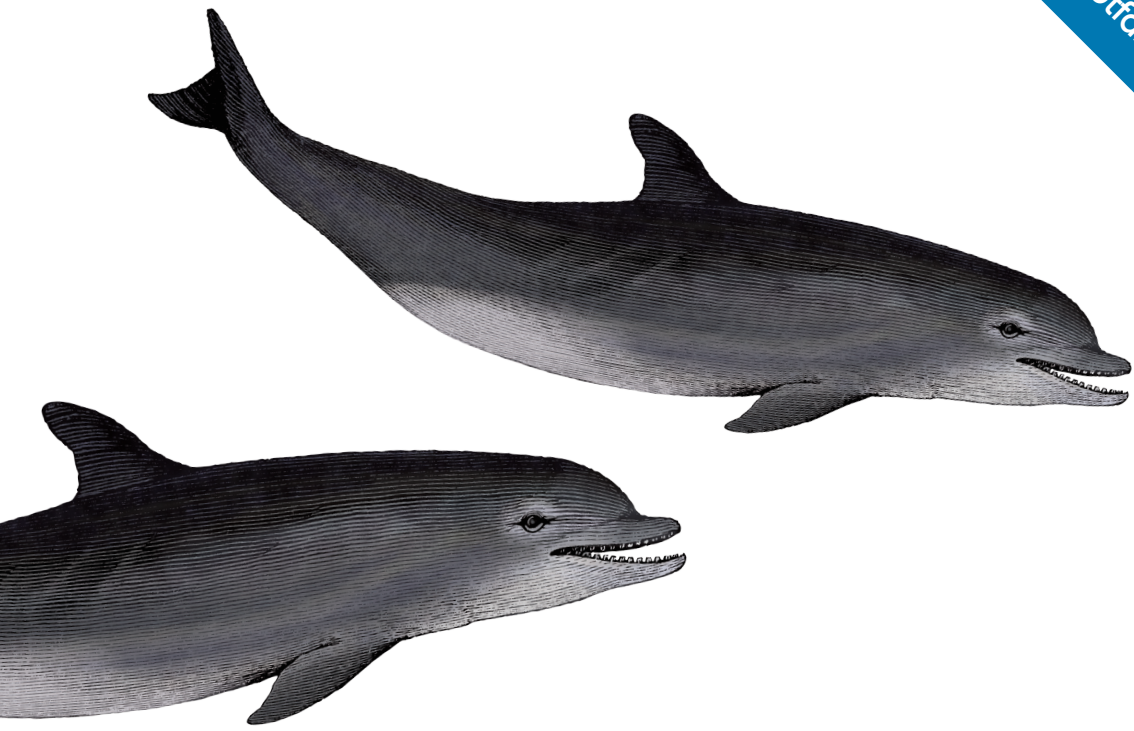
O'REILLY®

Inkl. Case Study und 10-Punkte-Notfallplan



Kommunikation in der Cyberkrise

Sprach- und handlungsfähig im IT-Ernstfall

Isabelle Ewald &
Alexander Schinner

KAPITEL 1
Einleitung

Wer regelmäßig Wirtschaftsnachrichten liest, wird festgestellt haben, dass sich binnen kürzester Zeit[1] eine neue Gattung von Neuigkeiten darin etabliert hat, nämlich Berichte über elementare Cyberkrisen. Zwischen positiven Umsatzmeldungen und Analysen prosperierender Märkte rücken immer öfter auch Beschreibungen gezielter Angriffe durch Hacker und andere Kriminelle auf Unternehmen und Organisationen in den Fokus der Medien. Man erfährt von Firmen, die durch gezielte Phishing-Attacken Millionenbeträge verloren haben, oder von Datendiebstählen, bei denen vertrauliche Informationen in die Hände von Computerkriminellen gelangt sind. Auch Meldungen über Ransomware-Angriffe, bei denen ganze Landkreise mit der Verschlüsselung ihrer Daten erpresst werden und darum bangen müssen, sie wiederzuerlangen, sind keine Seltenheit mehr.

Im Idealfall gelingt es einer Gruppe übermüdeter, aber entschlossener IT-Administratoren, innerhalb einer einzigen Nachtschicht den alten Zustand wiederherzustellen – eine schöne Vorstellung, aber leider kaum realistisch. Im Worst Case, und von diesem sollten wir ausgehen, bedeutet ein Angriff weit mehr als nur das Zurückspielen von Backups. Mitarbeiterinnen und Mitarbeiter müssen informiert, Kunden beruhigt und Zulieferer um Geduld gebeten werden. Verträge, Service-Level-Agreements und gesetzliche Meldepflichten treten plötzlich in den Vordergrund. Die eigentliche Herausforderung ist nicht nur der technische Wiederanlauf, sondern der Wiederaufbau von Vertrauen – und dieser erfordert Zeit, strategische Kommunikation und konsequente Maßnahmen.

Da sich genau dieses Szenario zunehmend als Status quo etabliert, nehmen wir es in diesem Buch als Ausgangspunkt für alle weiteren Überlegungen und Maßnahmen.

In diesen Momenten zeigt sich, dass Kommunikation mehr als nur ein Werkzeug ist – sie wird zum Lebensnerv eines jeden Krisenmanagements. Gerade in den ersten Stunden einer Krise, wenn Unsicherheit und Chaos dominieren, kommt es darauf an, klare Botschaften zu formulieren und die richtigen Informationen an die richtigen Adressaten weiterzugeben. Intern müssen die Mitarbeiterinnen und Mitarbeiter wissen, wie sie handeln sollen, während extern das Vertrauen von Kunden und Part-

1 Dass diese Cyberkrisen schon seit sehr viel längerer Zeit in Fachkreisen bekannt sind, soll hier nicht unerwähnt bleiben.

nern in die Kompetenz des Unternehmens aufrechterhalten werden muss. Diese präzise, zielgerichtete und transparente Kommunikation wird zur zentralen Aufgabe, um Eskalationen zu vermeiden.

Dieses Buch führt Krisenmanagerinnen und Krisenmanager nicht nur näher an die grundlegenden Prinzipien zur Bewältigung von Cyberkrisen heran, sondern zeigt auch die entscheidenden Schnittstellen auf, die eine effektive Krisenkommunikation ermöglichen. Es verbindet operative Maßnahmen mit strategischer Planung und berücksichtigt dabei auch regulatorische Vorgaben, sodass Unternehmen ihre internen Prozesse optimal an externe Anforderungen anpassen können.

