
A.1.3.1. Einhaltung der Sorgfaltspflichten .....	7
A.1.3.2. Mindestumfang der Präventionsmaßnahmen .....	8
A.1.3.3. Lückenlose Dokumentation der ergriffenen Maßnahmen .....	10
A.1.4. Klassischer Ablauf eines Ransomware-Angriffs – worauf kommt es in der Praxis an .....	11
A.1.4.1. Bewusste Druckausübung durch die Angreifer .....	11
A.1.4.2. Erhebung des Status Quo und Identifikation des Risikos .....	12
A.1.4.3. Einhaltung von Melde- und Informationspflichten und Obliegenheiten .....	13
A.1.4.4. Laufende Dokumentation, Aktualisierung und Kooperation .....	14
<b>B. Überblick über die wichtigsten Cybercrime-Delikte .....</b>	<b>17</b>
<b>B.1. Überblick über die wichtigsten Cybercrime-Delikte und ihre Ausformung         (Stephan Mikiss) .....</b>	<b>19</b>
B.1.1. Einleitung .....	19
B.1.2. Grundbegriffe der gängigen Angriffe .....	20
B.1.3. Warum kommt es zu erfolgreichen Angriffen? Häufigste Fehler/Ursachen in der Praxis .....	22
B.1.4. Wesentliche Begriffe in der Prävention .....	23
B.1.5. Ablauf eines Angriffes in der Praxis .....	25
B.1.6. Abwehr von Angriffen .....	28
<b>C. Haftungsvermeidung durch Prävention – Schutz vor dem Ernstfall .....</b>	<b>33</b>
<b>C.1. Einführung und Überblick (Axel Anderl/Nino Tlapak) .....</b>	<b>35</b>
C.1.1. Problemaufriss – rechtliche Vorgaben .....	35
C.1.2. Saubere Dokumentation und Aufstellung der Prozesse .....	36
C.1.3. Implementierung der wesentlichen Abläufe zur Minimierung von Reibungsverlusten .....	37
C.1.4. Vermeidung bzw. Milderung der Haftung .....	38

<b>C.2. Datenschutzrechtliche Pflichten zur Etablierung angemessener Präventionsmaßnahmen</b> ( <i>Nino Tlapak/Alona Klammer</i> ) .....	40
C.2.1. Einführung .....	40
C.2.2. Geeignete technische und organisatorische Maßnahmen .....	40
C.2.2.1. Überblick .....	40
C.2.2.2. Risikobasierter Ansatz .....	42
C.2.2.3. Informationssicherheitsmanagement-System .....	43
C.2.2.3.1. Information Security Policy .....	45
C.2.2.3.2. Information Security Risk Management .....	46
C.2.2.3.3. Festlegung geeigneter TOMs .....	46
C.2.2.3.4. Auditing-Programm .....	48
C.2.2.3.5. Schulung und Sensibilisierung der Mitarbeiter .....	48
C.2.2.3.6. Information Security Incident Management .....	49
C.2.2.4. Rechenschaftspflicht .....	50
C.2.3. Privacy by Design und Privacy by Default .....	51
C.2.3.1. Privacy by Design .....	51
C.2.3.2. Privacy by Default .....	51
C.2.4. Checkliste .....	52
<b>C.3. Technische Vorkehrungen im Rahmen der Prävention</b> ( <i>Michael Zenger</i> ) .....	53
C.3.1. Einleitung – keine technische Generallösung .....	53
C.3.2. IST-Analyse der technischen Vorkehrungen .....	54
C.3.3. Weiterführende Maßnahmen und Best Practice .....	56
C.3.3.1. Konsequentes Patchmanagement .....	56
