ManagerWISSEN

ANZEIGE

Ausgabe Mai 2023

Ad Special im Harvard Business manager
www.manager-wissen.com

KRISENMANAGEMENT

Aus der Krise zum resilienten Unternehmen – Navigating the Avalanche

Von Claudia Nestler und Jakob Großehagenbrock

Beim Weltwirtschaftsforum in Davos stand der Begriff der „Polycrisis" im Zentrum, andernorts liest man von Multi- oder Permakrise. Das ist nicht neu – allerdings hat es in den vergangenen Jahren einige bemerkenswerte Entwicklungen im Krisenmanagement gegeben. Vor allem drei Trends prägen das Krisenmanagement in den kommenden Jahren.

Trend Nr. 1 – Regulierung und Standards

Trotz bestehender Normen zu verwandten Disziplinen wie Sicherheit oder Business Continuity Management (BCM) war das Feld Krisenmanagement bislang weitgehend ohne konkrete Vorgaben oder Richtlinien – ganz im Sinne der Agilität. Auch durch das Fehlen von Standards begünstigt, sind in den vergangenen Jahren teils stark unterschiedliche Prozesse, Strukturen und Prinzipien in Unternehmen gewachsen. Derartige Unterschiede erschweren jedoch eine Vergleich- und Messbarkeit der Effektivität des Krisenmanagements. Aufgrund fortdauernder Unsicherheiten in den globalen Märkten und Lieferketten rückt die operative Resilienz von Zulieferern und Dienstleistern gegenwärtig stärker in den Fokus - somit auch deren Krisenmanagement.

Mit ISO 22361:2022 besteht erstmals eine ISO-Norm zum Krisenmanagement, das als Führungsaufgabe definiert wird. Die Anforderungen an Manager und Führungskräfte werden klar herausgestellt: nämlich nicht nur die Krise, sondern das strategische Ganze im Blick zu behalten und den Mitarbeitenden sowie externen Stakeholdern mittels klarer Kommunikation einen Weg durch die Krise aufzuzeigen. Sebastian Riedel von der Kommunikationsberatung Klenk & Hoursch zeigt anhand des Krisenszenarios Cyberangriff beispielhaft auf, wie die Krisenkommunikationsorganisation aufgebaut sein sollte und welche Fragen vor, während und nach einer Krise zu stellen sind (Seite 2).

Darüber hinaus steht die Resilienz kritischer Einrichtungen im Fokus der Aufsichtsbehörden, die somit indirekt Krisenmanagement adressieren, wie z. B. mit dem EU Digital Operational Resilience Act (DORA), der seit Januar 2023 in Kraft ist. Der Fokus liegt hier zwar auf der stärker regulierten Finanzindustrie und Anbietern kritischer Services wie Cloud-Dienstleistungen. Erfahrungen aus den USA und Großbritannien, wo die Regulatorik zur Operational Resilience schon länger besteht, zeigen jedoch schnelle Spill-Over-Effekte auf andere Sektoren – sei es aufgrund geänderter Anforderungen von Versicherungen oder aber auch von Geschäftspartnern.

Trend Nr. 2 – Digitalisierung

DORA macht es deutlich – es geht oft zunächst um digitale Resilienz. Dazu gehört auch ein digitales Krisenmanagement, in zweierlei Hinsicht: Zum einen sind die immer häufiger werdenden Cyberangriffe nur noch selten ein reines IT-Problem, sondern führen auch schnell zu einem geschäftlichen Problem mit signifikanten Kosten und enormer Reichweite, sodass eine zentrale, geschäftsbereichsübergreifende Steuerung erforderlich ist. In der Praxis bedeutet das: Digitales Notfallmanagement ist gut – aber erst durch (Cyber-)Krisenmanagement sind Unternehmen in der Lage, ganzheitlich auf diese Herausforderungen zu reagieren.