Orientierung in digitalen Ausnahmesituationen: Warum es dieses Buch braucht

Eine Cyberkrise bringt Unternehmen und Organisationen in eine Ausnahmesituation, die rasches Handeln und bereichsübergreifende Koordination erfordert. Dabei wird eine ganze Bandbreite von Akteuren mobilisiert, denn Cyberkrisen als solche haben eine ganz eigene Dynamik, die sie zum Teil stark von anderen Krisenarten unterscheidet (dazu mehr im Abschnitt »Schnellstart für Eilige – die wichtigsten Kapitel für den schnellen Einstieg« auf Seite 26). Um sie zu überstehen, ist das Zusammenspiel von Verantwortlichen quer durchs Organigramm wesentlich geworden. Dabei sind Jobtitel weniger entscheidend als vielmehr der Handlungsbereich der jeweiligen Person. Die einzelnen Rollen zu orchestrieren, ist zu einer zentralen Herausforderung in digitalen Zeiten geworden, da jeder Einzelne gezwungen ist, über seinen Aktionsradius hinauszuschauen und interdisziplinär zu denken und zu handeln. Krisenmanager haben in zentraler koordinierender Funktion also eine entscheidende Aufgabe: Sie müssen sicherstellen, dass alle Beteiligten effektiv zusammenarbeiten und dass die verschiedenen Kompetenzen im Unternehmen optimal genutzt werden. Aber auch die fachlich Verantwortlichen haben eine wichtige Rolle: Sie müssen in der Lage sein, ihre Expertise gezielt einzubringen und gleichzeitig über ihre gewohnten Zuständigkeitsbereiche hinauszublicken.

»Wir wurden gehackt, das war sicher ein Virus!«: Solche Pauschalaussagen klingen in einer Cyberkrise ähnlich fundiert wie eine medizinische Diagnose aus der Antike: »Die gelbe Galle ist nicht im Gleichgewicht.« Aussagen wie diese zeigen vor allem eines: gefährliches Halbwissen. Und genau das ist der Anfang allen Übels. Solche Formulierungen mögen für Laien harmlos erscheinen, doch in der Krisenkommunikation sind sie fatal. Sie vermitteln ein Bild von Planlosigkeit, verhindern eine fundierte Ursachenanalyse und bieten Raum für Spekulationen. Eine unpräzise oder uninformierte Kommunikation kann nicht nur das Vertrauen der Stakeholder erschüttern, sondern auch dazu führen, dass falsche Maßnahmen ergriffen werden. Deshalb ist es wichtig, dass Unternehmen die Anatomie eines Cyberangriffs verstehen und ihre Kommunikation auf Fakten stützen – sowohl intern als auch extern.

Nach der Lektüre dieses Buchs sind Verantwortliche nicht nur deutlich besser informiert und vorbereitet, sondern haben auch konkrete Maßnahmen vor Augen – so-

dass alle Beteiligten genau wissen, was im Ernstfall zu tun ist. Um dies zu verdeutlichen, hilft es, sich einmal die folgenden Fragen zu stellen:

- Habe ich einen Plan, wann ich die Öffentlichkeit informiere, um Schaden zu minimieren und Vertrauen zu erhalten, ohne dabei die laufende Krisenbewältigung zu gefährden?
- Bin ich in der Lage, alle relevanten Akteure, unabhängig von ihrer Position im Unternehmen, rasch zu koordinieren und sicherzustellen, dass sie ihre Rollen und Verantwortlichkeiten in der Krise kennen?
- Wie stelle ich sicher, dass Kunden, Partner und die Öffentlichkeit mir auch im Ernstfall Gehör schenken und meine Kommunikation ernst nehmen? Habe ich die technischen Möglichkeiten und die notwendigen Informationen, um mit jeder Person zu kommunizieren, mit der ich kommunizieren möchte?
- Kann ich gewährleisten, dass unser Unternehmen nach einem Cyberangriff schnell wieder funktionsfähig ist, und welche Maßnahmen kann ich präventiv treffen, um den Schaden zu begrenzen?
- Wie gut bin ich darauf vorbereitet, in einer hochstressigen Situation mit den psychologischen Taktiken der Angreifer umzugehen, die darauf abzielen, maximalen Druck aufzubauen, und diese Strategie im Krisenstab und im Unternehmen zu kommunizieren?
- Verstehe ich, warum ein professioneller Verhandler so agiert, wie er es tut – warum er gezielt verhandelt, wann er bewusst Zeit gewinnt, wann er klare Grenzen setzt und wie er dabei stets die Kontrolle über die Situation behält?

Spätestens jetzt sollte ersichtlich geworden sein, dass es entscheidend ist, dass Fachabteilungen nicht isoliert agieren, sondern ihr Wissen und ihre Ressourcen im Kontext des Gesamtereignisses einbringen. Dieses Buch zeigt, wie genau diese Zusammenarbeit vorbereitet, koordiniert und in der Praxis umgesetzt werden kann. Sie lernen, wie Sie komplexe Sachverhalte verständlich aufbereiten und kommunizieren, um fundierte Entscheidungen zu ermöglichen. Darüber hinaus wird vermittelt, welche Strukturen und Prozesse notwendig sind, damit Fachabteilungen flexibel und kooperationsbereit agieren – nicht nur im akuten Krisenfall, sondern auch präventiv, um Risiken frühzeitig zu erkennen und eigenständig zu handeln. So werden sie zu unverzichtbaren Partnern im Krisenmanagement, die durch ihre Expertise und ihr Engagement maßgeblich zur Bewältigung der Krise beitragen. »Communication is key« – in der Krise ist sie entscheidend. Schnelligkeit, Klarheit und Strategie bestimmen, ob eine Cyberkrise bewältigt wird oder eskaliert. Wer vorbereitet ist, bleibt handlungsfähig. Mit der Lektüre dieses Buches haben Sie, liebe Leserinnen und Leser, einen wichtigen Schritt gemacht, um einer potenziellen Cyberkrise resilient zu begegnen.

An wen sich das Buch richtet

Die effiziente Bewältigung einer Cyberkrise erfordert, wie wir bereits festgestellt haben, eine koordinierte Anstrengung verschiedener Expertisen innerhalb eines Unter-

nehmens oder einer Organisation (dazu zählen auch öffentliche Einrichtungen). Dieses Buch richtet sich daher an eine breite Zielgruppe in Unternehmen und Organisationen, denn eine ganze Reihe von Expertinnen und Experten spielen in der Krisenbewältigung eine wichtige Rolle. Dazu zählen allen voran die hier aufgelisteten Profilgruppen:

