Holger Kaschner

Cyber Crisis Management

Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation

2. Auflage

Springer Vieweg

Cyber Crisis Management

Holger Kaschner

Cyber Crisis Management

Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation

2. Auflage

Springer Vieweg

Holger Kaschner
Berlin, Deutschland

ISBN 978-3-658-43464-9 ISBN 978-3-658-43465-6 (eBook)
https://doi.org/10.1007/978-3-658-43465-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Das Papier dieses Produkts ist recycelbar.

An wen sich dieses Buch richtet, was es behandelt und wie es aufgebaut ist

Zielgruppe
Dieses Buch ist für Mitglieder von Krisenstäben gedacht, die Experten und/oder Führungskräfte in ihrem Fachgebiet, aber mit Krisenmanagement und Cyberrisiken nur am Rande vertraut sind. Ebenso ist es für CISOs gedacht, die ihren Aufgabenbereich besser mit dem organisationsweiten Notfall- und Krisenmanagement verzahnen wollen.

Krisenstab, Notfallorganisation und IT-Fachebene
Während die IT-Fachebene (oder ein Dienstleister, an den die IT ausgelagert ist) bei einer Cyber-Krise das technische Trouble-Shooting (oft als (Major) Incident Management bezeichnet) übernimmt, müssen Krisenstäbe das große Ganze im Blick behalten, d. h. die Ziele und die wesentlichen Stakeholder der Organisation sowie deren Erwartungen an die Organisation. Die Brücke zwischen dem Krisenstab auf der strategischen Ebene und der operativen IT-Fachebene bildet als taktische Ebene die Notfallorganisation, die den Notbetrieb der kritischen (Geschäfts-)Prozesse sicherstellt. Das Zusammenspiel der drei Ebenen ist ein wesentlicher Erfolgsfaktor für professionelles und erfolgreiches Krisenmanagement.

Was ist eigentlich eine Krise?
Unter einer Krise verstehen wir gemäß ISO 22361:2022 „anormale oder außergewöhnliche Ereignisse oder Situationen, die eine Organisation oder Gemeinschaft bedrohen und eine strategische, anpassungsfähige und rechtzeitige Reaktion erfordern, um ihre Lebensfähigkeit und Integrität zu bewahren“. Wenn wir dem altgriechischen Wortstamm folgen, erhalten wir obendrein die Eigenschaft eines „Wendepunkts“.

Krisenmanagement

- dient dem Schutz von (im-)materiellen Gütern (zuallererst Menschen);
- ist nicht im Detail planbar;
- muss auf unterschiedlichen Ebenen erfolgen;
- muss auch Themen wie Stakeholder- und Issuemanagement, Geschäftsfortführung, Incident Response etc. umfassen.

Damit orientieren wir uns an den Standards BS ISO 22361 und BfV/BSI/ASW 2000-3.

...und eine Cyber-Krise?
Eine Cyber-Krise ist demzufolge eine Krise, bei denen IT-Systeme und auf ihnen verarbeitete Daten eine zentrale Rolle spielen. Dabei geht es um die klassischen Schutzziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie Authentizität der Kommunikationsteilnehmer und Inhalte der Kommunikation (technisch wie auch organisatorisch).

Wir haben es also immer dann mit einer Cyber-Krise zu tun, wenn aus der Verletzung der Schutzziele reale Gefahren für Leib und Leben von Menschen beziehungsweise die strategischen Ziele, die Reputation oder die Überlebensfähigkeit unserer Organisation entstehen (können).

Nebenbei bemerkt: Das Management von Krisen aller Art und somit auch von Cyber-Krisen ist Bestandteil der Risikovorsorge, zu der Vorstände (§§ 91, 93 AktG) und Geschäftsführer (§ 43 Abs. 1 GmbHG) verpflichtet sind.

Analogie: Verkehrssicherheit und Cybersecurity
Cybersecurity (oder auf Neudeutsch: Cyber-Sicherheit) wird oftmals mit IT-Sicherheit gleichgesetzt und auf letztere reduziert. Wer auch nur ein bisschen Ahnung hat kann dann nur mit dem Kopf schütteln. Cybersecurity und IT-Sicherheit gleichzusetzen ist in etwa so, als wenn wir Verkehrssicherheit auf die ordentliche Bereifung eines Fahrzeugs reduzieren.

Verkehrssicherheit braucht Regeln – die Straßenverkehrsordnung. Cybersecurity braucht ebenfalls Regeln – u. a. das BSI-Gesetz, NIS2, DORA, VAIT, MaRisk und wie sie alle heißen. Fahrer und Autos werden nicht einfach so auf die Menschheit losgelassen – ohne Hauptuntersuchung und Zulassung sowie Führerscheinprüfung geht es nicht. Tests und Audits sind das Äquivalent im Cybersecurity-Kontext. Damit wir unser Auto angemessen bewegen (können), müssen wir zu Beginn unserer Autofahrerkarriere Fahrstunden nehmen und auch später im Straßenverkehr kontinuierlich aufmerksam bleiben. Das ist nichts anderes als der Ruf nach Trainings- und Awareness-Maßnahmen mit Blick auf Cyberrisiken. Stichwort Risiken: Im Straßenverkehr berücksichtigen wir bei unserem Fahrverhalten u. a. unser eigenes Geschick, die Witterungsverhältnisse, den Zustand unseres Fahrzeugs sowie vor allem, ob wir allein unterwegs sind oder mit uns lieben Passagieren in einer hektischen und gefährlichen Umgebung. Nichts anderes tun wir mit Blick auf Cybersecurity, wenn wir eine Informationssicherheitsstrategie aufsetzen und ein Cyber-Risk-Management Programm betreiben. Was in unserer Analogie die Passagiere bzw. die kostbare Fracht sind, sind im Informationssicherheitskontext die Informationen, vulgo Daten. Und die besonders wichtigen, die wir hüten wollen wie unseren Augapfel, das sind die Crown Jewels.

Keine Frage, ein sicher konstruiertes Fahrzeug mit einer vollständigen Übersicht aller verbauten Teile und ihrer Spezifikation ist elementar. Genau wie die Informationssicherheitsarchitektur als Kern des Informations-, IT-Sicherheits- und Asset Managements.

Es ist aber eben nicht alles. Wenn wir uns im Straßenverkehr bewegen wollen, müssen wir auch immer einen Plan B in der Tasche haben, falls unser Fahrzeug mal liegen bleibt oder – Gott bewahre – wir einen Unfall gebaut haben. Uns aus dem Fahrzeug befreien, Unfallstelle absichern, erste Hilfe leisten, Rettungskräfte und Polizei rufen, Abschleppwagen und anschließende Reparatur organisieren und mit Gaffern am Unfallort umgehen. Und was bedeutet das für die Cybersecurity-Analogie? Nun, wir brauchen eine wirksame Incident Response sowie ein wirksames Stakeholder- und Issuemanagement, Business und IT Service Continuity Management bzw. ICT readiness for business continuity und nicht zuletzt Krisenmanagement (!).