Zum anderen wird auch das Krisenmanagement selbst digitaler: Der klassische „War Room" hat zwar nicht ausgedient, in international agierenden Unternehmen sind jedoch die Mitglieder eines Krisenstabs häufig global disloziert. Klassische Anwendungen und Systeme sind da häufig nicht mehr ausreichend. Der Trend geht daher zu digitalen, cloudverfügbaren Incident Management Tools, die sowohl schnell verfügbare Daten für die Krisensteuerung aufbereiten, als auch Entscheidungen und Mitarbeiterkommunikation unterstützen können, wie Owen Miles von Everbridge in diesem Special (Seite 3, Technologiegestütztes Vorfalls- und Krisenmanagement) aufzeigt. Der daraus entstehende Informations- und Entscheidungsvorsprung kann in großflächigen Krisen den wesentlichen Wettbewerbsvorteil ausmachen und so zu einer schnelleren Erholung beitragen.

Trend Nr. 3 – Verbindung der Funktionen: Resilienz gegen volatile Krisenszenarien

Der dritte Trend ist die Etablierung umfassender Resilienzprogramme, die klassische Krisen-, Kontinuitäts-, Sicherheits- und Risikomanagementfunktionen integrieren. Diese logische Weiterentwicklung der Funktionen zielt darauf ab, nicht nur Führungsstrukturen für Krisensituationen oder bestimmte Szenarien vorzuhalten, sondern auch kleinere Organisationseinheiten so auszustatten, dass Vorfälle bereits dort gelöst werden können und gar nicht erst zu existenzbedrohenden Krisen eskalieren. Der Blick gilt insbesondere der strategischen Ausrichtung des Unternehmens, da diese auch in Krisensituationen als Leitmotiv dient, um Prioritäten festzulegen.

Dadurch ergibt sich eine neue Perspektive: Statt vieler kleiner, aber konkreter Pläne für bestimmte Szenarien kommt es in der Polykrise darauf an, auch auf überraschend auftretende Szenarien schnell und angemessen reagieren zu können. Das setzt eine im wirtschaftlichen Sinne gesunde Organisation ebenso voraus wie Robustheit und Flexibilität – anhand vordefinierter Prinzipien.

Dies erscheint zunächst als komplexe Herausforderung, lässt sich aber mit drei einfachen Fragen zusammenfassen: Was sind die kritischen Geschäftsprozesse? Welche Toleranzen bestehen gegenüber Störungen? Und wie können Störungen erkannt und beseitigt werden?

Durch mehr Kommunikation und Abstimmung zwischen den einzelnen Funktionen entsteht im Unternehmen eine breitere Wissensbasis und ein Bewusstsein für Resilienzthemen – und so die Voraussetzung für agiles und flexibles Handeln in außergewöhnlichen Situationen. Dazu können digitale Tools beitragen, die alle Funktionen übersichtlich zusammenbringen, wie Steve Richardson von Fusion in seinem Beitrag (Seite 4) zeigt.

Trotz dieser Trends: Eine Ideallösung für Krisenmanagement gibt es nicht - dafür sind Krisen zu volatil und Unternehmen zu unterschiedlich. Es muss daher darum gehen, die eigenen Mitarbeiterinnen und Mitarbeiter auf möglichst vielen Führungsebenen zu befähigen, auf unvorhergesehene oder gar disruptive Ereignisse zu reagieren und so Krisen frühzeitig im Unternehmen zu navigieren und gestärkt aus der Krise hervorzugehen.

Die Autoren

Claudia Nestler, *Herausgeberin dieses Specials, ist Partnerin in Risk & Regulatory bei PricewaterhouseCoopers in Deutschland. Sie hat den Bereich Forensic Services inklusive Krisenmanagement mehr als 20 Jahre geleitet.*

Jakob Großehagenbrock *ist zertifizierter Krisen- und Business Continuity Manager bei PricewaterhouseCoopers in Deutschland. Er berät Unternehmen beim Aufbau operativer Resilienz. Zudem unterstützt er sie in akuten Krisensituationen.*

Impressum

Verlag: Reif Verlag GmbH · Peter Reif · Alfred-Jost-Straße 11
69124 Heidelberg · E-Mail: peter.reif@reifverlag.de

Redaktion: Christian Deutsch · Redaktionsbüro
E-Mail: info@deutsch-werkstatt.de
Regina Gödde, E-Mail: regina.goedde@reifverlag.de

