Holger Kaschner

Cyber Crisis Management

Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation

EBOOK INSIDE

Springer Vieweg

Cyber Crisis Management

Holger Kaschner

Cyber Crisis Management

Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation

Springer Vieweg

Holger Kaschner
Berlin, Deutschland

ISBN 978-3-658-27913-4 ISBN 978-3-658-27914-1 (eBook)
https://doi.org/10.1007/978-3-658-27914-1

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

Springer Vieweg

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

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 betreibt, 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 BS 11200 eine „unnormale und instabile Situation, die die strategischen Ziele, die Reputation oder die Überlebensfähigkeit einer Organisation bedroht". 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 11200 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.

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.

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 gar 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.

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. Diese und weitere Maßnahmen stellen wir im Kap. 4 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 Management-Disziplinen und -Systeme:

- Asset Management
- Business Continuity Management (BCM)
- Cybersecurity Management
- ICT readiness for business continuity (IRBC) bzw. IT Service Continuity Management (ITSCM)
- (Cyber) Incident Management
- Information Risk Management (IRM)
- Information Security Management (ISM)
- Stakeholder- und Issuemanagement

Dies schauen wir uns im Kap. 5 näher an.

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. 6.

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 27005, ISO 27031, ISO 27032, ISO 27035, ISO 31000 sowie BSI 200-x und ITIL® v3 respektive 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 BS 11200 sowie BfV/BSI/ASW 2000-3.

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.

Inhaltsverzeichnis

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 unseren Zweck geradezu prädestinieren:

- 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 Verdacht, 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 gera-

H. Kaschner, *Cyber Crisis Management*, https://doi.org/10.1007/978-3-658-27914-1_1

ten 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

- 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.

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

- IT-Systeme werden von Grund auf neu aufgesetzt.

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?

Das Wichtigste zuerst: Der Faktor Mensch beim Management von (Cyber-)Krisen

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 Fantasie, um uns einige prototypische Fragen vorzustellen: Sollen wir

- den Krisenstab einberufen?
- der Öffentlichkeit mitteilen, dass wir ein Datenleck hatten?

H. Kaschner, *Cyber Crisis Management*, https://doi.org/10.1007/978-3-658-27914-1_2

- 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.

Herausforderungen Die Herausforderungen sind angesichts dieser permanenten Entscheidungszwänge vielfältig:

- Wir haben kein auch nur annähernd vollständiges Lagebild.
- Die Belastbarkeit der vorliegenden Informationen ist oft unklar.
- Das Interesse wesentlicher Stakeholder (Presse, Anteilseigner, Kunden, Aufsicht etc.) reduziert den Spielraum für Fehler erheblich.
- Die Krise selbst erzeugt Stress, macht müde und laugt uns aus – gerade bei länger andauernden Krisen.
- …

All das beeinflusst unser Entscheidungsverhalten.

Anforderungen an Entscheidungen zur Krisenbewältigung Unsere Entscheidungen müssen (mindestens) zwei Anforderungen erfüllen:

- Schnelligkeit
- Zweckmäßigkeit

Um Missverständnissen vorzubeugen: Schnelligkeit bedeutet nicht Aktionismus, im Gegenteil. Schnelligkeit bedeutet vielmehr, so zeitnah wie möglich erkennen zu geben, dass wir uns der Situation bewusst sind und gleichzeitig ist sie Ausdruck dafür, dass die im Tagesgeschäft gerade im mittleren Management beliebte Strategie des „Zuwartens“ (d. h. totstellen und auf neue Erkenntnisse hoffen) bei der Krisenbewältigung selten eine Option darstellt. Eine langsame Reaktion wird uns als Untätigkeit oder Schwäche ausgelegt. Beides Eigenschaften, die nicht gerade positiv konnotiert und damit wenig geeignet sind, auf unser übergeordnetes Ziel bei der Krisenbewältigung einzuzahlen: auf den Erhalt des Vertrauens in unsere Organisation.

Zweckmäßigkeit meint nicht, dass wir stets die für uns persönlich sicherste Option bevorzugen sollten. Derart defensives Entscheidungsverhalten kann zwar durchaus zweckmäßig sein, muss es aber nicht. Zweckmäßigkeit meint vielmehr, dass unsere Entschei-

dungen sowohl geeignet als auch angemessen sein müssen, um angesichts der spezifischen Krisensituation das Vertrauen in unsere Organisation direkt oder auch indirekt zu schützen. Wohlgemerkt, das gilt für den Zeitpunkt und Kontext, aus dem heraus wir die Entscheidung treffen. Im Nachhinein werden wir immer schlauer sein, so dass wir gut beraten sind, wenn wir zu jeder wesentlichen Entscheidung den Kontext und Zeitpunkt schriftlich festhalten.

Konsequenzen der An- und Herausforderungen Wenn wir den Herausforderungen nun die Anforderungen entgegenhalten, die unsere Entscheidungen zur Krisenbewältigung erfüllen müssen, wird eines klar: Wir haben Handlungsbedarf. Dazu können wir gleichzeitig oder nacheinander an verschiedenen Punkten ansetzen. Beispielsweise hilft es uns, wenn wir Maßnahmen ergreifen, um

- die Eintrittswahrscheinlichkeit und Auswirkungen von Krisen zu reduzieren (Kap. 5). Der Grund ist einfach: wo keine Krise, da kein Bedarf an Entscheidungen zur Krisenbewältigung sowie
- im Fall einer Krise keine Zeit zu verlieren, Automatismen nutzen zu können und die richtigen Hilfsmittel an der Hand zu haben (Kap. 3 und 4).

Das ist aber nur die halbe Miete. Unabdingbar ist vor allem, dass wir verstehen, warum Menschen Situationen so bewerten und reagieren, wie sie es tun (siehe Abschn. 2.2).

2.2 Bewertungen, Verhaltensmuster und Stress

2.2.1 Wie Menschen Situationen wahrnehmen und bewerten

Wahrnehmung ist subjektiv Wie unsere Stakeholder eine Situation wahrnehmen ist höchst individuell und hängt von einer ganzen Palette an Faktoren ab, die wir als Organisation nicht immer beeinflussen können. Zu den Faktoren gehören unter anderem:

- Betroffenheit
  Ist die Person direkt oder indirekt betroffen?
- Nähe
  Wie groß ist die räumliche und emotionale Distanz des Stakeholders zum Risiko?
- Freiwilligkeit
  Ist er das Risiko, das durch unsere Krise schlagend wurde, freiwillig eingegangen oder nicht? Hat er sich freiwillig auf uns eingelassen oder nicht?
- Kontrollierbarkeit
  Ist bzw. war die Situation für den Einzelnen subjektiv kontrollierbar oder nicht?
- Unmittelbarkeit
  Ist der Stakeholder zeitlich unmittelbar oder nur verzögert betroffen?