Zusammen ist man weniger allein

Cybersecurity herzustellen und aufrechtzuerhalten ist genau wie das Management von Cyber-Krisen etwas, das nur im Verbund gelingt. Aus einer Cybersecurity-Perspektive sitzen wir alle in einem Boot, auch dank wechselseitiger Abhängigkeiten (Stichwort: Lieferketze). Daher ist regelmäßiger Austausch mit anderen Unternehmen nicht zu unterschätzen. Denn niemand kann alles wissen. Um in der Verkehrssicherheitsanalogie bleiben: Es ist illusorisch, an uns selbst den Anspruch zu formulieren, unser Fahrzeug komplett selbst zu entwickeln, bei einem Unfall sämtliche Hilfeleistungen inklusive Abschleppen und anschließend auch noch die Reparatur selbst zu bewerkstelligen zu wollen. Bei all dem können und müssen uns Partner helfen, zu denen wir hoffentlich eine Vertrauensbeziehung aufgebaut haben. Wie auch im Privatleben können, werden und müssen diese Partner uns auch mal den Spiegel vorhalten und unliebsame Wahrheiten aussprechen. Das wird nicht immer angenehm sein. Aber genau deshalb sollten wir ihnen zuhören.

Psychologie

Egal, um welche Art von Krise es sich handelt: Für die Beteiligten und Betroffenen ist es eine Ausnahmesituation, die sie aus ihrer Komfortzone herausholt und unter Zeit- und Erwartungsdruck setzt. Anders ausgedrückt: Krisen bedeuten Stress und Stress führt häufig dazu, dass Menschen anders reagieren, als sie es normalerweise täten. Daher enthält das Buch Hintergründe zu den Verhaltensweisen, die Menschen unter Stress an den Tag legen – und natürlich Tipps zum Umgang mit Stresssituationen.

Dies behandeln wir in Kap. 2 „Das Wichtigste zuerst: Der Faktor Mensch beim Management von (Cyber-)Krisen“.

Bewältigung von (Cyber-)Krisen

Um in einer Cyber-Krise Krisenstabsarbeit, Krisenkommunikation, Notfallmanagement (IT- und prozessseitig) sowie technische Gegenmaßnahmen aus einem Guss liefern zu können, müssen nicht nur die Krisenstabsmitglieder verstehen, wie Cyber-Krisen

- entstehen,
- typischerweise verlaufen und
- bewältigt werden

können. Sondern damit die Bewältigung personenunabhängig zum Erfolg führt, muss auch die Krisenbewältigung schnell eingeleitet werden und anhand eines strukturierten Prozesses erfolgen. Dies müssen alle Mitglieder einer Notfall- und Krisenorganisation im Schlaf beherrschen.

Die praktische Krisenbewältigung kann noch so gut sein – ohne eine effektive begleitende Kommunikation verliert sie viel von ihrer Wirkung. Oftmals sind gerade in den Anfangsstunden einer Krise noch keine Fortschritte erkennbar. Gerade dann (aber nicht nur dann) kommt der Krisenkommunikation zentrale Bedeutung zu. Bei der Krisenbewältigung müssen wir unterschiedliche Ebenen berücksichtigen. Während die meisten Krisenmanagementbücher nur die strategische Ebene behandeln, richten wir den Blick auch auf die taktisch-operativen Elemente – ohne diese sind sämtliche strategischen Ansätze nur Schall und Rauch.

Die Krisenbewältigung – operativ und kommunikativ, strategisch und taktisch-operativ – behandeln wir im Kap. 3 „Cyber Crisis Response“.

Vorbereitung auf (Cyber-)Krisen

Damit die unterschiedlichen Ebenen und Elemente der Krisenbewältigung ihre Wirkung voll entfalten können, müssen wir Vorkehrungen treffen. Dazu zählt insbesondere, eine schlagkräftige Notfall- und Krisenorganisation aufzubauen und ihr die nötigen Hilfsmittel zur Bewältigung von (Cyber-)Krisen an die Hand zu geben.

Dabei helfen folgende Management-Disziplinen und -Systeme:

- Business Continuity Management (BCM)
- ICT readiness for business continuity (IRBC) bzw. IT Service Continuity Management (ITSCM)
- Information Security Incident Management

Diese und weitere Maßnahmen stellen wir im Kap. 4 „Cyber Crisis Preparation“ vor.

Vorbeugung gegen (Cyber-)Krisen

Aber nicht nur das, denn: Mit ein wenig Glück (und vor allem den richtigen Präventionsmaßnahmen) können Organisationen durchaus verhindern, dass aus einem Cyber-Incident eine ausgewachsene Krise wird.

Dabei helfen insbesondere folgende Bausteine:

- IT-Sicherheitsarchitektur
- Cybersecurity Management
- Information Risk Management (IRM)
- Information Security Management (ISM)

Dies schauen wir uns im Kap. 5 „Cyber Crisis Prevention“ näher an.

Grundlagen zum Management von Cyber-Sicherheit und Cyber-Krisen
All das setzt auf einigen Grundlagen auf, ohne die wir keine der anderen Phasen des Cyber Crisis Management vernünftig angehen können. Diese Grundlagen sind eine Informationssicherheitsstrategie, die unsere präventiven du reaktiven Fähigkeiten mit Schwerpunktsetzung auf Crown Jewels definiert, ein hoffentlich profundes Verständnis von Kritikalitäten und Abhängigkeiten sowie die Fähigkeit, externe und interne Stakeholder so zu integrieren, dass sie alle an einem Strang ziehen (und das vorzugsweise in die gleiche Richtung).

Dies vertieft Kap. 6 „Cyber Crisis (& Security) Grundlagen".

Aufräumarbeiten nach (Cyber-)Krisen
Nach der Krise ist vor der Krise (und umgekehrt). Wenn sich die Wogen wieder geglättet haben und sich die Situation normalisiert, stehen wichtige Nacharbeiten an. Meist beschädigt eine Krise die Beziehungen einer Organisation zu ihren Stakeholdern. Diese Beziehungen gilt es zu reparieren. Bei Cyber-Krisen kommt oft noch eine technisch-organisatorische Dimension hinzu. Bei all dem müssen wir den Blick gleichermaßen in unsere Organisation hinein wie auch nach außen richten. Derartige Aspekte sind Gegenstand des Kap. 7 „Post Crisis Care – Krisennachsorge und -nachbereitung".