Internet: www.manager-wissen.com
Layout: metropolmedia · 69245 Bammental
Druck: ColorDruck Solutions · 69181 Leimen

Kommunikation in der Krise: Aktiver Schutz der Reputation

Von Sebastian Riedel

Krisensituationen stellen ein enormes Risiko für die Reputation von Unternehmen und Organisationen dar. Entsprechend sollten die Kommunikationsexperten von Anfang an in die Krisenbewältigung eingebunden sein. Dabei geht es um weitaus mehr als die Bereitstellung eines Krisenkommunikationsplans. Es geht um professionelle, strategische Krisenkommunikation – vor, während und nach der Krise.

Krisenmanagement ist mehr als die operative Bewältigung der Krisenursachen und einhergehender Rückkehr in einen „Normalmodus". Auch der Schutz bzw. die Widerherstellung der Reputation bei internen und externen Stakeholdern ist im Krisenfall eine wesentliche Aufgabe von Unternehmen oder Organisationen. Dieser Aufgabe kommt die Krisenkommunikation nach.

Kommunikation ist eine vertrauensbildende Maßnahme

Krisensituationen sind von einem zentralen Dilemma bestimmt: Dem hohen Kommunikationsdruck stehen fehlende gesicherte Informationen entgegen, der weitere Verlauf der Situation ist ungewiss. Das erschwert das Ziel von Krisenkommunikation, mit bedürfnisorientierter Kommunikation das Ansehen und Integrität bei internen und externen Stakeholdern zu schützen und das operative Krisenmanagement aktiv zu unterstützen.

Verstärkt wird dieses Dilemma durch die Vielzahl an internen und externen Kommunikations-Plattformen und -Kanälen, die Unternehmen heutzutage bedienen. Folglich muss der Dialog mit den diversen Stakeholdern auf verschiedenen Kanälen und in verschiedenen Formaten stattfinden – zeitlich und inhaltlich aufeinander abgestimmt. Denn gute Krisenkommunikation ist wahrhaftig, transparent und vor allem konsistent.

Hacker forcieren den Angriff auf die Reputation

Um der Reputation eines Unternehmens oder einer Organisation zu schaden, veröffentlichen Angreifer mittlerweile Attacken eigenständig in Foren oder gehen direkt auf Medien bzw. Kunden der Opfer zu. Nicht selten erfährt man erst darüber, dass man Opfer eines Cyberangriffes geworden ist – dann muss umgehend in den Krisenmodus geschaltet werden.

Wer in Krisensituationen, ob selbst- oder fremdverschuldet oder durch höhere Gewalt hervorgerufen, noch mit grundlegenden internen Organisationsfragen beschäftigt ist, wird dem Ziel, die Reputation aktiv zu schützen, nicht gerecht werden können. Vorbereitung ist der Schlüssel für erfolgreichen Reputationsschutz im Ernstfall.

Vor der Krise: Sensibilisierung, Prozess-Definition und Training

Krisenprävention beginnt mit Sensibilisierung. Es gilt, verschiedene Krisensituationen hinsichtlich ihrer Gefahr für die Reputation zu besprechen, um so die Interessen der Beteiligten abzugleichen und das Situationsbewusstsein zu schärfen. Ein starkes Tool für die strategische Analyse möglicher Fälle ist die „Szenario-Technik" („Eintrittswahrscheinlichkeit" versus „Auswirkungen auf die Reputation"). So können gemeinsame Leitlinien und Handlungsempfehlungen als Basis für die strategische Krisenkommunikation erarbeitet werden.

Vorbereitung auf den Cyberangriff heißt Lernen

Die Vorbereitung auf Krisenfälle durch Cyberangriffe geht für Kommunikationsverantwortliche häufig mit gänzlich neuen Situationen einher. Für das Reputationsrisiko ergeben sich so unterschiedliche Szenarien: Die Kommunikationshoheit kann z. B. bei einer Behörde liegen oder bestehende Präventionsmaßnahmen durch konkrete Auswirkungen auf das Unternehmen (u. a. inaktive Systeme) nahezu unbrauchbar werden.