- **IT-Security** als Expertengruppe mit der Verantwortung, Sicherheitsvorfälle zu überwachen, Bedrohungen abzuwehren, Schäden zu begrenzen und die IT-Infrastruktur nach einem Angriff wiederherzustellen.
- **Datenschutz** als überwachende Instanz, die sicherstellt, dass der Schutz personenbezogener Daten von Kunden, Mitarbeiterinnen und Mitarbeitern und Geschäftspartnern gewahrt bleibt – insbesondere in Krisensituationen. Sie spielt eine zentrale Rolle bei der rechtlichen Bewertung, der Einhaltung regulatorischer Vorgaben und der Kommunikation mit den Aufsichtsbehörden.
- **Management und Führungskräfte** als Entscheiderinnen und Entscheider, die Strategien vorgeben, notwendige Ressourcen bereitstellen und die gesamte Krisenreaktion koordinieren, während sie das Unternehmen gegenüber relevanten Stakeholdern vertreten. Das Team rund um CIO, CTO und CISO nimmt hier eine besondere Rolle ein.
- **Krisenstab** als Koordinator, der die Gesamtabläufe während der Krise steuert, Notfallpläne umsetzt und sicherstellt, dass alle Abteilungen koordiniert und effektiv zusammenarbeiten, um die Krise zu bewältigen.
- **Compliance- und Risikomanagement** als Überwacher der Einhaltung gesetzlicher Vorgaben und interner Richtlinien, die Risiken bewerten und notwendige Maßnahmen einleiten, um den Vorfall zu dokumentieren und die Sicherheitsstrategien zu verbessern.
- **Juristen** als Beraterinnen und Berater, die juristische Unterstützung bieten, insbesondere in Bezug auf die Einhaltung von Gesetzen und anderen verbindlichen Bestimmungen. Sie helfen, die rechtlichen Risiken der Krise zu bewerten und notwendige Schritte zur Schadensbegrenzung einzuleiten.
- **Human Resources** als zentrale Stelle, die Mitarbeiterinnen und Mitarbeiter im Umgang mit der Krise unterstützen und ihre Bedürfnisse berücksichtigen, um das Wohlbefinden und die effektive Kommunikation innerhalb des Unternehmens zu gewährleisten.
- **Unternehmenskommunikation** als Team, das Kunden, Partner und Medien informiert und die Krisenkommunikation steuert, um Reputationsschäden zu minimieren und das Vertrauen ausgewählter Stakeholder sicherzustellen.

In einer Cyberkrise bilden alle beteiligten Gruppen innerhalb einer Organisation eine Schicksalsgemeinschaft, in der alle aufeinander angewiesen sind. In dieser Situation sollten einzelne Gruppen nicht isoliert voneinander agieren. Umso wichtiger ist es, die Bedürfnisse der jeweils anderen Involvierten zu verstehen, und die wichtigste Grundlage für diese Zusammenarbeit ist nun mal die Kommunikation. Nur durch transparente, schnelle und präzise Informationsflüsse kann sichergestellt wer-

den, dass alle Beteiligten jederzeit auf dem gleichen Stand sind und effektiv agieren können. Eine klare und kontinuierliche Kommunikation ist der Schlüssel, um Missverständnisse zwischen den Parteien zu vermeiden und Reaktionszeiten zu optimieren. Ohne diese enge Abstimmung drohen Fehlinformationen und Verzögerungen, die den Erfolg der Krisenbewältigung gefährden könnten.

Nicht zuletzt in dezentralen Strukturen und/oder einer unübersichtlichen Gemengelage ist es von enormer Bedeutung, dass die oben genannten Gruppen Hand in Hand zusammenarbeiten und ihren Beitrag zur Bewältigung einer Cyberkrise leisten. Das ist kommunikativer Hochleistungssport, da im Eifer des Gefechts wertvolle Informationen verloren gehen oder falsch interpretiert werden könnten, was am Ende negativen Einfluss auf die Reaktionszeit hat. Aus diesem Grund gibt es dieses Buch: Es soll als umfassender Leitfaden dienen, der bewährte Verfahren und Strategien für die interdisziplinäre Zusammenarbeit und Kommunikation während einer Cyberkrise detailliert beschreibt. Ziel ist es, eine gute Struktur und effektive Kommunikationskanäle zu schaffen, um sicherzustellen, dass alle Beteiligten schnell und präzise auf Vorfälle reagieren können und so die Auswirkungen der Krise minimiert werden.

Wie Sie mit dem Buch arbeiten

Das vorliegende Werk soll Ihnen dabei helfen, Ihre Kommunikation als eines der wichtigsten Werkzeuge zur Bewältigung einer Cyberkrise (was auch immer diese ausgelöst haben mag) »gut geölt« zu halten. Kommunikation ist schließlich mehr als nur das bloße Übermitteln von Informationen – sie bildet einen integralen Bestandteil des Krisenmanagements, indem sie die Grundlage für Transparenz, Glaubwürdigkeit und koordinierte Reaktionen schafft. Sie muss agil, angemessen, wertschätzend und zielführend sein, was ein hohes Maß an Flexibilität erfordert.

Es ist nicht entscheidend, dass Sie jedes Kapitel dieses Buches von Anfang bis Ende stringent durcharbeiten. Sie können auch punktuell und nach Bedarf auf bestimmte Abschnitte zugreifen, je nachdem, in welcher Phase Ihrer Krisenbewältigung Sie sich befinden. Nutzen Sie das Buch als flexibles Nachschlagewerk, das Ihnen spezifische Informationen und Handlungsempfehlungen bietet, wenn Sie sie am dringendsten benötigen.

Dieses Buch bietet eine ausgewogene Mischung aus fundamentalen Konzepten und praxisnahen Anleitungen, mit denen Sie sowohl strategisch als auch operativ auf eine Cyberkrise vorbereitet sind. Betrachten Sie es als Ihren Begleiter, der Sie durch die dynamischen Phasen eines digitalen Ernstfalls führt – sei es bei präventiven Maßnahmen, in der akuten Krisenbewältigung oder bei der nachträglichen Analyse.

Die modular aufgebaute Struktur des Buches ermöglicht es Ihnen, gezielt die für Ihre Situation relevanten Kapitel zu konsultieren. Durch diese flexible Herangehensweise können Sie die für Ihre individuellen Bedürfnisse und den aktuellen Stand Ihrer Krise passenden Informationen und Tools effizient nutzen. Der Gesamttext ist in elementare Bereiche gegliedert, die Ihnen helfen, sich umfassend und praxisnah auf Cyberkrisen vorzubereiten.

Aufbau des Buchs

Teil I: Der Einstieg

- Bevor es an Konzepte und Strategien geht, bietet das Buch mit Kapitel 2, *Case Study: Compor AG*, eine fiktive, aber realitätsnahe Fallstudie zur Compor AG, die typische Kommunikationsmuster, Fehlentscheidungen und Dynamiken im Verlauf einer Cyberkrise nachvollziehbar macht.
- Kapitel 3, *Historische Beispiele*, ergänzt diesen Einstieg um reale Beispiele von Cyberkrisen aus Politik, Wirtschaft und öffentlicher Verwaltung – inklusive Lessons Learned und Kommunikationsanalyse.

Teil II: Background – Grundlagen von Cyberkrisen

- Kapitel 4, *Anatomie einer Cyberkrise*, bietet Ihnen eine fundierte Einführung in die verschiedenen Arten von Cyberkrisen und deren Auswirkungen. Sie müssen diese theoretischen Grundlagen kennen, um die aus ihnen resultierenden praktischen Anleitungen und Maßnahmen zu verstehen.
- Kapitel 5, *Vorbereitung und Risikoanalyse*, befasst sich mit Bedrohungsanalysen, Risikobereitschaft und präventiven Maßnahmen wie Bedrohungsmodellierungen und mit der Kommunikationsvorbereitung auf Basis gängiger Standards.
- Kapitel 6, *Analyse von Cyberkrisen*, stellt bewährte Analysemodelle vor – wie die Cyber Kill Chain®, MITRE ATT&CK® oder das Diamond Model –, die dabei helfen, Angriffe systematisch zu analysieren.
- Kapitel 7, *Recht und Regulierung*, erläutert rechtliche Rahmenbedingungen, regulatorische Vorgaben und Meldepflichten.
- Ein wesentlicher Bestandteil des Buches ist die Krisenkommunikation, die sowohl grundlegende Prinzipien als auch spezifische Herausforderungen bei Cyberkrisen abdeckt. Kapitel 8, *Grundlagen und Prinzipien der Krisenkommunikation*, und Kapitel 9, *Kommunikation bei Cyberkrisen*, helfen Ihnen, eine effektive Kommunikationsstrategie zu entwickeln und anzuwenden, um Transparenz zu gewährleisten und die Akzeptanz bei Stakeholdern sicherzustellen.