C.3.3.2. Netzwerksicherheit – unabhängig von der Unternehmensgröße .....	58
C.3.3.3. Endpoint Protection .....	60
C.3.3.4. VPN/Multifaktor Authentifizierung (MFA/2FA) .....	60
C.3.4. Checkliste: 10 To Do's zur Prävention .....	62
<b>C.4. Organisatorische Präventionsmaßnahmen</b> ( <i>Julia Arbery/Kristof Wabl</i> ) .....	63
C.4.1. Problemaufriss .....	63
C.4.2. Cyberresilienz als Teil der Gesamtstrategie .....	63
C.4.3. Checkliste zur Klärung von organisatorischen Fragen .....	65
C.4.4. Maßnahmen zur Steigerung von Resilienz gegen Cyberangriffe .....	67
C.4.4.1. Krisenplanung ist das halbe Leben .....	67
C.4.4.2. Einrichtung eines Krisenstabs .....	70
C.4.4.3. Zusammenarbeit im Krisenstab .....	71
C.4.5. Akute und nachgelagerte Maßnahmen als Reaktion gegen Cyberangriffe .....	72
C.4.6. Fazit .....	75
<b>C.5. Gesellschaftsrechtliche Verpflichtungen im Rahmen der Prävention</b> ( <i>Kathrin Weber</i> ) .....	76
C.5.1. Einleitung .....	76
C.5.2. Internes Kontrollsystem .....	76
C.5.3. IT-Organisationspflichten .....	77
C.5.4. Cyberversicherung .....	78



- C.10. Cyberversicherung als Teil der Lösung (*Stephan Eberlein/Felix Hörlsberger*) ..... 110
  - C.10.1. Einleitung ..... 110
  - C.10.2. Übersicht einer typischen Cyberversicherungslösung ..... 111
    - C.10.2.1. Gegenstand einer Cyberversicherung ..... 112
    - C.10.2.2. Umfang des Versicherungsschutzes ..... 113
      - C.10.2.2.1. Ersatz von Serviceleistungen ..... 113
      - C.10.2.2.2. Ersatz von Eigenschäden ..... 115
      - C.10.2.2.3. Haftungen gegenüber Dritten ..... 116
    - C.10.2.3. Wesentliche Ausschlüsse ..... 117
    - C.10.2.4. Allgemeine Bestimmungen ..... 118
  - C.10.3. Pflichten vor und bei Eintritt eines Schadenfalls ..... 119
    - C.10.3.1. Vorvertragliche Anzeigepflicht ..... 119
    - C.10.3.2. Obliegenheiten vor Eintritt des Versicherungsfalls ..... 120
    - C.10.3.3. Obliegenheiten nach Eintritt des Versicherungsfalls ..... 121
  - C.10.4. Antragsprozess durch Fragebögen und Risikodialoge ..... 121
  - C.10.5. Managerhaftpflichtversicherung bei Cyberrisiken ..... 123
- D. Richtiges Verhalten im Anlassfall – Vorgehen und Fokus im Ernstfall ..... 125
  - D.1. Worauf es im Anlassfall ankommt (*Axel Anderl/Nino Tlapak*) ..... 127
    - D.1.1. Eintritt der Krisensituation ..... 127
    - D.1.2. Fokus auf die wichtigsten Pflichten, Schritte und Dokumentation ..... 128
    - D.1.3. Weichenstellung zur Haftungsminimierung ..... 129
  - D.2. Technische Aufarbeitung (*Michael Denzel/Tobias Weisskopf/Michael Zenger*) ..... 130
    - D.2.1. Unterscheidung: Incident Response gegenüber Digitaler Forensik ..... 130
      - D.2.1.1. Incident Response ..... 130
      - D.2.1.2. Digitale Forensik ..... 130
      - D.2.1.3. Gemeinsamkeiten zwischen Incident Response und Digitaler Forensik ..... 131