Schwerpunkt: Crown Jewels
Da wir beim Management von Krisen nicht jede Facette gleichermaßen angehen können, sollten wir einen (!) Schwerpunkt setzen (mehrere Schwerpunkte kann es nicht geben, sondern wäre eine Schwerfläche).

Als Schwerpunkt – sprich, Ziel – hat sich der Schutz der sogenannten Crown Jewels bewährt.

Ausgangspunkt sollte immer die Unternehmensstrategie sein, aus der wir die Crown Jewels ableiten sowie grundlegende Fähigkeiten zu ihrem Schutz definieren können. Die Fähigkeiten wiederum lassen sich ihrerseits in Anforderungen und die Anforderungen letztlich in Unternehmens- und IT-Architekturen sowie damit verbundene Maßnahmen übersetzen.

Prototypische Crown Jewels auf strategischer Ebene sind:

- Leib und Leben von Menschen;
- Umwelt und Tierwohl;
- kritische Geschäftsbereiche und Wertschöpfungsketten;
- Beziehungen zu den wichtigsten Stakeholdern.

Diese Schwerpunktsetzung greift in allen Phasen: Response, Preparation, Prevention und Post Crisis Care. Daher werden uns die Crown Jewels im gesamten Buch wieder und wieder begegnen – inklusive praxiserprobter Lösungsvorschläge, wie wir den Schutz auch tatsächlich operationalisieren können.

Disclaimer: Governance-Systeme und (ISO-)Standards

Wer sich bereits mit Governance-Systemen und (ISO-)Standards beschäftigt hat, wird in diesem Buch viele Elemente wiedererkennen, insbesondere aus den Standards ISO 22301, ISO 27001, ISO 27002, ISO 27005, ISO 27031, ISO 27032, ISO 27035, ISO 31000 sowie BSI 200-x und ITIL® v4.

Die Elemente sind jedoch nicht streng nach dem jeweiligen Governance-System bzw. (ISO-)Standard sortiert. Stattdessen sind sie über das ganze Buch verteilt, damit deutlich wird, welchen konkreten Beitrag sie zum Management von Cyber-Krisen leisten können. Ähnliches gilt für Hinweise aus den Krisenmanagementstandards ISO 22361, BfV/BSI/ASW 2000-3 sowie dem mittlerweile zugunsten des ISO-Standards zurückgezogenen BS 11200.

Aufbau des Buchs

Das alles (und noch ein bisschen mehr) erklärt dieses Buch und gibt Tipps zur praktischen Umsetzung der einzelnen Elemente. Dazu müssen wir aber nicht ein Kapitel nach dem anderen und schon gar nicht das ganze Buch lesen. Vielmehr ist das Buch so aufgebaut, dass jedes Kapitel isoliert gelesen werden kann. Wo angebracht, finden sich Hinweise auf inhaltlich eng verbundene Kapitel. Auf diese Weise kann sich jeder Leser gezielt auf die Inhalte konzentrieren, die für ihn von Interesse sind.

Diese Flexibilität hat jedoch ihren Preis. Ohne kleinere Redundanzen geht es nicht, ansonsten bestünde das Buch aus nichts anderem als wechselseitigen Querverweisen. Sollte das Verhältnis von Redundanzen zu Verweisen kein ausgewogenes sein, trägt die Verantwortung dafür allein der Autor.

Holger Kaschner

Inhaltsverzeichnis

1 Cyber-Krisen wie aus dem Lehrbuch 1
1.1 Cyber Crisis re-invented: Sony Pictures Entertainment. 1
1.2 Dramaturgie unzureichend gemanagter Cyber-Krisen 3

2 Menschen und andere Crown Jewels 9
2.1 Crown Jewels – oder: Wie wir Schwerpunkte setzen 9
2.2 Faktor Mensch 11
2.2.1 Entscheidungen oder die Essenz von Krisenbewältigung 11
2.2.2 Bewertungen, Verhaltensmuster und Stress 13
2.2.2.1 Wie Menschen Situationen wahrnehmen und bewerten 13
2.2.2.2 Verhaltensmuster und wie sie sich äußern. 14
2.2.2.3 Stress und wie er entsteht 15
2.2.2.4 Stress und was wir dagegen tun können 17
2.2.3 Anforderungen an die Mitglieder der Krisenorganisation 20

3 Cyber Crisis Response 23
3.1 Executive Summary: Crown-Jewels-basierte Cyber Crisis Response 23
3.2 Alarmierung, Eskalation und Benachrichtigung 26
3.2.1 Grundsätze und Erfolgsfaktoren. 26
3.2.2 Verantwortlichkeiten und Abläufe 30
3.2.3 Erreichbarkeits- oder Bereitschaftsregelung 33
3.2.4 Informationskanäle oder: Alarmierungstools vs. Telefonkaskaden. 34
3.2.5 Eskalationskriterien vs. Verantwortungsfreude und Fehlerkultur 37
3.3 Reaktion auf strategischer Ebene. 39
3.3.1 Die Weichen stellen: Initialisierung der Krisenstabsarbeit. 39
3.3.1.1 Bevor wir zur Tat schreiten: Die „Du-kommst aus-dem-Gefängnis-frei-Karte“. 40
3.3.1.2 Erste Lagefeststellung oder: Was ist überhaupt los? 44

3.3.1.3 Betroffene Stakeholder oder: Mit wem müssen wir rechnen? 46
3.3.1.4 Ausnahmsweise mal negativ denken: Was wäre wenn? 54
3.3.1.5 Von der Feststellung zur Beurteilung: Ziel, Ziel und nochmals Ziel. 58
3.3.1.6 Die formale Feststellung des Krisenfalls: Houston, wir haben ein Problem 63
3.3.2 Cyber-Krisen strukturiert bewältigen: Krisenbewältigungsprozess 64
3.3.2.1 Die Qual der Wahl: Nach welchem Schema wollen wir arbeiten? 65
3.3.2.2 Deep Dive: Bewältigungsprozess auf strategischer Ebene 66
3.3.2.2.1 Lagebewertung: Wo drückt der Schuh am meisten? 68
3.3.2.2.2 Handlungsfelder und -optionen: Was tun, sprach Zeus? 69
3.3.2.2.3 Entscheidung und Delegation: Nicht reden, handeln! 70
3.3.2.2.4 Lagefeststellung/Überprüfung: Wirkt es schon? 72
3.3.3 Krisenkommunikation 74
3.3.3.1 Faustregeln für die Krisenkommunikation 75
3.3.3.2 Ausgangspunkt: Bedürfnisse und Nöte der Stakeholder in Cyber-Krisen 76
3.3.3.3 W-Fragen der Krisenkommunikation 79
3.3.3.3.1 Wer kommuniziert mit wem? 79
3.3.3.3.2 Was kommunizieren wir? 80
3.3.3.3.3 Wie kommunizieren wir (hoffentlich)? 82
3.3.3.3.4 Wann kommunizieren wir? 84
3.3.3.4 Von Bloggern, YouTubern und Journalisten: Grenzen des Presserechts 85
3.3.4 Aus der Praxis: Strategien und Taktiken in akuten Cyber-Krisen 86
3.3.4.1 Victim Care über alles 87
3.3.4.2 Wir sind selbst auch Opfer! 89
3.3.4.3 Angriff ist die beste Verteidigung 92
3.3.4.4 Die Karten auf den Tisch legen vs. Kommunikationsverweigerung 94
3.3.4.5 Den Kopf aus der Schlinge ziehen oder aus der Schusslinie verschwinden 95