Teil III: Der Werkzeugkasten – Reaktion auf die Krise

- Kapitel 10, *Kickstart Krisenmanagement*, bietet Ihnen konkrete Handlungsempfehlungen, um direkte und gezielte Reaktionen auf eine Krise zu ermöglichen. Hier finden Sie praktische Tipps, die Sie unmittelbar in der Krisensituation umsetzen können – inklusive Aufbau eines Krisenstabs, Kommunikationsstart, Prioritätensetzung und Dokumentation.
- Kapitel 11, *Rollen und Verantwortlichkeiten*, erläutert die Struktur von Krisenteams, Zuständigkeiten und das Schnittstellenmanagement.

- Kapitel 12, *Interne Kommunikation*, und Kapitel 13, *Externe Kommunikation*, liefern Ihnen Anleitungen zur internen und externen Kommunikation mit verschiedenen Anspruchsgruppen.
- Kapitel 14, *Digitale Kanäle und Social Media*, zeigt, wie Unternehmen digitale Kanäle in der Krise sinnvoll einsetzen können. Es erläutert ein durchdachtes Social-Media-Management, das auf Monitoring, Reaktionsstrategien und proaktive Kommunikation setzt.
- Kapitel 15, *Medienarbeit in der Cyberkrise*, widmet sich der Frage, wie Unternehmen ihre Reputation in einer digital beschleunigten Krisendynamik schützen können – und was zu tun ist, wenn das Vertrauen bereits Risse zeigt. Sie lernen Strategien kennen, um mit Medienanfragen souverän umzugehen und Narrative aktiv zu steuern.
- Kapitel 16, *Wer darf was wann wissen? – Vertraulichkeit, Geheimhaltung und Informationsaustausch*, hat die Informationsklassifizierung und den Informationsschutz zum Thema. Es wird erläutert, welche Informationen geschützt werden sollten, welche geteilt oder veröffentlicht werden können und welche Methoden es dafür gibt.
- Kapitel 17, *Kommunikation mit Angreifern*, beschäftigt sich mit der Frage, ob man mit Cyberkriminellen kommunizieren sollte, und wenn ja, wie. Es gibt einen Überblick über Verhandlungsstrategien und rechtliche Rahmenbedingungen.

Teil IV: Gute Vorbereitung

- Kapitel 18, *Toolbox für die Praxis*, bietet eine Auswahl an Checklisten, Mustervorlagen und einen Kommunikations-Selbstcheck, mit dem Sie Ihre Organisation auf den Prüfstand stellen können.
- Kapitel 19, *Training und Übungen*, führt in Szenarientrainings, Simulationen und Verhalten unter Druck ein. Es zeigt, wie realitätsnahe Übungen und Trainings die Krisenresilienz stärken – insbesondere im Bereich der Kommunikation.

Teil V: Nachbereitung und Ausblick

- Kapitel 20, *Analyse und Nachbereitung*, widmet sich der systematischen Nachbereitung – mit Methoden zur Root-Cause-Analyse, zur Kommunikationsevaluation und zu den Lessons Learned.
- Das abschließende Kapitel 21, *Die Cyberkrisenkommunikation von morgen: Von der Reaktion zur Resilienz*, schließlich gibt einen Ausblick auf die Weiterentwicklung der Cyberkrisenkommunikation – etwa mit Blick auf neue Bedrohungslagen durch künstliche Intelligenz.

Diese Publikation bietet eine wertvolle Ergänzung zu einem möglicherweise bereits vorhandenen internen Krisenhandbuch, das in Ihrer Organisation entwickelt wurde. Während Ihr Krisenhandbuch spezifische, auf Ihre Organisation zugeschnittene Prozesse und Notfallpläne enthält, liefert dieses Buch umfassende Strategien, Prinzipien und Methoden für das Krisenhandling. Unsere Empfehlung lautet daher:

- Nutzen Sie die Informationen in diesem Buch, um bestehende Prozesse in Ihrem Notfallmanagement zu verfeinern und zu erweitern.
- Integrieren Sie neue Erkenntnisse und bewährte Praktiken aus dem Buch in Ihr internes Krisenhandbuch, um es auf dem neuesten Stand zu halten.
- Verwenden Sie die hier beschriebenen Kommunikations- und Reaktionsstrategien, um Ihre Trainingsszenarien im Krisenhandbuch zu verbessern und sich gezielter auf Akutsituationen vorzubereiten.

Unser Use Case: Die Compor-AG

Um komplexe Prozesse und Theorien besser nachvollziehbar zu machen, präsentieren wir in Kapitel 2 einen fiktiven Fall in Form einer Case Study. Er dient als illustrative Brücke zwischen komplexer Theorie und praktischer Anwendung, um die behandelten Konzepte anschaulicher und verständlicher zu gestalten. Alle im Fall dargestellten Personen, Ereignisse und Daten sind rein fiktiv, und jegliche Ähnlichkeiten mit realen Personen oder tatsächlichen Ereignissen sind zufällig und unbeabsichtigt. Der fiktive Fall soll ein vertieftes Verständnis der behandelten Themen fördern und ist daher nicht als tatsächliche Darstellung realer Szenarien zu interpretieren.

Schnellstart für Eilige – die wichtigsten Kapitel für den schnellen Einstieg

Es ist passiert, die Cyberkrise ist im Anmarsch – Verantwortliche müssen schnell ins Tun kommen, denn jede Minute zählt. Für diesen Fall zeigt Tabelle 1.1 Ihnen die wesentlichen Kapitel, die einen raschen Einstieg in die dringend benötigten Maßnahmen und Kommunikationsstrategien ermöglichen. Von den Sofortmaßnahmen am IT-Unfallort bis hin zur effektiven internen und externen Krisenkommunikation – hier finden Betroffene kompakt jene Bausteine, die sie brauchen, um in der akuten Cyberkrise den Überblick zu behalten, rasch fundierte Entscheidungen zu treffen und den Krisenverlauf erfolgreich zu steuern.