    - D.2.2. Incident Response ..... 132
      - D.2.2.1. Vorbereitung (Prepare) ..... 133
      - D.2.2.2. Identifikation des Angriffs (Identify) ..... 134
        - D.2.2.2.1. System-Analyse ..... 135
        - D.2.2.2.2. Netzwerk-Analyse ..... 135
      - D.2.2.3. Abschottung (Contain) ..... 136
      - D.2.2.4. Bereinigung der Systeme (Eradicate) ..... 136
      - D.2.2.5. Wiederherstellung & Wiederanlauf (Recovery) ..... 136
      - D.2.2.6. Lessons Learnt/Post-Incident ..... 137
    - D.2.3. Digitale Forensik ..... 137
      - D.2.3.1. Identification ..... 138
      - D.2.3.2. Preservation ..... 138
      - D.2.3.3. Collection/Acquisition ..... 139
      - D.2.3.4. Datenverarbeitung (Processing) ..... 140
      - D.2.3.5. Review/Analyse ..... 140
      - D.2.3.6. Abschlussbericht und Wiedergabe der Ergebnisse (Production) ..... 141
      - D.2.3.7. Dokumentationsanforderungen ..... 141

<b>D.3. Rechtzeitige Einbindung der Versicherung</b>	
<i>(Stephan Eberlein/Felix Hörlsberger)</i>	145
D.3.1. Einleitung	145
D.3.2. Funktionsweise der Hotline	145
D.3.3. Sinnvolle Nutzung von Netzwerkpartnern	146
<b>D.4. Datenschutzrechtliche Maßnahmen</b>	<i>(Nino Tlapak/Michael Hardt)</i>
D.4.1. Data Breach-Meldung und Vorbereitung auf Betroffenenanfragen	147
D.4.1.1. Cyberangriff als Data Breach	147
D.4.1.2. Wesensmerkmale eines Data Breach	147
D.4.1.2.1. Verletzung der Sicherheit	147
D.4.1.2.2. Vernichtung, Verlust, Veränderung personen-	
bezogener Daten (Verletzung von Verfügbarkeit	
und Integrität)	148
D.4.1.2.3. Unbefugte Offenlegung oder unbefugter Zugang	
zu personenbezogenen Daten (Verletzung von	
Vertraulichkeit)	148
D.4.1.3. Beurteilung der Meldepflicht an die	
Datenschutzbehörde(n)	149
D.4.1.3.1. Verpflichtung zur Meldung	149
D.4.1.3.2. Kurze Meldefristen und rascher Handlungs-	
bedarf	151
D.4.1.3.3. Inhalt der Meldung	153
D.4.1.3.4. Benachrichtigung der Betroffenen	154
D.4.1.3.5. Fazit	156
D.4.1.3.6. Proaktives Beschwerdemanagement	156
<b>D.5. Einbindung der Polizei</b>	<i>(Stephan Steinhofner/Elias Schönborn)</i>
D.5.1. Strategische Überlegungen	157
D.5.2. Kompetenzen – Sicherstellung und Beschlagnahme, Auskunft über	
Stamm- und Zugangsdaten	159
D.5.2.1. Allgemeines	159
D.5.2.2. Sicherstellung (§§ 110 ff StPO)	160
D.5.2.3. Beschlagnahme (§ 115 StPO)	162
D.5.2.4. Verhältnismäßigkeit und gelindere Mittel	162
D.5.2.5. Auskunft über Stamm- und Zugangsdaten (§ 76a StPO)	163
D.5.3. Zusammenfassung	164
<b>D.6. Gesellschaftsrechtliche Verpflichtungen</b>	<i>(Kathrin Weber)</i>
D.6.1. Allgemeines	166
D.6.1.1. Cyber Incident Response Plan (CIRP)	167
D.6.1.2. Response Team	168
<b>D.7. Exkurs: Zusätzliche Pflichten aus dem NISG</b>	<i>(Axel Anderl/Michael Hardt)</i>
D.7.1. Einleitung	169
