

# Inhaltsverzeichnis

|                                                                                            |           |
|--------------------------------------------------------------------------------------------|-----------|
| <b>1 Cyber-Krisen wie aus dem Lehrbuch .....</b>                                           | <b>1</b>  |
| 1.1 Cyber Crisis re-invented: Sony Pictures Entertainment .....                            | 1         |
| 1.2 Dramaturgie unzureichend gemanagter Cyber-Krisen .....                                 | 3         |
| <b>2 Das Wichtigste zuerst: Der Faktor Mensch beim Management von (Cyber-)Krisen .....</b> | <b>9</b>  |
| 2.1 Entscheidungen oder die Essenz von Krisenbewältigung .....                             | 9         |
| 2.2 Bewertungen, Verhaltensmuster und Stress.....                                          | 11        |
| 2.2.1 Wie Menschen Situationen wahrnehmen und bewerten .....                               | 11        |
| 2.2.2 Verhaltensmuster und wie sie sich äußern .....                                       | 12        |
| 2.2.3 Stress und wie er entsteht.....                                                      | 13        |
| 2.2.4 Stress und was wir dagegen tun können .....                                          | 15        |
| 2.3 Anforderungen an die Mitglieder der Krisenorganisation.....                            | 18        |
| <b>3 Cyber Crisis Response.....</b>                                                        | <b>21</b> |
| 3.1 Alarmierung, Eskalation und Information.....                                           | 21        |
| 3.1.1 Grundsätze und Erfolgsfaktoren .....                                                 | 21        |
| 3.1.2 Verantwortlichkeiten und Abläufe .....                                               | 24        |
| 3.1.3 Erreichbarkeits- oder Bereitschaftsregelung .....                                    | 27        |
| 3.1.4 Informationskanäle oder: Alarmierungstools vs. Telefonkaskaden .....                 | 28        |
| 3.1.5 Eskalationskriterien vs. Verantwortungsfreude und Fehlerkultur .....                 | 31        |
| 3.2 Reaktion auf strategischer Ebene .....                                                 | 32        |
| 3.2.1 Die Weichen stellen: Initialisierung der Krisenstabsarbeit .....                     | 32        |
| 3.2.1.1 Bevor wir zur Tat schreiten: Die „Du-kommst aus-dem-Gefängnis-Frei-Karte“ .....    | 35        |
| 3.2.1.2 Erste Lagefeststellung oder: Was ist überhaupt los? .....                          | 38        |
| 3.2.1.3 Betroffene Stakeholder oder: Mit wem müssen wir rechnen? .....                     | 40        |
| 3.2.1.4 Ausnahmsweise mal negativ denken: Was wäre wenn? .....                             | 47        |