Tabelle 1.1: Schnellstart in die Cyberkrisenkommunikation

Kapitel	Inhalt
Kapitel 10: **Kickstart Krisenmanagement – Ein 10-Punkte-Plan für Sofortmaßnahmen am IT-Unfallort, wenn's richtig brennt**	Dieses Kapitel liefert einen 10-Punkte-Plan mit Sofortmaßnahmen, der direkt ansetzt, wenn ein IT-Incident eskaliert. Besonders der frühzeitige Kommunikationsstart (siehe Abschnitt »3. Bereiten Sie frühzeitig die Kommunikation vor!« auf Seite 182) und das Einrichten sicherer Kommunikationskanäle (siehe Abschnitt »4. Sichere Kommunikationskanäle sind unverzichtbar!« auf Seite 188) sind wichtig, um rasch handlungsfähig zu werden.
Kapitel 8: **Grundlagen und Prinzipien der Krisenkommunikation**	Hier werden die fundamentalen Definitionen, Ziele und Strategien der Krisenkommunikation erläutert – eine unverzichtbare Basis, um in der Krise strukturiert und zielgerichtet zu agieren.
Kapitel 9: **Kommunikation bei Cyberkrisen**	Da Cyberkrisen spezifische Herausforderungen mit sich bringen, bietet dieses Kapitel praxisnahe Empfehlungen, wie diese im Kommunikationsprozess adressiert werden können, etwa bei der Entwicklung eines Krisenkommunikationsplans.
Kapitel 12: **Interne Kommunikation**	Eine schnelle und zielgerichtete Information der Mitarbeiter ist entscheidend, um intern Ruhe zu bewahren und koordiniert zu reagieren. Dieses Kapitel gibt Ihnen praxisnahe Maßnahmen an die Hand, wie intern mobilisiert und informiert wird.
Kapitel 13: **Externe Kommunikation**	Neben der internen Abstimmung muss auch die Kommunikation mit Kunden, Partnern und der Öffentlichkeit souverän gesteuert werden – Kapitel 13 liefert hier konkrete Ansätze und Strategien.
Kapitel 15: **Medienarbeit in der Cyberkrise**	Insbesondere wenn die Krise nach außen dringt, ist der richtige Umgang mit Medien und Presseanfragen zentral. Dieses Kapitel zeigt, wie Pressemitteilungen, Stellungnahmen und Medienkonferenzen zielgerichtet umgesetzt werden können.
Kapitel 18: **Toolbox für die Praxis**	Praktische Tools wie Checklisten und Muster können im akuten Krisenfall den schnellen Überblick und die Umsetzung von Maßnahmen unterstützen.

Die Website zum Buch

Weitere Materialien, Checklisten, Vorlagen, die CR-Card, Errata sowie ergänzende und aktualisierte Links zum Thema finden Sie unter:

https://www.cyberkrisenkommunikation.com

KAPITEL 11

Rollen und Verantwortlichkeiten

Wer spricht für das Unternehmen, wenn es brennt? Eine klare Definition von Zuständigkeiten ist fundamental, um in der Krise handlungsfähig zu bleiben. In diesem Kapitel erhalten Sie einen Überblick über die verschiedenen Rollen in der Krisenkommunikation, der aufzeigt, wie eine effektive Zusammenarbeit zwischen IT-Security, Management und Kommunikationsteams gelingt.

Teamstruktur in der Krise

An einigen Stellen in diesem Buch haben wir den Begriff der **Schicksalsgemeinschaft** verwendet, um die Dynamik und den Zusammenhalt zu beschreiben, die eine Cyberkrise unweigerlich erzeugt. Denn sie tangiert nicht nur einzelne Abteilungen oder Fachbereiche, sondern bringt alle Beteiligten – von Mitarbeiterinnen und Mitarbeitern über das Management bis hin zu externen Stakeholdern – in eine gemeinsame Verantwortungslage. Jede Entscheidung, jede Handlung und jede unterlassene Reaktion beeinflusst nicht nur den Verlauf der Krise, sondern auch die Beziehung und die Zusammenarbeit der Betroffenen.

Der Begriff der Schicksalsgemeinschaft verdeutlicht, dass eine Cyberkrise kein isoliertes Ereignis ist, sondern eine kollektive Herausforderung, die nur durch eine enge und abgestimmte Zusammenarbeit bewältigt werden kann. Dieser Gedanke zieht sich wie ein roter Faden durch die Prinzipien der Krisenkommunikation, die in diesem Buch beschrieben werden. Es geht darum, klare Strukturen zu schaffen, Verantwortung zu übernehmen und gemeinsam Lösungen zu entwickeln – unabhängig von Hierarchien oder Zuständigkeitsbereichen.

Dies ist bei Weitem kein einfaches Unterfangen, denn Egos müssen zurückgestellt und Kompetenz sowie Verantwortung klar verteilt werden. In einer Krisensituation – welcher Natur sie auch immer sein mag – steht nicht die individuelle Leistung im Vordergrund, sondern der gemeinsame Anspruch, die Krise zu bewältigen. Dies erfordert, dass alle Beteiligten ihre persönlichen Interessen zugunsten des Gesamtergebnisses zurückstellen und stattdessen auf Zusammenarbeit und gegenseitiges Vertrauen setzen. Kompetenz muss gezielt genutzt und Aufgaben müssen entspre-

chend den jeweiligen Stärken und Erfahrungen verteilt werden. Die Qualität der Kommunikation in einer Cyberkrise steht und fällt daher auch mit der Struktur des Krisenstabs, jenes Gremiums, das die taktische Verantwortung während der Krise trägt. Der Krisenstab umfasst die Rollen, die unabhängig von der Art der Krise immer ins Krisenmanagement eingebunden sind. Dazu gehören in der Regel folgende Positionen:[1]

- Leiter des Krisenstabs
- Geschäftsführendes Mitglied des Krisenstabs
- Kommunikation
- Recht
- Protokoll

In Tabelle 11.1 werden die Funktionen beschrieben, die diese Rollen ausüben.

Tabelle 11.1: Rollen und deren Funktion in einem Krisenstab

Rolle	Funktion
Krisenstabsleitung	Verantwortlich für die übergreifende Koordination, Priorisierung und Entscheidungsfindung. Er oder sie trägt die Gesamtverantwortung und sorgt dafür, dass alle Mitglieder effizient zusammenarbeiten.
Geschäftsführendes Mitglied[2]	Stellt die Verbindung zwischen der strategischen Ebene der Geschäftsführung und der operativen Arbeit des Krisenstabs her. Sorgt dafür, dass die Entscheidungen der Geschäftsleitung in den Krisenstab eingebracht und dort umgesetzt werden. Gleichzeitig berichtet es regelmäßig an die Geschäftsführung über den aktuellen Stand und die Fortschritte der Krisenbewältigung.
Kommunikation	Verantwortlich für die Entwicklung und Steuerung der internen sowie externen Kommunikation, für die Sicherstellung von konsistenten Botschaften und das Management von Anfragen von Medien, Kunden und Partnern
Recht	Berät zu rechtlichen Verpflichtungen, z. B. Meldepflichten nach DSGVO, Stellt sicher, dass Maßnahmen im Einklang mit gesetzlichen Anforderungen stehen.
Protokoll	Dokumentiert alle relevanten Informationen und Entscheidungen während der Krisenbewältigung. Dies umfasst insbesondere die Protokollierung/Aufzeichnung/Erfassung, welche Handlungsoptionen gewählt wurden, deren Zielsetzungen, die verantwortlichen Personen für die Umsetzung, den Zeitpunkt der Entscheidungsfindung sowie die festgelegten Fristen für die Durchführung.