3.3.4.6 Einen Sündenbock gegen eine Identifikationsfigur tauschen . . . 97
3.3.4.7 Wenn wir erpresst werden . . . 98
3.3.4.8 Die juristische Keule schwingen . . . 100
3.4 Reaktion auf taktisch-operativer Ebene . . . 102
3.4.1 Die Show muss weitergehen oder: Wiederanlauf von Prozessen und IT-Systemen . . . 102
3.4.1.1 Wiederanlauf: kritische (Geschäfts-)Prozesse . . . 104
3.4.1.2 Wiederanlauf: IT-Systeme und Daten . . . 106
3.4.2 Cybersecurity Incident Response . . . 112
3.4.2.1 Cybersecurity Incident Response . . . 114
3.4.2.2 Faustregeln bei der Cybersecurity Incident Response . . . 116

4 Cyber Crisis Preparation . . . 119
4.1 Executive Summary: Crown Jewels basierte Cyber Crisis Preparation . . . 119
4.2 Nichts für die Linie oder: Notfall- und Krisenorganisation . . . 123
4.2.1 Die Rettungsmannschaft oder: der Krisenstab . . . 124
4.2.1.1 Der organisatorische Rahmen des Krisenstabs . . . 126
4.2.1.2 Zusammensetzung des Krisenstabs . . . 128
4.2.1.3 Gretchenfrage: Wer (besser nicht) Mitglied des Krisentabs sein sollte . . . 132
4.2.2 Lagezentrum . . . 134
4.2.3 Kommunikationsstab . . . 135
4.2.4 Notfallgremien der taktisch-operativen Ebene . . . 137
4.3 Hilfsmittel . . . 139
4.3.1 Krisenhandbuch . . . 139
4.3.2 Krisenstabsraum . . . 143
4.3.3 Templates, Poster und Vorlagen . . . 145
4.3.4 IT-gestützte Krisenmanagement-Tools . . . 146
4.3.5 Alarmierungstools . . . 149
4.3.6 Governance-Suiten für BCM, IRBC und ISM . . . 150
4.3.7 Tools zur Detektion von und Reaktion auf Angriffe . . . 151
4.4 Logistik sichert Durchhaltefähigkeit . . . 153
4.5 Vorbereitung der Krisenkommunikation . . . 155
4.5.1 Rechtzeitig die Hausaufgaben machen . . . 155
4.5.2 Kommunikationshilfen . . . 157
4.6 Es ist noch kein Meister vom Himmel gefallen: Trainings und Übungen . . . 162
4.6.1 Formate . . . 162
4.6.2 Trainingsprogramm . . . 164
4.7 Voraussetzungen für die Fortsetzung des Geschäftsbetriebs schaffen . . . 167

4.7.1 Notbetrieb der (Geschäfts-)Prozesse vorbereiten: Geschäftsfortführungspläne . . . 169
4.7.2 Wiederanlauf der IT-Systeme ermöglichen . . . 171
4.7.2.1 Technische Lösungen . . . 171
4.7.2.2 Organisatorische Vorbereitungen: Playbooks, Wiederanlaufpläne und Restore-Konzepte . . . 172
4.7.3 Rahmenbedingungen für Cybersecurity Incident Response schaffen . . . 176
4.8 Was funktioniert und was nicht: Tests . . . 176
4.9 Versicherung von Cyberrisiken . . . 181

5 Cyber Crisis Prevention . . . 185
5.1 Executive Summary: Crown Jewels basierte Cyber Crisis Prevention . . . 185
5.2 Bevor wir losfahren: IT-Sicherheitsarchitektur und drei Prinzipien . . . 187
5.2.1 (Privileged) Access Management . . . 188
5.2.2 Weitere Pfeiler der IT-Sicherheitsarchitektur . . . 189
5.3 (Früh-)Warnsystem: Gefahr erkannt, Gefahr gebannt . . . 192
5.3.1 Issue Management . . . 192
5.3.2 Awareness . . . 193
5.3.3 Threat Intelligence . . . 195
5.3.4 Logging, Monitoring, Alerting . . . 198
5.4 Unverzichtbar: Information und IT Security Management . . . 200
5.5 Cyber Risk Management . . . 201
5.5.1 Vorarbeiten . . . 202
5.5.2 Risk Assessment . . . 203
5.5.2.1 Risikoidentifikation . . . 203
5.5.2.2 Risikoanalyse . . . 205
5.5.2.3 Risikobewertung . . . 207
5.5.3 Risikobehandlung . . . 208
5.5.4 Akzeptanz von (Rest-)Risiken . . . 210
5.6 Unsere Cyber Resilience und wie es um sie bestellt ist: Audits und Assessments . . . 211

6 Cyber Crisis (& Security) Grundlagen . . . 215
6.1 Executive Summary: Crown Jewels . . . 215
6.2 Geht auch ohne, aber dann wird's halt…: Informationssicherheitsstrategie . . . 216
6.3 Ordnung im Chaos: Kritikalitäten und Abhängigkeiten . . . 217
6.3.1 Ermittlung von Business Impact und Schutzbedarfen, oder: schon wieder Crown Jewels . . . 218
6.3.2 Asset Management und Strukturanalyse, oder: Welche Fleißarbeit müssen wir leisten? . . . 222

6.4 Integration von Stakeholdern, oder: Macht denn hier jeder, was er will? . . . 225
6.4.1 Stakeholder und ihre Issues . . . 225
6.4.2 Risikokommunikation (und ihre Tücken) . . . 228
6.4.3 3rd Party Risk & Provider Management . . . 231
6.4.4 Governance . . . 234