|          |                                                                                     |            |
|----------|-------------------------------------------------------------------------------------|------------|
| 3.2.1.5  | Von der Feststellung zur Beurteilung: Ziel, Ziel und nochmals Ziel .....            | 51         |
| 3.2.1.6  | Die formale Feststellung des Krisenfalls: Houston, wir haben ein Problem .....      | 56         |
| 3.2.2    | Cyber-Krisen strukturiert bewältigen:<br>Krisenbewältigungsprozess.....             | 57         |
| 3.2.2.1  | Variante A: Führungsprozess .....                                                   | 58         |
| 3.2.2.2  | Variante B: FOR-DEC .....                                                           | 65         |
| 3.2.3    | Krisenkommunikation.....                                                            | 66         |
| 3.2.3.1  | Faustregeln für die Krisenkommunikation .....                                       | 67         |
| 3.2.3.2  | Ausgangspunkt: Bedürfnisse und Nöte der Stakeholder in Cyber-Krisen .....           | 68         |
| 3.2.3.3  | W-Fragen der Krisenkommunikation .....                                              | 71         |
| 3.2.3.4  | Von Bloggern, YouTubern und Journalisten:<br>Grenzen des Presserechts .....         | 76         |
| 3.2.4    | Aus der Praxis: Strategien in akuten Cyber-Krisen .....                             | 78         |
| 3.2.4.1  | Victim Care über alles .....                                                        | 78         |
| 3.2.4.2  | Wir sind selbst auch Opfer! .....                                                   | 80         |
| 3.2.4.3  | Angriff ist die beste Verteidigung.....                                             | 82         |
| 3.2.4.4  | Die Karten auf den Tisch legen vs.<br>Kommunikationsverweigerung.....               | 84         |
| 3.2.4.5  | Den Kopf aus der Schlinge ziehen oder aus der<br>Schusslinie verschwinden.....      | 85         |
| 3.2.4.6  | Einen Sündenbock gegen eine Identifikationsfigur<br>tauschen .....                  | 87         |
| 3.2.4.7  | Wenn wir erpresst werden .....                                                      | 88         |
| 3.3      | Reaktion auf taktisch-operativer Ebene.....                                         | 90         |
| 3.3.1    | Die Show muss weitergehen oder: Wiederanlauf von<br>Prozessen und IT-Systemen ..... | 90         |
| 3.3.1.1  | Wiederanlauf: kritische (Geschäfts-)Prozesse .....                                  | 91         |
| 3.3.1.2  | Wiederanlauf: IT-Systeme und Daten.....                                             | 93         |
| 3.3.2    | Cybersecurity Incident Response.....                                                | 98         |
| 3.3.2.1  | Ablauf der Cybersecurity Incident Response .....                                    | 99         |
| 3.3.2.2  | Faustregeln bei der Cybersecurity Incident Response.....                            | 101        |
| <b>4</b> | <b>Cyber Crisis Preparation .....</b>                                               | <b>103</b> |
| 4.1      | Nichts für die Linie oder: Notfall- und Krisenorganisation.....                     | 103        |
| 4.1.1    | Die Rettungsmannschaft oder: der Krisenstab.....                                    | 106        |
| 4.1.1.1  | Der organisatorische Rahmen des Krisenstabs.....                                    | 108        |
| 4.1.1.2  | Zusammensetzung des Krisenstabs .....                                               | 109        |
| 4.1.1.3  | Gretchenfrage: Wer besser (nicht) Mitglied des<br>Krisenstabs sein sollte .....     | 114        |

---

|          |                                                                                  |            |
|----------|----------------------------------------------------------------------------------|------------|
| 4.1.2    | Lagezentrum .....                                                                | 115        |
| 4.1.3    | Kommunikationsstab .....                                                         | 116        |
| 4.1.4    | Notfallgremien der taktisch-operativen Ebene.....                                | 118        |
| 4.2      | Infrastrukturen und Hilfsmittel.....                                             | 119        |
| 4.2.1    | Krisenhandbuch .....                                                             | 119        |
| 4.2.2    | Krisenstabsraum.....                                                             | 123        |
| 4.2.3    | Templates, Poster und Vorlagen .....                                             | 125        |
| 4.2.4    | IT-gestützte Krisenmanagement-Tools .....                                        | 125        |
| 4.2.5    | Alarmierungstools.....                                                           | 127        |
| 4.2.6    | Governance-Suiten für BCM, IRBC und ISM.....                                     | 128        |
| 4.2.7    | IDS und SIEM-Tools .....                                                         | 129        |
| 4.3      | Logistik sichert Durchhaltefähigkeit .....                                       | 130        |
| 4.4      | Vorbereitung der Krisenkommunikation .....                                       | 132        |
| 4.4.1    | Kommunikationshilfen.....                                                        | 133        |
| 4.5      | Es ist noch kein Meister vom Himmel gefallen: Trainings und Übungen.....         | 138        |
| 4.5.1    | Formate .....                                                                    | 138        |
| 4.5.2    | Trainingsprogramm.....                                                           | 140        |
| 4.6      | Voraussetzungen für die Fortsetzung des Geschäftsbetriebs schaffen.....          | 143        |
| 4.6.1    | Notbetrieb der (Geschäfts-)Prozesse vorbereiten .....                            | 143        |
| 4.6.1.1  | Kritikalitäten und Ressourcen .....                                              | 143        |
| 4.6.1.2  | Geschäftsfortführungspläne.....                                                  | 146        |
| 4.6.2    | Wiederanlauf der IT-Systeme ermöglichen.....                                     | 147        |
| 4.6.2.1  | Technische Lösungen .....                                                        | 147        |
| 4.6.2.2  | Organisatorische Vorbereitungen: Wiederanlaufpläne<br>und Restore-Konzepte ..... | 149        |
| 4.6.3    | Rahmenbedingungen für Cybersecurity Incident Response<br>schaffen .....          | 151        |
| 4.7      | Was funktioniert und was nicht: Tests .....                                      | 151        |
| 4.8      | Versicherung von Cyberrisiken .....                                              | 155        |
| <b>5</b> | <b>Cyber Crisis Prevention .....</b>                                             | <b>159</b> |
| 5.1      | Analogie zum Einsteig .....                                                      | 159        |
| 5.2      | Gefahr erkannt, Gefahr gebannt: Awareness .....                                  | 161        |
| 5.3      | Frühwarnsystem: Risikokommunikation, Stakeholder- und<br>Issuemanagement .....   | 162        |
| 5.3.1    | Stakeholder- und Issuemanagement.....                                            | 164        |
| 5.3.2    | Risikokommunikation (und ihre Tücken) .....                                      | 166        |
| 5.4      | Nicht sexy, aber fundamental: Asset Management und Strukturanalyse.....          | 169        |
| 5.5      | Unverzichtbar: Information und IT Security Management .....                      | 172        |
| 5.5.1    | ISM im Schnelldurchlauf.....                                                     | 173        |
| 5.5.2    | Handlungsfelder für Informationssicherheit.....                                  | 174        |