1 Kaschner, Holger. »Cyber-Krisenmanagement: Das umfassende Handbuch zur Bewältigung von Krisen und Krisenkommunikation in der digitalen Welt«. Springer Vieweg, Wiesbaden, 2020.

2 **Wichtig:** Das geschäftsführende Mitglied des Krisenstabs ist nicht gleichzusetzen mit der Geschäftsführung selbst. Während die Geschäftsführung strategische Leitlinien vorgibt und den übergeordneten Überblick behält, ist das geschäftsführende Mitglied direkt in die operative Arbeit des Krisenstabs eingebunden. Es dient als Vermittler, sorgt für die Umsetzung strategischer Entscheidungen im Krisenstab und gewährleistet die Berichterstattung an die Geschäftsführung.

Die Rolle der Geschäftsführung

Es empfiehlt sich, die Geschäftsführung aus der operativen Krisenstabsarbeit herauszuhalten, denn in Krisen entstehen oft Unsicherheiten und Spekulationen, die das Vertrauen in das Unternehmen erschüttern können. Wenn die Geschäftsführung zu nah am operativen Geschehen ist, könnte sie unbeabsichtigt solche Gerüchte verbreiten oder mit Informationen umgehen, die noch nicht bestätigt sind. Ihre Rolle besteht also eher darin, die strategische Leitung zu übernehmen und gezielt die Unterstützung der Stakeholder zu sichern. Indem sie sich auf übergeordnete Entscheidungen und die Kommunikation beispielsweise mit Investoren, Kunden und Behörden konzentriert, kann sie eine klare Linie vorgeben und die Stabilität des Unternehmens wahren.

Der erweiterte Krisenstab hingegen setzt sich aus Fach- und Führungskräften zusammen, deren Expertise in der aktuellen Krisensituation zusätzlichen Wert bietet. Sie verfügen über spezifisches Wissen, beispielsweise zu:

- Risiken der Geldwäsche
- Umweltschutz
- Arbeitssicherheit
- Facility-Management

Die Aufteilung in einen auf operative Krisenbewältigung ausgerichteten Kernkrisenstab und einen erweiterten Krisenstab mit einem Fokus auf strategischer Führung hat mehrere Vorteile: Der Kernkrisenstab besteht aus Mitgliedern, die immer in das Krisenmanagement einbezogen werden, unabhängig von der Art der Krise. Diese Mitglieder fokussieren sich darauf, was im Moment der Krise von zentraler Bedeutung ist. Der erweiterte Krisenstab hingegen setzt sich aus Fach- und Führungskräften zusammen, deren Expertise spezifische Mehrwerte für bestimmte Szenarien bietet.

Damit beide Einheiten effektiv zusammenarbeiten können, bedarf es allerdings verbindlicher Spielregeln, die sicherstellen, dass die Kommunikation und Zusammenarbeit zwischen den Stäben reibungslos funktioniert. Dazu zählen:

- **Definierte Rollen und Zuständigkeiten:** Jeder Stab kennt seine Aufgaben und Verantwortlichkeiten.
- **Regelmäßige Briefings:** Es gibt tägliche oder regelmäßige Updates zwischen den Stäben, um alle auf dem gleichen Stand zu halten.
- **Zentralisierte Kommunikation:** Ein zentraler Ansprechpartner sorgt für die konsistente und koordinierte Weitergabe von Informationen.
- **Echtzeit-Kommunikation:** Informationen müssen sofort und ohne Verzögerung weitergegeben werden.
- **Einheitliche Botschaften:** Alle Kommunikation muss klar und konsistent sein, ohne Widersprüche.

- **Vertraulichkeit:** Sensible Informationen werden nur an die relevanten Stellen weitergegeben.
- **Dokumentation:** Wichtige Kommunikationsflüsse werden dokumentiert, um ihre Nachvollziehbarkeit zu gewährleisten.

Wichtig – auch zugunsten eines effektiven Kommunikationsflusses – ist, dass der Krisenstab nicht zu groß wird. So werden lange Diskussionen vermieden und die Effizienz gewährleistet. Die Faustregel lautet: so klein wie möglich, so groß wie nötig. Nicht selten wird außerdem auf die Dienste von externen Beratern zurückgegriffen, z. B. von IT-Forensikern, Cybersecurity-Beratern oder spezialisierten PR-Agenturen. Sie kommen dann zum Einsatz, wenn Unternehmen mit eigenen Bordmitteln an ihre Grenzen stoßen. Abbildung 11.1 zeigt ein typisches Organigramm eines Krisenstabs.

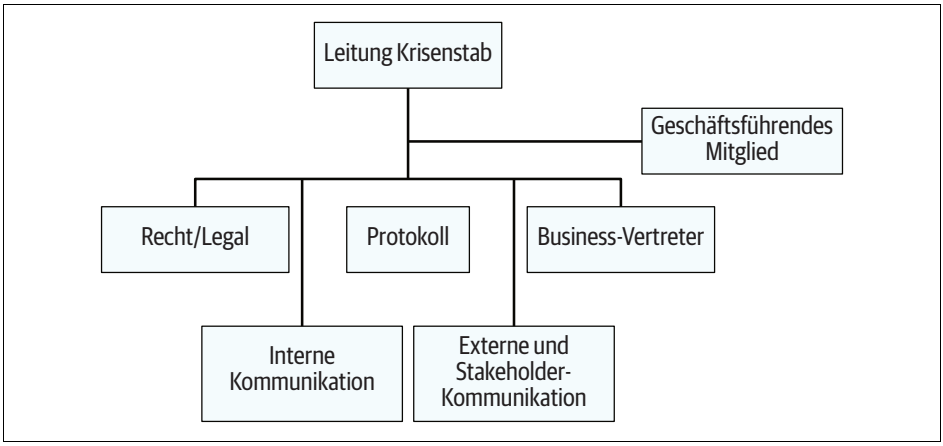


Abbildung 11.1: Beispiel-Organigramm eines Krisenstabs

Schnittstellen verstehen und nutzen – Kommunikation ohne Reibungsverluste

Ein Krisenstab kommt selten allein. Zwar bildet er den Nukleus der Krisenbewältigung, doch seine Effektivität hängt, wie wir wissen, vor allem von der engen Zusammenarbeit mit anderen Abteilungen und Expertengruppen ab. Bevor wir uns die damit verbundene kommunikative Aufgabe genauer anschauen, widmen wir uns zunächst einmal dem grundlegenden Dreiklang aus Strategie, Taktik und Operative:

Die **strategische Ebene** liegt in der Verantwortung der Unternehmensleitung. Hier werden die übergeordneten Ziele definiert, Prioritäten gesetzt und die langfristige Ausrichtung während der Krise festgelegt. Kurzum: Die strategische Ebene konzentriert sich auf das große Ganze – die Sicherung des Unternehmensimages, die Kommunikation mit hochrangigen (!) Stakeholdern und die Einhaltung von Compliance- und rechtlichen Vorgaben.