In der Prävention geht es aber auch darum, Prozesse, ein resilientes Team-Setup sowie hilfreiche Tools aufzusetzen. Wie verlaufen Erstmeldung und Informationsweitergabe? Welche Schnittstellen zu anderen Abteilungen oder externen Stellen sind nötig? Wer bedient welchen Kanal? Prozesse für die Content-Erstellung und die Übersetzung von Fakten in Kernbotschaften gehören zu den Hauptaufgaben der Kommunikation und sind ebenso zentral wie eine Planung der Kommunikationskaskade – vom Intranet, über den Social-Media-Post bis zur Pressemitteilung.

Teil der Vorbereitung ist auch das Aufsetzen eines Team-Setups sowie die Definition der benötigten Rollen mit einhergehenden Aufgaben und Zuständigkeiten. Und letztlich geht es darum, über Tools die Arbeit im Krisenfall zu erleichtern bzw. zu beschleunigen, unter anderem durch professionelles Monitoring oder vorbereitete Inhalte pro Szenario, die auf die tatsächlichen Krisensituationen „nur noch" angepasst werden müssen.

Jedoch ist alle Theorie nutzlos, wenn sie nicht auch regelmäßig angewendet wird. In Form von realistischen Trainings, sogenannten Echtzeit-Simulationen, entweder mit Kommunikationsfokus oder im Rahmen eines operativen Gesamttrainings, lassen sich Prozesse erproben, das Team-Setup testen und Optimierungspotentiale erkennen.

Während der Krise: Die Strategie ist entscheidend

Erfolgreiches Krisenmanagement beginnt bereits beim Issue Management. Erste Anzeichen einer möglichen Krise müssen frühzeitig erkannt und Maßnahmen eingeleitet werden. In einer Krisensituation ist die Kommunikationsstrategie entscheidend. Ziel ist es „vor die Lage zu kommen": nicht Getriebener von Medien und der Öffentlichkeit zu sein, sondern die Berichterstattung mit eigenen Botschaften mitzugestalten, Gerüchte frühzeitig zu unterdrücken und ausgewählte Botschaften an die wichtigen Zielgruppen zu senden.

Bei Cyberangriffen ist der Kommunikationszeitpunkt entscheidend

Kommunikationsziel ist es, den Cyberkriminellen den Wind aus den Segeln zu nehmen („stealing thunder"). Aber Vorsicht: Besonders bei unbedachten, zu schnellen Reaktionen besteht die Gefahr, dass unvollständige oder falsche Informationen herausgegeben werden, die Kommunikation vage wirkt und Vertrauensverlust droht. Eine frühe öffentliche Reaktion birgt zudem das Risiko, dass Angreifer gewarnt und mögliche Nachverfolgungen erschwert werden.

Nach der Krise: Manöverkritik und Reputationsaufbau

Ist eine Krise ausgestanden, ist eine Manöverkritik wichtig: Neben der Betrachtung der eigenen Prozesse und der Rollenverteilung ist darauf zu schauen, welche Medien wie berichtet haben, wie die Reaktionen auf internen und externen Kanälen zu bewerten sind und wie die Kommunikation mit anderen Stakeholdern lief. Ziel ist es, Optimierungsmöglichkeiten zu finden und Learnings für den nächsten Vorfall mitzunehmen. Zudem kommt es auf Maßnahmen an, die wieder Vertrauen und Reputation aufbauen. Dazu zählt eine fortlaufende Kommunikation zu möglichen nachgelagerten Auswirkungen der Krise und zu Maßnahmen zur Vermeidung ähnlicher Vorfälle. Letztlich sind auch das aktive Beenden der Krisenkommunikationsphase sowie der bewusste Übergang in die Regelkommunikation wichtig.

Der Autor

***Sebastian Riedel** ist Director bei Klenk & Hoursch AG, einer inhabergeführten Beratung für Kommunikation und Public Affairs. Er berät seit über zehn Jahren Unternehmen und Organisationen im Bereich der Krisenkommunikation – sowohl bei der Prävention wie auch im Krisenmanagement.*

Technologiegestütztes Vorfalls- und Krisenmanagement

Von Owen Miles

Damit Unternehmen wirksam auf Risiken reagieren können, müssen sie Technologie auf allen Ebenen einsetzen. Nur so können sie sicherstellen, dass Zwischenfälle nicht zu Krisen oder gar Katastrophen eskalieren. Wie sich die erforderliche Widerstandsfähigkeit schaffen lässt, zeigt dieser Beitrag am Beispiel einer internationalen Großbank.