D.7.2. Vorfälle und Sicherheitsvorfälle	169
D.7.2.1. Begrifflichkeiten	169
D.7.2.2. Regelung für Anbieter digitaler Dienste	170

D.7.3.	Meldung an das Computer-Notfallteam .....	170
D.7.3.1.	Verpflichtende Meldungen .....	170
D.7.3.2.	Freiwillige Meldungen .....	172
D.7.4.	Zeitpunkt der Meldung .....	172
D.7.5.	Weiterleitung der Meldung bei internationalem Bezug .....	173
<b>D.8.</b>	<b>Exkurs: Börserechtliche Vorgaben</b> ( <i>Christoph Brogyányi/ Clemens Burian-Kerbl</i> ) .....	<b>174</b>
D.8.1.	Einleitung .....	174
D.8.2.	Gesetzlicher Rahmen .....	174
D.8.3.	Börserechtliche Compliance im Anlassfall .....	174
D.8.3.1.	Prüf- und Handlungspflichten .....	174
D.8.3.2.	Unrechtmäßige Offenlegung von Insiderinformationen (Art 10 MAR) .....	175
D.8.3.3.	Verpflichtung zum Führen von Insiderlisten .....	176
D.8.3.4.	(Aufschub der) Veröffentlichung einer Insiderinformation (Art 17 MAR) .....	176
<b>D.9.</b>	<b>Exkurs: Vorgaben aus dem Aufsichtsrecht</b> ( <i>Andreas Zahradnik/ Christian Richter-Schöller</i> ) .....	<b>180</b>
D.9.1.	Einleitung .....	180
D.9.2.	Gesetzlicher Rahmen .....	180
D.9.3.	Leitlinien der Aufsichtsbehörden .....	182
D.9.4.	Praktische Umsetzung .....	184
<b>D.10.</b>	<b>Exkurs: Telekommunikationsrechtliche Vorgaben</b> ( <i>Stefan Vouk</i> ) .....	<b>186</b>
D.10.1.	Strafen und Zuständigkeiten nach dem TKG 2021 .....	186
D.10.2.	Richtiges Verhalten im Anlassfall .....	186
D.10.2.1.	Meldepflichten .....	186
D.10.2.2.	Verfahren und Strafdrohungen .....	188
<b>E.</b>	<b>Lösegeldforderungen</b> .....	<b>191</b>
<b>E.1.</b>	<b>Sinnhaftigkeit einer Lösegeldzahlung</b> ( <i>Axel Anderl/Nino Tlapak</i> ) .....	<b>193</b>
E.1.1.	Problemaufriss .....	193
E.1.2.	Umfassendes Lagebild .....	194
E.1.3.	Zuständigkeiten und Berichtslinien .....	195
E.1.4.	Strategische Überlegungen .....	196
<b>E.2.</b>	<b>Strafrechtliche Zulässigkeit von Lösegeldzahlungen</b> ( <i>Stephan Steinhofer/ Elias Schönborn</i> ) .....	<b>198</b>
E.2.1.	Einleitung .....	198
E.2.2.	Einzelne Tatbestände .....	198
E.2.2.1.	Untreue (§ 153 StGB) .....	198
E.2.2.2.	Geldwäscherei (§ 165 StGB) .....	201
E.2.2.3.	Kriminelle Vereinigung (§ 278 StGB) .....	201
E.2.2.4.	Terroristische Vereinigung (§ 278b StGB) .....	202
E.2.2.5.	Terrorismusfinanzierung (§ 278d StGB) .....	203
E.2.3.	Rechtfertigungs- und Entschuldigungsgründe .....	204
E.2.3.1.	Notwehr und rechtfertigender Notstand .....	204
E.2.3.2.	Entschuldigender Notstand .....	206

E.2.4.	Exkurs: Verbandsverantwortlichkeit? .....	206
E.2.5.	Checkliste möglicher Delikte bei Lösegeldzahlung .....	208
<b>E.3.</b>	<b>Schnittstelle Haftung – Business Judgement Rule (Kathrin Weber) .....</b>	<b>209</b>
E.3.1.	Einleitung .....	209
E.3.2.	Die zivilrechtliche Haftung des Geschäftsführers im Überblick .....	210