Die **taktische Ebene** wird maßgeblich vom Krisenstab abgedeckt, der dafür sorgt, dass die strategischen Vorgaben in konkrete, umsetzbare Maßnahmen übersetzt wer-

den. Er koordiniert die beteiligten Teams, stellt sicher, dass Ressourcen effizient genutzt werden, und überwacht die laufende Lage. Insbesondere in einem IT-bezogenen Krisenfall arbeiten auf dieser Ebene das *Business Continuity Management* (BCM) und das *Computer Security Incident Response Team* (CSIRT) eng zusammen. Das BCM sorgt für die Aufrechterhaltung kritischer Geschäftsprozesse und -funktionen, während das CSIRT auf technischer Ebene eingreift, um IT-Sicherheitsvorfälle zu bewältigen und den normalen Betriebszustand schnellstmöglich wiederherzustellen.

Die **operative Ebene** umfasst spezialisierte Teams, die direkt an der Front der Krisenbewältigung arbeiten, allen voran das CSIRT-Team. Diese spezialisierte Einheit ergreift technische Maßnahmen zur Bewältigung der Krise, etwa durch die Wiederherstellung betroffener Systeme, die Eindämmung von Vorfällen und die Ursachenanalyse. Sie reagiert auf Sicherheitsvorfälle durch einen strukturierten Prozess, der typischerweise in mehrere Phasen unterteilt ist, die in Tabelle 11.2 beschrieben sind.

Tabelle 11.2: Phasen und ihre Funktionen in Rahmen der Krisenbewältigung

Phasen	Funktion
Identifikation	In diesem Schritt wird der Sicherheitsvorfall erkannt und es werden die Personen informiert, die angemessen mit dem spezifischen Vorfall umgehen können. Es ist wichtig, ein CSIRT zu etablieren, das über die nötigen technischen Hilfsmittel verfügt
Eindämmung	Zentral ist es, zunächst Maßnahmen zur kurzfristigen Eindämmung des Schadens zu ergreifen, um zu verhindern, dass der Vorfall sich weiter ausbreitet. Das Ziel ist, den Vorfall unter der Schwelle zu halten, ab der eine Krisensituation ausgelöst werden muss.
Beseitigung/ Entfernung	Dabei wird die Ursache des Vorfalls identifiziert und beseitigt. Alle notwendigen Maßnahmen müssen ergriffen werden, um die Bedrohung zu eliminieren.
Recovery	In dieser Phase werden die betroffenen Systeme in ihren Ursprungszustand zurückversetzt und wieder in die Produktivumgebung integriert. Dabei müssen Schwachstellen durch aktuelle Patches behoben werden.
Lessons Learned	Nach der Bewältigung des Vorfalls wird eine Analyse durchgeführt, um aus den Erfahrungen zu lernen. Dies hilft, zukünftige Vorfälle zu verhindern und die Reaktionsstrategien kontinuierlich zu verbessern.

Das BCM spielt in dieser Phase eine unterstützende Rolle, indem es sicherstellt, dass weiterhin geschäftskritische Prozesse ausgeführt werden und Ausfallzeiten minimiert werden. Das gemeinsame Ziel des CSIRT und des BCM ist es, die operativen Auswirkungen der Krise zu reduzieren und den normalen Betriebszustand so schnell wie möglich wiederherzustellen.

Eine Anmerkung zum Thema **Vertrauen in der Kommunikation** ist hier aber noch wichtig: Gerade in der Cyberkrise entsteht bei den Beteiligten sehr schnell eine gewisse Paranoia – der Angreifer ist ja in die eigene Infrastruktur eingebrochen, man sieht ihn nicht, aber er könnte überall sein. Gefühlt könnte er hinter jedem Stück an Information und hinter jeder Nachricht stecken. Wie wahrscheinlich das wirklich ist, lässt sich nur im konkreten Fall abschätzen; die ständige Sorge behindert aber die Arbeit. Im Abschnitt »Die CR-Karte: Spreche ich wirklich mit dem CEO?« auf Seite 320 stellen wir deswegen eine kleine, praktikable Methode vor, wie man hier mit einer einfachen Methode etwas Vertrauen wiedererlangen kann.

Die Interaktion an den Schnittstellen ist zweifellos kommunikativer Hochleistungssport. Sie sichert – richtig umgesetzt – aber auch ähnlich gute Ergebnisse, wenn es darauf ankommt. Dabei ist es entscheidend, dass jede Ebene inklusive ihrer Akteure ihre Rolle kennt, aber flexibel auf die anderen reagiert, um das Krisenmanagement als Ganzes voranzutreiben:

- **Zwischen der strategischen und der taktischen Ebene:** Die Unternehmensleitung definiert langfristige Ziele, die der Krisenstab in konkrete Maßnahmen umsetzt und bei Bedarf anpasst, um auf Krisenentwicklungen zu reagieren.
- **Zwischen der taktischen und der operativen Ebene:** Der Krisenstab koordiniert die operativen Teams, stellt Ressourcen bereit und überwacht den Fortschritt, während die operativen Teams die Maßnahmen direkt umsetzen. Hier spielen das BCM und das CSIRT eine Schlüsselrolle bei der Umsetzung der Maßnahmen.
- **Zwischen der operativen und der strategischen Ebene:** Die operativen Teams liefern wichtige Rückmeldungen, die der Unternehmensleitung helfen, die Krisenstrategie anzupassen und zu optimieren. Hier sind sowohl das BCM als auch das CSIRT von entscheidender Bedeutung, um die strategischen Entscheidungen auf die operativen Gegebenheiten auszurichten.

Abbildung 11.2 zeigt das Zusammenspiel der drei Ebenen.