Ob Klimawandel, extremes Wetter, Cyber-Angriffe, Unruhen oder Terroranschläge – Unternehmen müssen schnell und wirksam reagieren. Der Widerstandsfähigkeit von Unternehmen stehen jedoch viele Hindernisse entgegen: Teams sind in komplexe Prozesse eingebunden, häufig kommt es zu Konflikten zwischen Mitarbeitern, Standort, IT und Betrieb. Organisch wachsende Unternehmen sehen sich immer wieder mit einem veralteten Technologie-, System- und Prozesserbe konfrontiert und sind zu träge, daran etwas zu ändern („wir haben das schon immer so gemacht").

Besondere Herausforderungen stellen sich bei Übernahmen: Etablierte Teams mit etablierten Systemen und Prozessen wollen sich nicht ändern, werden aber plötzlich und häufig ohne Ankündigung zusammengebracht, denn das Geschäft darf nicht unterbrochen werden.

Wie lässt sich in dieser komplexen Gesamtlage sicherstellen, dass Vorfälle nicht zu einer Krise eskalieren? Wie können sich Unternehmen für den Umgang mit Bedrohungen rüsten?

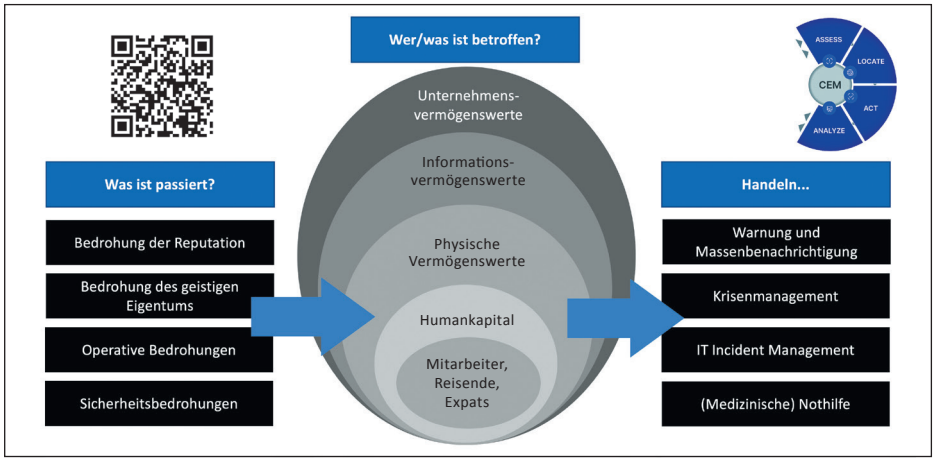
Risiken identifizieren und irrelevante Warnmeldungen vermeiden

Es gibt viele Herausforderungen beim Aufbau der erforderlichen Widerstandsfähigkeit: Unternehmen müssen zunächst wissen, was passiert oder passieren könnte, welcher Art die Bedrohungen sind, ob sie der Informationsquelle vertrauen können und welche Auswirkungen diese Bedrohung nicht nur auf die physische Präsenz, sondern auch auf die eventuell betroffenen Menschen und digitalen Systeme haben. Dazu müssen häufig mehrere Teams mit mehreren Systemen versuchen, Daten zusammenzuführen und diese Informationen auszutauschen, bevor eine Reaktion in Betracht gezogen werden kann. Die Gebäudemanagementteams müssen wissen, wo sich die Büros befinden, die Sicherheitsteams, wer sich im Gebäude befindet, die HR-Teams, wo die Mitarbeiter arbeiten, und die Betriebsteams müssen die Auswirkungen auf den Kunden kennen.