E.3.2.1.	Voraussetzungen für die Haftung .....	210
E.3.2.2.	Haftung gegenüber der Gesellschaft .....	211
E.3.2.3.	Zuständigkeit für die Geltendmachung des Schadenersatz- anspruchs .....	211
E.3.2.4.	Besondere Beweislastverteilung .....	212
E.3.2.5.	Verjährung .....	212
E.3.3.	Business Judgement Rule .....	212
E.3.3.1.	Unternehmerische Entscheidung .....	213
E.3.3.2.	Keine sachfremden Interessen .....	215
E.3.3.3.	Angemessene Information als Grundlage der Entscheidung .....	216
E.3.3.4.	Ex ante betrachtetes Handeln zum Wohl der Gesellschaft .....	217
E.3.4.	Weisung der Gesellschafter zur Zahlung von Lösegeld .....	218
E.3.4.1.	GmbH .....	218
E.3.4.2.	AG .....	218
E.3.5.	Zusammenfassung: BJR und Lösegeldzahlung .....	219
E.3.6.	Exkurs: BJR und andere unternehmerische Entscheidungen .....	219
<b>F.</b>	<b>Krisenkommunikation .....</b>	<b>221</b>
<b>F.1.</b>	<b>Kommunikation als Schlüsselfaktor (Axel Anderl/Nino Tlapak) .....</b>	<b>223</b>
F.1.1.	Problemaufriss .....	223
F.1.2.	Kommunikationskanäle und Zeitachse .....	224
F.1.3.	Der schmale Grat der Interessensabwägung .....	225
F.1.4.	Wahrung der Vertraulichkeit und Geheimhaltung .....	227
<b>F.2.</b>	<b>Erfolgreiche Krisenkommunikation bei Cyberangriffen (Nicole Bäck-Knapp/ Christoph Görg/Alona Klammer) .....</b>	<b>229</b>
F.2.1.	Einleitung .....	229
F.2.2.	Reputation .....	230
F.2.2.1.	Reputation – ein kostbares Gut .....	230
F.2.2.2.	Reputation und (Kunden-)Vertrauen .....	231
F.2.3.	Strategische Kommunikation im Krisenfall .....	233
F.2.3.1.	Das Krisenteam – Herzkammer der Krisenkommunikation .....	233
F.2.3.2.	Ressourcenplanung .....	234
F.2.3.3.	Schnelles, transparentes Handeln .....	235
F.2.3.4.	Das richtige Narrativ vorbereiten .....	236
F.2.3.5.	Standhaftigkeit braucht innere Geschlossenheit .....	238
F.2.4.	Rechtliche Anforderungen bei der Krisenkommunikation .....	239
F.2.4.1.	Inhalt .....	239
F.2.4.2.	Form .....	241
F.2.5.	Best Case-Krisenkommunikation am Beispiel Clarksons .....	242



F.2.6.	Geben Sie das Steuer nicht aus der Hand .....	242
F.2.7.	Checkliste: Strategische Kommunikation bei Cyberangriffen .....	243
<b>G.</b>	<b>Nachbearbeitung</b> .....	<b>245</b>
<b>G.1.</b>	<b>Wiederaufbau der IT</b> ( <i>Michael Zenger</i> ) .....	<b>247</b>
G.1.1.	Einleitung .....	247
G.1.2.	Bereitstellung der erforderlichen Ressourcen .....	248
G.1.2.1.	Personalressourcen .....	249
G.1.2.2.	Hardwareressourcen .....	249
G.1.2.3.	Cloud-Ressourcen .....	250
G.1.3.	Partnernetzwerk .....	251
<b>G.2.</b>	<b>Dokumentation und Organisation</b> ( <i>Axel Anderl/Nino Tlapak</i> ) .....	<b>252</b>
G.2.1.	Notwendigkeit der Nachbearbeitung und Aufarbeitung .....	252
G.2.2.	Wesentliche Inhalte einer Post Incident Analyse .....	253