7 Post Crisis Care – Krisennachsorge und -nachbereitung . . . 237
7.1 Executive Summary: Crown Jewels basierte Post Crisis Care . . . 237
7.2 Der Blick nach außen: Reparieren der Stakeholderbeziehungen . . . 238
7.3 Der Blick nach innen: Menschen, Abläufe und Technik . . . 239
7.3.1 Faktor Mensch . . . 240
7.3.2 Crown Jewels . . . 242
7.3.3 Alarmierung und Eskalation . . . 242
7.3.4 Zusammenspiel der Ebenen der Notfall- und Krisenorganisation . . . 243
7.3.5 Strategische Ebene . . . 243
7.3.6 Taktische Ebene: BCM und IRBC . . . 245
7.3.7 Operative Ebene: Cybersecurity Incident Response . . . 246
7.3.8 Krisenkommunikation . . . 247
7.3.9 Prävention, Cyberhygiene und Dienstleistersteuerung . . . 248

8 Auf einen Blick: Sieben Todsünden des Cyber Crisis Managements . . . 249

Zum Weiterlesen . . . 253

Abkürzungen und Glossar . . . 259

Abbildungsverzeichnis

Abb. 3.1 Telefonkaskade 35
Abb. 3.2 Initialisierung der Krisenbewältigung 41
Abb. 3.3 Krisenstabsprotokoll 43
Abb. 3.4 zyklischer Führungsprozess 67
Abb. 3.5 Krisenbewältigungsprozess (Gesamtdarstellung) 67
Abb. 3.6 Wiederanlaufreihenfolge der Technologiegruppen 110
Abb. 4.1 Krisenstab 130
Abb. 5.1 Risk Map 207
Abb. 6.1 Stakeholderlandkarte 227

Tabellenverzeichnis

Tab. 4.1 Krisenkommunikationsplan bei einer DDoS-Attacke. 158
Tab. 4.2 Trainingsprogramm (Auszug). 166
Tab. 6.1 Verfügbarkeitsregelungen in SLA. 232

Cyber-Krisen wie aus dem Lehrbuch

1

1.1 Cyber Crisis re-invented: Sony Pictures Entertainment

Warum ausgerechnet SPE?
Der Angriff auf SPE aus dem Jahr 2014 ist ein Paradebeispiel, weshalb professionelles Cyber Crisis Management im 21. Jahrhundert für jede Organisation eine Schlüsselkompetenz sein muss. Jede Organisation besitzt Daten, die vertraulich sind und immer verfügbar sein müssen. Ebenso ist die Integrität der Daten wichtig – nicht nur für die Buchhaltung, sondern auch für Fertigungsprozesse, Transaktions- und Steuerungssysteme. Und wem gefällt schon der Gedanke, einem Wildfremden Informationen anzuvertrauen, nur weil uns nicht auffällt, dass es sich um einen Fremden handelt?

Gleichzeitig erfüllt der Fall weitere Kriterien, die ihn für uns zu einem guten Übungsbeispiel machen:

- Die Dramaturgie des Krisenverlaufs ist prototypisch – von einer falschen Lagebeurteilung über mangelhafte Krisenkommunikation, Insideraktivitäten, Präzedenzfällen im Unternehmen bis hin zu peinlichen öffentlichen Reaktionen und nicht abschließend geklärter Täterschaft
- Zahlreiche Details sind öffentlich bekannt, d. h. es besteht kein Risiko, Kundeninteressen zuwiderzuhandeln.

Was wäre wenn…?
Stellen wir uns vor, wir erhielten eine Mail, in der mit der Übernahme unserer IT-Systeme, der Veröffentlichung von Gehältern, internen Mails oder Kundendaten gedroht würde, kurz, mit einem massiven Angriff sowohl auf unsere materiellen als auch immateriellen Werte. Wüssten wir, was zu tun ist im Fall einer Erpressung, bei einem Hackerangriff oder wenn vertrauliche Informationen an die Öffentlichkeit zu geraten

H. Kaschner, *Cyber Crisis Management,* https://doi.org/10.1007/978-3-658-43465-6_1

drohen? Was, wenn wir uns über unseren Firmen-E-Mail-Account abschätzig über Aufsichtsbehörden, Journalisten oder Kooperationspartner geäußert hätten und nun das ganze Internet mitlesen kann? Das klingt unrealistisch und übertrieben? Nun ja. Wie schnell ein solches Szenario Realität werden kann, musste die Geschäftsleitung von Sony Pictures Entertainment (SPE) erfahren.

Aus dem Nichts

Der 24. November 2014 beginnt für die Mitarbeiter von SPE, einer US-Tochter von Sony, wie jeder Montag. Die Mitarbeiter plaudern an der Kaffeemaschine über die Sportergebnisse und Erlebnisse des Wochenendes. Doch dann ist plötzlich alles anders. Auf ihren Arbeitsplatzrechnern verkündet eine Meldung, die Guardians of Peace (GOP) hätten die Geräte gekapert. Während dies einerseits für die Mitarbeiter bedeutete, tagelang auf Stift und Papier ausweichen zu müssen, war es andererseits für Unternehmensleitung und Führungskräfte der Auftakt einer komplexen Krise.

Aber der Reihe nach. Am 21. November 2014, einem Freitag, erhielt SPE eine Mail, in der eine bestimmte Geldsumme gefordert wurde. Drei Tage später attackierten Hacker die IT-Systeme. Sie stahlen mehrere Terabyte an Daten und veröffentlichten sie im weiteren Zeitverlauf im Internet, unter anderem via Wikileaks:

- Filme
- 47.000 Sozialversicherungsnummern
- Gehaltslisten
- Gesundheitsinformationen
- interne Mails
- Passwörter
- eine Liste mit den Tarnnamen bekannter Schauspieler

Obendrein kaperten die Angreifer verschiedene Twitter-Accounts von SPE.

Und SPE macht…?

Nach diesem Schock schaltete SPE Experten und Ermittlungsbehörden ein, will aber trotzdem erst am 1. Dezember – also eine Woche nach dem Angriff – bemerkt haben, dass auch Personaldaten betroffen waren. An diesem Tag begann SPE, die Mitarbeiter zu informieren.

Ergänzend bat Sony die Medien, die Berichterstattung über den Hack einzustellen und drohte mit rechtlichen Konsequenzen. Ebenso drohte das Unternehmen Twitter, falls Twitter nicht Accounts deaktiviere, über die gestohlene Informationen verbreitet wurden. Reddit löschte die Subpage zu dem Hack („SonyGOP“).

Am 15. Dezember (!) veröffentlichte SPE für Betroffene schließlich Informationen auf der Startseite seiner Homepage in einem schwarzen, an einen Trauerflor erinnernden Banner.

So ganz nebenbei: Eine Pressemitteilung zu den Ereignissen suchte man auf der Unternehmenshomepage lange Zeit vergeblich.