Eine internationale Großbank beispielsweise verfügte ursprünglich über eine Informationsfunktion, die sich in hohem Maße auf manuelle, hauptsächlich über E-Mails abgewickelte Prozesse stützte. Das Team musste täglich Hunderte von E-Mails aus verschiedenen Informationsquellen sichten, um potenziell gefährliche Ereignisse für Mitarbeiter, Filialen oder andere Vermögenswerte zu identifizieren. Nach der Identifizierung eines Risikos ermittelte das Team anhand von Karten die räumliche Nähe des Risikoereignisses zu verschiedenen Niederlassungen und erstellte eine manuelle Warnung, einen Hinweis oder eine vollständige Anweisung in Abhängigkeit vom Schweregrad dieses Risikos. Auf das Erkennen der Risiken folgte kein effizientes Verfahren zur Steuerung der Maßnahmen.

Klar war: Angesichts von Tausenden zu berücksichtigenden Mitarbeitern und Hunderten Anlagen benötigte das Unternehmen eine Lösung, die zeitaufwändige, inkonsistente und manuelle Prozesse abschaffte und die allgemeine Fähigkeit zur Verwaltung von Vorfällen optimierte.

Mit Technologie konnten die irrelevanten Warnmeldungen um 95 Prozent reduziert werden. Dazu wurde eine ausgeklügelte Filterung der Daten anhand einiger Schlüsselkriterien genutzt, nämlich Art, Schweregrad und Nähe der Bedrohung zu den Mitarbeitern und den Betriebsabläufen. Der Effekt: 2.000 tägliche Warnmeldungen wurden auf etwa 100 reduziert, die einer Triage unterzogen werden mussten. Wird tatsächlich eine Bedrohung erkannt, unterstützt das technologiegestützte Vorfalls- und Krisenmanagement bei der Reaktion.



Visualisierung des Unternehmensrisikos und der automatisierten Reaktionsabläufe in Echtzeit.

Anwendungsszenarien für das digitale Vorfalls- und Krisenmanagement

Eine entscheidende Komponente dabei ist die Zusammenführung von Daten, die die physischen Betriebsstandorte mit den physischen Standorten der Mitarbeiter zusammenbringt und mit vertrauenswürdigen Risikoinformationen kombiniert. Erfahrene Risikoinformationsmanager kategorisieren und klassifizieren diese Daten und ihre Korrelation in einer einzigen Technologielösung. Dies reduzierte die Zeit, die die Bank zum Erkennen einer Bedrohung brauchte, um 100 Prozent.

Das Wissen um eine Bedrohung ist nur eine Komponente, um einen Vorfall bewältigen und die Widerstandsfähigkeit des Unternehmens aufbauen zu können. Unternehmen müssen zudem Maßnahmen ergreifen und mit ihren Mitarbeitern kommunizieren, um ihnen die Reaktion zu erleichtern und zu ermöglichen – und zwar nicht nur innerhalb eines einzelnen Teams, sondern auch zwischen den Teams. Für viele Unternehmen ist das eine Herausforderung, die man im Falle der Großbank so ausdrückte: „Unsere Pläne waren nicht umsetzbar, und wir hatten Schwierigkeiten, den Fortschritt unserer Reaktion bei kritischen Ereignissen mit hohem Stressfaktor zu verfolgen." Durch die Digitalisierung und Operationalisierung dieser Pläne in einer Technologielösung, die die Integration von Kommunikations- und Vorfallsmanagement-Tools in dieselbe Datenaggregationsplattform ermöglicht, wird sichergestellt, dass Unternehmen nicht nur Bedrohungen erkennen, sondern auch vollständig orchestrierte Maßnahmen ergreifen können.

Das Aufbrechen von Silos mit Informationsbrücken zwischen verschiedenen Teams mithilfe einer Technologielösung ermöglicht Organisationen, zusammenzuarbeiten, um auf eine Bedrohung zu reagieren, aber auch, um die Prüfung und Rückverfolgbarkeit dieser Reaktion zu gewährleisten. Dies erfolgt nicht nur nach dem Ereignis in Form von Ereignisberichten, sondern vor allem während einer Situation, sodass Unternehmen den Kurs korrigieren können.