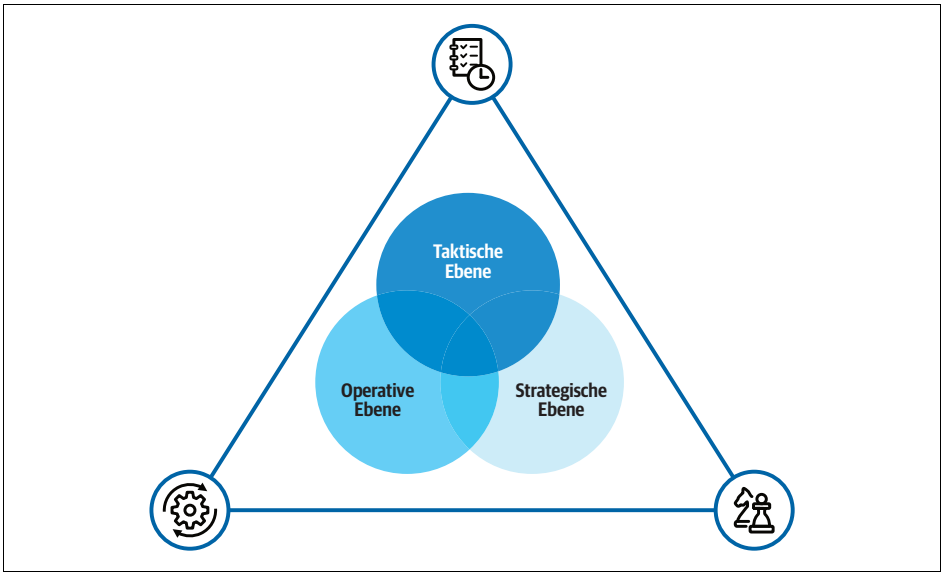


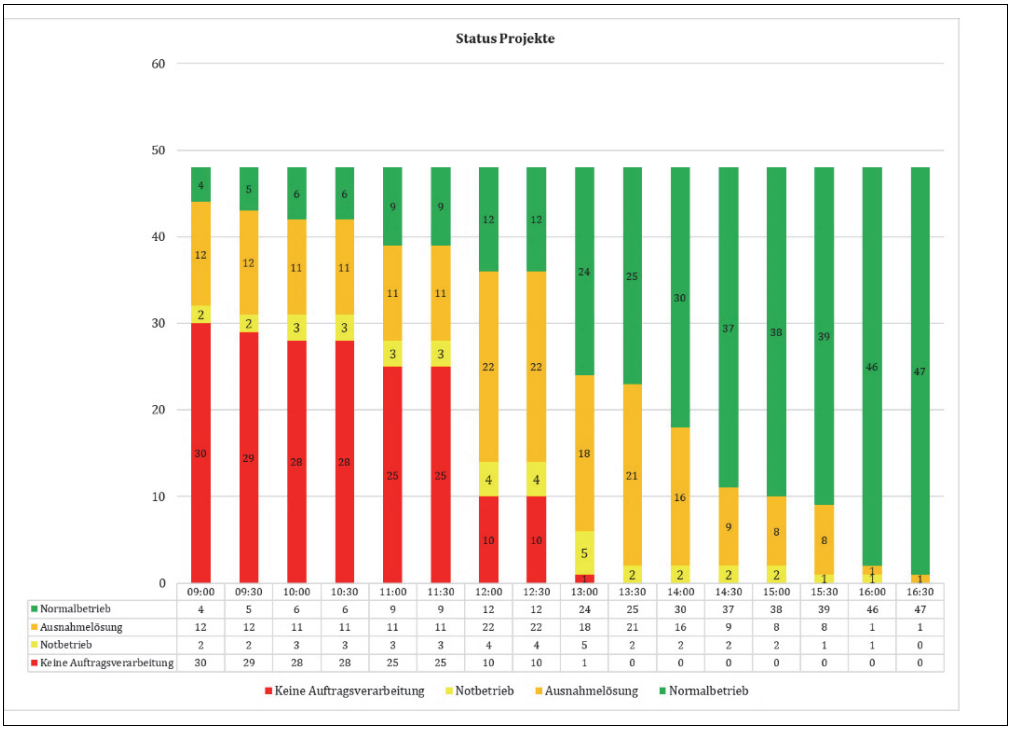
Abbildung 11.2: Zusammenspiel der Ebenen in der Krisenbewältigung

So weit die Theorie; in der Praxis kann es in Krisensituationen oft hektisch werden, worunter die Kommunikationskultur schnell leidet. Gleichzeitig bleibt wenig Raum für teambildende Maßnahmen oder Mediation – für lange Aussprachen und langwierige Diskussionen schon mal gar nicht. Was jetzt gebraucht wird, sind praktische Lösungen, die alle am Krisenmanagement Beteiligten unterstützen und die Motivation hochhalten.

Ein Ansatz, der hier unterstützend eingesetzt werden kann, ist das **Erfolgsmonitoring**, etwa in Form eines Status-Trackings. Das Prinzip ist simpel, aber effektiv: Auf einem Koordinatensystem wird in regelmäßigen Abständen die aktuelle Betriebslage als Balkendiagramm wiedergegeben, gemessen an der Anzahl der wesentlichen Einzelsysteme und -prozesse. Wir haben ein Beispiel mit insgesamt 50 Stück gewählt. Die Farben in den Balken symbolisieren verschiedene Status-Level:

- Rot: keine Auftragsbearbeitung
- Gelb: in Bearbeitung
- Grün: normale Bearbeitung
- Orange: Ausweichlösung

Abbildung 11.3 zeigt ein solches Status-Diagramm. (Wenn Sie das gedruckte Buch lesen, sehen Sie unterschiedliche Grautöne der verschiedenen Status-Level in dem Beispieldiagramm.)



	09:00	09:30	10:00	10:30	11:00	11:30	12:00	12:30	13:00	13:30	14:00	14:30	15:00	15:30	16:00	16:30
Normalbetrieb	4	5	6	6	9	9	12	12	24	25	30	37	38	39	46	47
Ausnahmelösung	12	12	11	11	11	11	22	22	18	21	16	9	8	8	1	1
Notbetrieb	2	2	3	3	3	3	4	4	5	2	2	2	2	1	1	0
Keine Auftragsverarbeitung	30	29	28	28	25	25	10	10	1	0	0	0	0	0	0	0

Abbildung 11.3: Übersicht der Status-Verteilung über verschiedene Zeiträume

Jeder Zeitstempel auf der X-Achse zeigt den Fortschritt, indem er auf Basis der Farbskala den Gesamtstatus des operativen Betriebs anzeigt. Am unteren Rand ist eine Übersicht, die den Fortschritt in Tabellenform dokumentiert. Wer also über mehrere Tage hinweg den Fortschritt seiner Bemühungen auch visuell nachvollziehen kann, hat eine klare, objektive Grundlage, mit der er die operativen Maßnahmen steuern kann.

Gerade in stressigen Situationen wie einer Krise hilft eine präzise Informationsvisualisierung, die kognitive Belastung bei der Entscheidungsfindung zu reduzieren.[3] Sie stellt externe Darstellungen von Konzepten bereit, auf die Menschen zurückgreifen können, anstatt diese im Arbeitsgedächtnis behalten zu müssen. Dies ermöglicht eine effizientere Informationsverarbeitung und verbessert die Leistung bei Urteilen und Entscheidungen. Je weniger das Arbeitsgedächtnis beansprucht wird, desto besser fällt das Urteil aus. Übersichtlich gestaltete Diagramme sind leichter zu erfassen als Text, der mehr kognitiven Aufwand erfordert.

Visualisierungen, die sich leicht erfassen lassen, ermöglichen überdies einen einfacheren und schnelleren Zugriff auf die notwendigen Informationen, wodurch die Reaktionszeit bei Entscheidungen sinkt. Ebenso schärfen sie das Bewusstsein für Unsicherheit und Risiko in einer Datenmenge. Dadurch können Entscheidungsträger unsichere Situationen besser verstehen und mit ihnen umgehen.

3 Eberhard, K. (2023). »The effects of visualization on judgment and decision-making: A systematic literature review.« Management Review Quarterly, 73(1), 167 -214. *https://doi.org/10.1007/s11301-021-00235-8*

Auf einen Blick

Inhalt