Insider- und Historiendrama
Ehemalige Mitarbeiter erklärten öffentlich, SPE habe wissentlich die Informationssicherheit vernachlässigt und reichten Klage gegen das Unternehmen ein.

Nicht genug: Fast zeitgleich behauptete eine weitere Hackergruppe, Sonys Videospielebereich gehackt zu haben, um auf Sicherheitslücken hinzuweisen. Tenor: Sony sollte eigentlich die finanziellen Mittel haben, um die Sicherheit seiner Netzwerke zu gewährleisten.

Der Alptraum
Da der Zugriff auf die Buchhaltungssysteme sogar Ende Januar 2015 noch nicht wieder voll gegeben war, musste SPE eine Fristverlängerung für den Quartalsbericht beantragen. Für Unternehmen, die an der US-Börse notiert sind, eine alles andere als wünschenswerte Situation. Allein im ersten Quartal 2015 investierte SPE rund 15 Mio. US-$ im Rahmen des Cyber Crisis Managements. Vor dem Hintergrund des Hacks und seiner Folgen erklärte Amy Pascal im Mai 2015 ihren Rücktritt als Co-Vorstandsvorsitzende von SPE.

Tappen im Dunkeln
Bis heute ist nicht abschließend geklärt, wie lange der Angriff vom Eindringen in die IT-Systeme bis zur Veröffentlichung der Daten insgesamt dauerte und wer dafür tatsächlich verantwortlich ist. Überwiegend wird eine Dauer von mindestens zwei Monaten und vor dem Hintergrund des SPE-Films The Interview eine wie auch immer geartete Beteiligung Nordkoreas angenommen. Wenn dies stimmt, liegt eine asymmetrische Konfliktlage vor: auf der einen Seite ein privatwirtschaftliches Unternehmen, auf der anderen ein staatlicher Akteur.

1.2 Dramaturgie unzureichend gemanagter Cyber-Krisen

Phasen
Unabhängig davon, ob wir durch eine Cyber-Attacke, klassische technische Probleme oder einen Ausfall bedingt durch höhere Gewalt (Elementarereignisse etc.) in eine Cyber-Krise schlittern: Wir können prototypische Phasen und darin wiederkehrende Ereignisse identifizieren.

Alles scheint ruhig
Zunächst scheint alles ruhig zu sein, alles wie immer. Die Öffentlichkeit und alle unsere Stakeholder interessieren sich nur für uns, insofern sie ein konkretes Anliegen an uns haben. Ansonsten interessieren sie sich nicht für uns und wollen in der Regel auch nicht von uns behelligt werden.

In dieser Phase machen wir die ersten, grundlegenden Fehler: Wir

- versäumen, die technischen oder organisatorischen Voraussetzungen zu schaffen, die einen Abfluss oder Ausfall von IT-Ressourcen (Systeme, Daten) im Idealfall verhindern oder alternativ wenigstens wieder schnellstmöglich beheben;
- versäumen, Schwachstellen und damit verbundene Risiken systematisch zu identifizieren oder zu behandeln – oftmals entgegen der expliziten Warnungen von Mitarbeitern oder Dienstleistern, die Schwachstellen können technischer, organisatorischer oder menschlicher Natur sein;
- haben keinen geregelten Prozess, mittels dessen wir unsere Sicherheitsarchitektur kontinuierlich weiterentwickeln;
- versäumen, Pläne für die Geschäftsfortführung von kritischen Prozessen aufzusetzen, in denen beschrieben ist, wie der Ausfall zentraler IT-Ressourcen zu kompensieren wäre;
- sind blind gegenüber host- oder netzwerkbasierten Angriffen, da wir weder IDS oder IPS, noch SIEM-Lösungen nutzen bzw. kein SOC im 24/7 betreiben;
- versäumen uns ein gutes Verständnis unserer Informationsarchitektur zu verschaffen – damit fehlt uns elementares Wissen für fundierte Entscheidungen im Krisenfall;
- pflegen eine negative Feedback- und Fehlerkultur, die nicht gerade geeignet ist, die Loyalität von (ehemaligen) Mitarbeitern zu sichern;
- haben keine oder nur rudimentäre organisatorische Maßnahmen ergriffen, um im Bedarfsfall effektive Krisenbewältigung inklusive Krisenkommunikation betreiben zu können;
- nehmen bei einem Migrationsprojekt für IT-Systeme aufgrund der Kosten und Zeitvorgaben Risiken in Kauf bzw. reden diese bewusst klein.

Es beginnt
Auslöser

- Bei der letztlichen Migration von IT-Systemen geht etwas gravierend schief. Wir merken es jedoch nicht sofort, sondern erst mit etwas Zeitverzug. Bis dahin feiern wir uns selbst und posten Bilder von der Feier auf Social-Media-Plattformen (ok, zugegeben, die Postings sind nicht typisch, aber leider schon mal vorgekommen).
- Ein Erpressungsschreiben geht ein, aber möglicherweise verloren bzw. wird nicht ernst genommen.
- Gerüchte, dass Datenbestände, die uns gehören, im Internet kursieren, tauchen auf. Oder gleich die Daten selbst.

Operative Ebene

- Bewegung auf der XDR-Plattform. IDS/IPS und SIEM schlagen an.
- Die Vielzahl der Alarme kann durch das Cybersecurity Operation Center (CSOC) kaum bewältigt werden, zumal es ohnehin unter zu vielen False Positives leidet oder mit zusätzlichen Aufgaben betraut ist oder nicht 24/7 betrieben wird.

Eskalation

- Es herrscht Unsicherheit auf allen Ebenen, ob, und wenn ja, wer und wie, alarmiert werden soll.
- Mitglieder der Notfallteams sind nur schwer erreichbar, da die Situation außerhalb der üblichen Arbeitszeiten erfolgt.

Taktische Ebene

- Die Beschreibungen in den Notfallplänen sind unzureichend.
- Bei der Aufnahme des Notbetriebs hakt es, da nicht alle kritischen Geschäftsprozesse korrekt identifiziert waren.

Strategische Ebene

- Der Krisenstab und/oder die oberste Leitungsebene wird bestenfalls verzögert alarmiert.
- Es herrscht Uneinigkeit, wie die Lage zu bewerten ist.
- Es herrscht Unsicherheit, inwieweit Maßnahmen nötig sind.
- Der Krisenstab tut sich schwer mit der Entscheidung, den Krisenfall festzustellen und die Krisenbewältigung an sich zu ziehen.