In der Praxis bedeutet dies die Erfassung, Zusammenführung und Korrelation aller verfügbaren Datenquellen, Risikoinformationen, Personaldaten, Standorte von Einrichtungen und Personen sowie digitaler Assets auf einer einzigen Plattform, die nicht nur Geolokalisierung und Visualisierung bietet, sondern vor allem in Reaktionsabläufe integriert ist. Warnungen und Benachrichtigungen werden ausgelöst, was die Reaktion auf Vorfälle und ihr Management ermöglicht – und letztlich die Widerstandsfähigkeit des Unternehmens und die Kunden unterstützt.

Der Autor

***Owen Miles** ist seit über 20 Jahren im Bereich Enterprise Resilience und Critical Event Management tätig. In den letzten 7 Jahren begleitete er über 800 Kunden dabei, ihre betriebliche Resilienz durch den Einsatz der CEM-Plattform von Everbridge zu stärken.*

***Everbridge, Inc.** bietet Enterprise-Software-Anwendungen, mit denen Organisationen die Reaktion auf kritische Ereignisse automatisieren und beschleunigen, sodass die Sicherheit von Menschen gewährleistet und der Geschäftsbetrieb aufrechterhalten wird.*

Entscheiden(d) in Krisen: Daten als Grundlage operativer Resilienz

Von Steve Richardson

In Krisensituationen – aber auch schon davor – geht es im geschäftlichen Kontext letztendlich um das Treffen bestmöglicher Entscheidungen. Das Aufbrechen bestehender Grenzen zwischen unterschiedlichen Funktionen wie Krisen-, Kontinuitäts-, und Risikomanagement führt zu umfassenden Lagebildern und einer besseren Informationsgrundlage – nicht nur für Krisenmanager, sondern über alle Führungsebenen hinweg.

Ich habe im vergangenen Jahr viele Unternehmen und Organisationen besucht und festgestellt, dass deren Programme auf dem Weg zur Erfüllung gesetzlicher, politischer und geschäftlicher Anforderungen in Bezug auf die operationelle Stabilität stark unterschiedliche Reifegrade aufweisen. Die Programme variieren deutlich in Bezug auf ihre Struktur und Sponsorship, Bewertungs- und Testverfahren, Abstimmung mit anderen Disziplinen, Werkzeuge und Standardisierung der Taxonomie.

Besonders auffällig sind die Unterschiede zwischen einzelnen Industrien: Vorreiter aufgrund der klar definierten regulatorischen Anforderungen ist der Banken- und Finanzdienstleistungssektor, der Konzepte und Rahmenwerke zur Absicherung der operationellen Resilienz entwickelt hat und anwendet. Diesem nah sind Organisationen und Unternehmen der kritischen Infrastruktur. Weitere Unternehmen und damit Industrien folgen, jedoch mit einigem Abstand. Trotz aller Unterschiede im Reifegrad ist die Zielsetzung jedoch meist sehr ähnlich:

- Erhöhung funktionsübergreifender Transparenz und des Wissens;
- Angleichung von Methoden, Metriken/Definitionen, Programmplänen und Bewertungspraktiken;
- Gewährleistung einer einheitlichen Organisation und Prozesstaxonomie.

Diese gemeinsamen Ziele führen zu der Notwendigkeit, die Konnektivität, Interaktion und Integration des Denkens in Bezug auf bestehende Risikodaten und -programme zu verbessern, da für eine optimale Krisenreaktionen schnellere und abgestimmtere Entscheidungen erforderlich sind. Fähigkeiten und einzelne Programme wie Business Continuity, Disaster Recovery, Cybersicherheit, Krisenmanagement, Unternehmenssicherheit, Risikomanagement, Compliance etc. bestehen jedoch in der Regel eigenständig und sind nicht umfassend integriert. Im Hinblick auf die Resilienz in Krisensituationen sind Teams, Daten und Messgrößen aufeinander abzustimmen – und Silos aufzubrechen. Erfolgreiche Unternehmen bilden Resilience-Hubs oder Plattformen, um eine gemeinsame Betriebssprache zu entwickeln und die notwendigen Verwaltungs-, Schutz- und Berichtsfunktionen für ihre wichtigsten Geschäftsfelder („Critical Business Services") zu vereinheitlichen.