---

|          |                                                                            |            |
|----------|----------------------------------------------------------------------------|------------|
| 5.6      | Fokus Verfügbarkeit: Continuity Management.....                            | 175        |
| 5.6.1    | Business Continuity Management .....                                       | 175        |
| 5.6.2    | IRBC/IT Service Continuity Management .....                                | 177        |
| 5.7      | Cyber Risk Management .....                                                | 180        |
| 5.7.1    | Vorarbeiten .....                                                          | 181        |
| 5.7.2    | Risk Assessment.....                                                       | 182        |
| 5.7.2.1  | Risikoidentifikation .....                                                 | 182        |
| 5.7.2.2  | Risikoanalyse.....                                                         | 184        |
| 5.7.2.3  | Risikobewertung .....                                                      | 185        |
| 5.7.3    | Risikobehandlung .....                                                     | 186        |
| 5.7.4    | Akzeptanz von (Rest-)Risiken .....                                         | 188        |
| 5.8      | Unsere Cyber Resilience und wie es um sie bestellt ist: Audits.....        | 189        |
| <b>6</b> | <b>Post Crisis Care – Krisennachsorge und -nachbereitung .....</b>         | <b>193</b> |
| 6.1      | Der Blick nach außen: Reparieren der Stakeholderbeziehungen .....          | 193        |
| 6.2      | Der Blick nach innen: Menschen, Abläufe und Technik .....                  | 194        |
| 6.2.1    | Faktor Mensch .....                                                        | 195        |
| 6.2.2    | Alarmierung und Eskalation .....                                           | 196        |
| 6.2.3    | Zusammenspiel der Ebenen der Notfall- und Krisenorganisation .....         | 196        |
| 6.2.4    | Strategische Ebene .....                                                   | 197        |
| 6.2.5    | Operative Ebene: BCM und IRBC.....                                         | 198        |
| 6.2.6    | Taktische Ebene: CSIRT und Cybersecurity Incident Resonse .....            | 199        |
| 6.2.7    | Krisenkommunikation.....                                                   | 200        |
| <b>7</b> | <b>Auf einen Blick: Sieben Todsünden des Cyber Crisis Managements.....</b> | <b>201</b> |
|          | <b>Zum Weiterlesen.....</b>                                                | <b>205</b> |
|          | <b>Abkürzungen und Glossar .....</b>                                       | <b>211</b> |