Stakeholder

- Unzufriedenheit macht sich unter den Kunden und Partnern breit: Wir seien unfähig und noch nicht einmal erreichbar. Und wenn wir erreichbar sind, seien unsere Antworten nichtssagend.
- Kunden richten immer mehr Anfragen an uns, die wir nur unzureichend beantworten können.
- Erste Anfragen von Medien trudeln ein. Wir sind nicht sprachfähig.

In der Krise
Operative Ebene

- Netzsegmente werden abgeschaltet, Systeme heruntergefahren.
- Die Eindämmung und Beseitigung der Ursache des Incidents schreitet auf technischer Ebene voran.

Taktische Ebene

- Zunächst hakt es bei der Aufnahme des Notbetriebs, aber nach einiger Zeit stehen die kritischen Prozesse zumindest in gewissem Umfang wieder zur Verfügung.
- Der Output, der im Notbetrieb produziert werden kann, reicht nicht aus.
- Die Wiederherstellung von IT-Systemen und Datenbeständen schreitet voran.

Strategische Ebene

- Der Krisenstab verliert sich in Diskussionen.
- Es dauert viel zu lange, bis wir ein offizielles Signal geben, dass wir uns des Problems bewusst sind.

Stakeholder

- Kunden laufen Sturm.
- Mitarbeiter beschweren sich, dass sie nicht oder in ungenügender Weise informiert werden.
- „Heckenschützen" tauchen auf: ehemalige Mitarbeiter, Dienstleister oder sonstige Insider erklären, ein derartiger Zwischenfall sei zu erwarten gewesen. (Vermeintliche) Defizite seien intern längst bekannt gewesen, aber ignoriert worden.
- Datenschützer, Aufsicht und Pressure Groups: Alle verlangen Aufklärung.

Krise scheint überwunden
Operative Ebene

- Die weitergehende forensische Untersuchung beginnt.

Taktische Ebene

- Die wesentlichen IT-Systeme und Daten sind wiederhergestellt.
- Wir kehren mit unseren kritischen (Geschäfts-)Prozessen zum Normalbetrieb zurück.

Strategische Ebene

- Der Krisenstab hebt den Krisenfall auf.

Stakeholder

- Unser Geschäftsbetrieb normalisiert sich.
- Das Vertrauen in unsere Organisation ist beschädigt, mit ein wenig Glück aber noch nicht irreparabel.

- Falls Versprechen aus vorangegangen Phasen nicht eingehalten werden: Missfallensäußerungen via Social Media, ggfs. auch klassische Medien.
- Insgesamt: Das Interesse der Öffentlichkeit nimmt ab, da andere Themen neuer und spannender sind.

Krise reloaded
Operative Ebene

- Die forensische Untersuchung fördert Teile eines Root Kits zutage.
- Der Angreifer konnte nicht vollständig aus den Systemen verdrängt werden.
- Einfallstore wurden nicht so gründlich geschlossen, dass ein erneutes Eindringen möglich ist.

Taktische Ebene

- Wir versuchen, den Rückstau abzuarbeiten, der aufgrund der Einschränkungen der letzten Tage aufgelaufen ist.

Strategische Ebene

- Alles deutet darauf hin, dass Daten über einen viel längeren Zeitraum als bislang angenommen abgeflossen sind oder manipuliert wurden.
- Eine neuerliche Lagefeststellung und Bewertung ist nötig.

Stakeholder

- Informationen über schlummernde Zeitbomben sickern durch.
- Falls Versprechen aus vorangegangen Phasen nicht eingehalten werden: Missfallensäußerungen via Social Media, ggfs. auch klassische Medien.
- Ein echter Shitstorm bricht los, gegen den alles aus den vorangegangenen Phasen ein laues Lüftchen war.
- Vorwürfe werden wiederholt und immer lauter: Wir seien immer noch unfähig oder gar unwillig sowie vor allem ignorant und lernresistent.
- Unsere Aufsicht kündigt eine Sonderprüfung an.
- Datenschützer drohen mit Bußgeld, Pressure Groups mit Abmahnungen.
- Partner und Wettbewerber distanzieren sich öffentlich.
- Akteure aus der Politik (Kommunal-, Landes-, Bundespolitik) geben der Versuchung nach und positionieren sich gegen uns.
- Anteilseigner verlangen Aufklärung.

Nach der Krise
Operative Ebene

- Die Angreifer sind (hoffentlich) vollständig aus den Systemen vertrieben.
- IT-Systeme werden von Grund auf neu aufgesetzt.
- Schwachstellen (Einfallstore) werden (hoffentlich) systematisch geschlossen (kurzfristig).
- IT-Berechtigungen werden (hoffentlich) restriktiver gehandhabt (kurzfristig).
- Detektionsfähigkeiten werden (hoffentlich) systematisch verbessert (mittelfristig).

Taktische Ebene

- Der IT-Betrieb und die Geschäftsprozesse normalisieren sich.
- Zusätzliche Kapazitäten (bspw. von extern) sind nötig, um den aufgelaufenen Rückstau abzuarbeiten.

Strategische Ebene

- Die Leitungsebene unserer Organisation ist unter Druck: Anteilseigner, Aufsicht und Kunden sind gleichermaßen verärgert.
- Die Lessons Learned ergeben, dass weitreichende Änderungen in der Governance unserer Organisation nötig sind.
- Erhebliche Kosten werden erwartet – für Kundenbindungs- und -gewinnungsmaßnahmen, für Strafzahlungen, aber auch für technisch-organisatorische Änderungen.
- Personelle Konsequenzen – auch auf Leitungsebene – sind unvermeidlich.

Stakeholder

- Falls Versprechen aus vorangegangen Phasen nicht eingehalten werden: Missfallensäußerungen via Social Media, ggfs. auch klassischen Medien.
- Kunden erwarten Wiedergutmachung.

Und was machen wir mit diesen Erkenntnissen?
Da wir den prototypischen Ablauf nun kennen, können wir gezielt an den Punkten ansetzen, die uns das meisten Kopfzerbrechen bereiten. Wie sind wir bei den Präventionsmaßnahmen aufgestellt, d. h. wie sind unsere Chancen, zumindest manche Arten von Cyber-Krisen zu verhindern? Wie sind wir organisatorisch auf den Tag X vorbereitet? Sind wir in der Lage, kurzfristig die unterschiedlichsten Arten von Cyber-Krisen zu bewältigen? Trauen wir uns eine professionelle Krisenkommunikation zu? Wie gehen wir das Stakeholdermanagement an? Was müssen wir bei der Krisennachsorge bedenken?