G.2.2.1.	Aufarbeitung des konkreten Vorfalls .....	254
G.2.2.2.	Post Incident Analyse – Abgleich mit dem Marktstandard .....	256
G.2.2.3.	Nachbearbeitung – Evaluierung von Lessons Learnt .....	258
G.2.3.	Nachbetrachtung in der Kommunikation .....	260
<b>G.3.</b>	<b>Beobachtung Darknet</b> ( <i>Julia Arbery/Kristof Wabl</i> ) .....	<b>262</b>
G.3.1.	Einführung .....	262
G.3.2.	Anonymität als Grundregel im Darknet .....	262
G.3.3.	Wo Licht ist, ist auch Schatten .....	263
G.3.4.	Strafverfolgung im Niemandsland .....	266
G.3.5.	Private Untersuchungshandlungen im Darknet .....	267
<b>H.</b>	<b>Schadenersatz</b> .....	<b>271</b>
<b>H.1.</b>	<b>Ansprüche des Unternehmens</b> ( <i>Axel Anderl</i> ) .....	<b>273</b>
H.1.1.	Problemaufriss .....	273
H.1.2.	Ansprüche gegen den Täter .....	275
H.1.3.	Ansprüche gegen Geschäftsleiter .....	275
H.1.4.	Ansprüche gegen Mitarbeiter .....	275
H.1.5.	Ansprüche gegen Dienstleister .....	276
H.1.6.	Exkurs: Ansprüche gegen Dienstleister, die Ziel eines Cyberangriffs waren .....	276
H.1.7.	Fazit .....	276
<b>H.2.</b>	<b>Ansprüche von Gesellschaftern und Vertragspartnern</b> ( <i>Kathrin Weber</i> ) .....	<b>278</b>
H.2.1.	Ansprüche gegen Geschäftsleiter – Business Judgement Rule .....	278
H.2.2.	Ansprüche gegen den Aufsichtsrat .....	280
H.2.3.	Ansprüche von Gesellschaftern und Vertragspartnern .....	280
H.2.3.1.	Allgemeines .....	280
H.2.3.2.	Ansprüche von Gesellschaftern .....	281
H.2.3.3.	Ansprüche von Vertragspartnern .....	281
H.2.4.	Exkurs: Pflicht zur Geltendmachung von Schadenersatzansprüchen im Konzern .....	282

H.3.	<b>Ansprüche Betroffener</b> ( <i>Axel Anderl/Nino Tlapak</i> ) .....	284
H.3.1.	Problemaufriss – rechtliche Grundlagen .....	284
H.3.2.	Keine Erheblichkeitsschwelle, aber viele offene Fragen .....	285
H.3.3.	Zahlreiche offene Fragen auf Unionsebene .....	286
I.	<b>Cybersecurity im Kontext von M&amp;A-Transaktionen</b> .....	289
I.1.	<b>Exkurs: Cybersecurity im Kontext von M&amp;A-Transaktionen</b> ( <i>Christian Ritschka/Patricia Backhausen</i> ) .....	291
I.1.1.	Einleitung .....	291
I.1.2.	Due Diligence zu Cybersecurity .....	291
I.1.2.1.	Rechtliche Due Diligence .....	292
I.1.2.2.	Technische Due Diligence .....	293
I.1.3.	Regelungen im Kaufvertrag .....	293
I.1.3.1.	Berücksichtigung der Due Diligence-Ergebnisse .....	293
I.1.3.2.	Gewährleistungszusagen (Representations and Warranties) .....	294
I.1.3.3.	Gewährleistungsversicherung .....	295
I.1.3.4.	Risiko im Zeitraum zwischen Signing und Closing .....	296
I.1.3.5.	Maßnahmen nach dem Closing .....	297
I.1.3.5.1.	Integration der IT-Systeme .....	297
I.1.3.5.2.	Erhöhung der Cybersecurity .....	297
I.1.3.5.3.	Cyberversicherung .....	298
J.	<b>Checkliste für den Anlassfall</b> .....	299
	<b>Stichwortverzeichnis</b> .....	301