Menschen und andere Crown Jewels

2

2.1 Crown Jewels – oder: Wie wir Schwerpunkte setzen

…und das hilft uns beim Crisis Management, weil…?
Egal, ob wir mitten in einer Krise stecken oder uns dagegen wappnen wollen: Wir können uns nicht um alles gleichzeitig und gleich gut kümmern. Das Leben ist kein Videospiel, in dem wir uns bei Bedarf weitere Leben oder unendlich viel Geld dazu cheaten können. Ohne Schwerpunktsetzung geht's also nicht. Nur, wie kommen wir zu einer Schwerpunktsetzung, die ihren Namen auch wert ist?

Crown Jewels oder die Conditio sine qua non
In (fast) jeder Organisation gibt es das berühmte Etwas, ohne das die Organisation nicht existieren könnte. Zu diesem Etwas zählen

- immer die Menschen, die für die Organisation mit arbeiten und mit ihr in Kontakt kommen;
- je nach Daseinszweck der Organisation meist bestimmte Tätigkeitsfelder, Produkte, Services oder Regionen, die für den (wirtschaftlichen) Erfolg der Organisation von zentraler Bedeutung sind.

Auf diese Crown Jewels müssen sich unsere Bemühungen konzentrieren. Herausfinden können wir sie durch eine sogenannte strategische Business Impact Analyse (BIA). Was wäre, wenn bestimmte

H. Kaschner, *Cyber Crisis Management,* https://doi.org/10.1007/978-3-658-43465-6_2

- Informationen kompromittiert (veröffentlicht, manipuliert, nicht verfügbar oder nicht mehr vertrauenswürdig) oder der
- Segmente ihren Geschäftsbetrieb bzw. die Leistungserbringung unterbrechen müsste?

An welchen Ecken unserer Organisation wären die Auswirkungen besonders drastisch, ja vielleicht sogar existenzgefährdend? Oder um in unserer Metapher zu bleiben: Was ist das Äquivalent zu einem Totalschaden?

Schwerpunktsetzung vs. Gießkannenprinzip
Der Fokus auf Crown Jewels ermöglicht (nicht nur) beim Management von Cyber-Krisen, Budgets zu allokieren. Die Grundlagen dazu legen wir insbesondere durch ein unserem Risikoprofil angemessenes Informationssicherheitsniveau. Aber Achtung: Alle Informationen und Prozesse gleichermaßen vor Cyber-Attacken zu schützen ist ein Ding der Unmöglichkeit und vor allem vollkommen unwirtschaftlich. Der Daseinszweck keiner Organisation besteht darin, für sich selbst Informationssicherheit zu betreiben. Geld für Sicherheitsmaßnahmen auszugeben ist immer nur Mittel zum Zweck und es nach dem Gießkannenprinzip in die Organisation zu schütten, macht uns nicht sicherer, sondern nur ärmer.

Aus der Praxis: strategische Business Impact Analyse
Für eine strategische BIA brauchen wir keinen überakademisierten Ansatz. Wir wollen schließlich keine akademische Abhandlung erstellen, sondern Schwerpunkte zur Budgetallokation herausfinden. Dazu gehen wir einfach die Geschäftsfelder, Produkte oder Regionen unserer Organisation durch.

Ausgehend von einer potenziellen Kompromittierung von Informationen und/oder einer Unterbrechung des Geschäftsbetriebs schauen wir uns dabei folgende Aspekte an:

- Gefährdungen für Leib und Leben
- Gefährdungen für die Umwelt (ESG als Investorenthema!)
- Wertschöpfungsbeiträge (Cash is Cake!)
- Reputationsaspekte (Wie schaffen wir es zu einer eigenen Folge in einem Podcast-Enthüllungsformat?)
- rechtliche Showstopper (Betriebslizenz, Marktzugänge)

Diese einfache Übung malt uns ein Bild unserer Crown Jewels. Die Praxis zeigt, dass die meisten Elemente des Bilds oftmals weder neu noch überraschend sind. Jedoch sind sie selten als Ganzes allen Mitgliedern des (Top-)Managements in dieser Deutlichkeit bewusst. Dieses Awareness-Defizit beeinträchtigt die Steuerungsfähigkeit von (Cybersicherheits-)Risiken, sodass die Schwerpunktsetzung für die Allokation von Security-Budgets oftmals reichlich arbiträr wirkt.

2.2 Faktor Mensch

2.2.1 Entscheidungen oder die Essenz von Krisenbewältigung

Krisenmanagement heißt, Menschen zu managen
Auch in Cyber-Krisen geht es nicht ohne Menschen, im Gegenteil. Es geht nicht nur nicht ohne sie, sondern explizit um sie. Warum ist das so? Nun, Krisen entstehen nicht durch irgendwelche Ereignisse, sondern erst durch die Bewertungen, die wir alle diesen Ereignissen geben. Ein Datenleck oder von einem Angreifer verschlüsselte und so unserem Zugriff entzogene Daten sind zunächst ein technisches Problem – aber eben nur zunächst, denn aus dem technischen wird schnell ein reales Problem: Aus einem Datenleck kann eine Bloßstellung resultieren und ein technisches Problem kann beispielsweise zu ausbleibenden, verzögerten oder fehlerhaften Überweisungen führen etc. Genau diese Folgen sind es, die wir nach unseren spezifischen (und oft ziemlich subjektiven) Maßstäben bewerten. Doch damit nicht genug: Abhängig vom Ergebnis der Bewertung dürfen wir mit einer Handlung rechnen. Und das ist der entscheidende Punkt. Wenn wir in der Lage sind, auf unsere Mitmenschen einzuwirken, können wir ihre Haltung gegenüber dem Ereignis und somit ihre Reaktion beeinflussen. Dazu bleibt uns leider wenig Zeit. Entscheidungen wollen getroffen werden, stets und ständig – gerade bei der Krisenbewältigung, wenn alle Beteiligten unter großer Anspannung (vulgo: Stress) stehen.

Entscheidungszwänge auf allen Ebenen
Beim Management von Cyber-Krisen werden wir auf strategischer wie auch auf taktisch-operativer Ebene permanent mit Fragen konfrontiert. Wir brauchen nur wenig Phantasie, um uns einige prototypische Fragen vorzustellen: Sollen wir

- den Krisenstab einberufen?
- der Öffentlichkeit mitteilen, dass wir ein Datenleck hatten?
- bestimmte IT-Systeme vom Netz trennen und somit zwar die Ausbreitung eines Virus verhindern, gleichzeitig aber auch wichtige Geschäftsprozesse zumindest temporär lahmlegen und damit einen meldepflichtigen Notfall provozieren?
- ein Backup einspielen oder das Risiko in Kauf nehmen, Dateninkonsistenzen zu erzeugen?
- …

Diese Liste können wir beliebig fortsetzen. Aber egal, welche Fragen wir ergänzen – eines haben sie gemeinsam: Unsere Entscheidung wird in der Regel weitreichende Konsequenzen haben.