Umsetzbare Erkenntnisse durch Datenautomatisierung und KI

In der Praxis bedeutet dies das Zusammenspiel proprietärer Methoden zur Risikoidentifikation mit tiefergehender Datenanalyse und -automatisierung. Die kombinierte Lösung hilft dem Unternehmen, Probleme über Personen, Prozesse, Technologien, Daten und Lieferketten hinweg zu identifizieren und zu lösen. Dabei müssen Daten aus verschiedenen Silos und Technologien innerhalb der Organisation aggregiert und in *umsetzbare* Erkenntnisse entwickelt werden, die zum Schutz der Organisation sowie zur Erfüllung von Markenversprechen des Unternehmens bei Geschäftsunterbrechungen genutzt werden können. Dabei sind folgende fünf Kriterien relevant:

> „Mit künstlicher Intelligenz vorausschauende Analysen und Simulationen erstellen"

1. Konnektivität – Eliminieren von organisatorischen Datensilos, um die Datenqualität und -effizienz zu verbessern.
2. Identifizieren und Priorisieren betrieblicher Abhängigkeiten und für die Widerstandsfähigkeit kritischer Daten und Assets.
3. Ganzheitliches Betriebsmanagement – Visualisieren von Schwachstellen im gesamten Unternehmen und Priorisieren von Investitionen in kritische Dienste, die sich direkt auf Kunden auswirken.
4. Stresstests – Automatisieren von End-to-End-Stresstests, um eine Modellierung potenzieller geschäftlicher Auswirkungen zu entwickeln.
5. Sichtbarkeit – Weiterentwicklung von Analysen und Business-Continuity-Plänen in umsetzbare geschäftliche Erkenntnisse.

Diese Kriterien finden sich auch in der Regulatorik, beispielsweise durch die britische FCA oder den europäischen Digital Operational Resilience Act (DORA) wieder. Von gesteigerter Bedeutung sind dabei die Sorgfaltspflicht und Risikoprüfung gegenüber Dritten.

Sowohl die geforderte Überwachung Dritter – gerade bei einer hohen Anzahl von Zulieferern und Dienstleistern – als auch das Zusammenbringen von Datenpunkten aus den bestehenden Silos wird nicht ohne den Einsatz fortschrittlicher Technologien möglich sein. KI (künstliche Intelligenz) und ML (maschinelles Lernen) werden eingesetzt, um vorausschauende Analysen zu erstellen und mit „Was-wäre-wenn"-Modellen datengesteuerte Simulationen zu unterstützen. Diese fortschrittlichen Technologien sind vor allem dann effektiv, wenn sie durch größere Mengen realer Daten ergänzt werden, die von Drittanbietern für die Überwachung von Risiken und Gefahren bereitgestellt werden.

***Steven Richardson** ist Chief Resilience Innovation Officer bei Fusion Risk Management.*

Verantwortung der obersten Führungsebene

Organisatorisch bilden Unternehmen die Integration von Unternehmensbereichen und Resilienzfunktionen häufig über die Einrichtung zentraler Lenkungsausschüsse ab, die – unter Einbindung der obersten Führungsebene – den „Tone from the Top" und das Zusammenführen der Daten definieren. Die organisatorische Umsetzung allein reicht jedoch nicht aus, um in Krisensituationen zu bestehen: Der Schlüssel zu umsetzbaren Erkenntnissen liegt in der Auswertung und Aufbereitung der aggregierten Datenmengen.

Durch eine weitgehende Automatisierung stehen Informationen schneller zur Verfügung und können so das Informationsdefizit in Krisensituationen verkleinern. Die Verlagerung der Auswertung in die Cloud und die Möglichkeit der Nutzung auch auf mobilen Endgeräten erhöht die Datenverfügbarkeit und macht eine Krisenreaktion unabhängiger von der Präsenz von Führungskräften. Die gemeinsame Datengrundlage, verbunden mit einer einheitlichen Betriebssprache ermöglicht eine höhere Sichtbarkeit von Problemen und Vorfällen, sodass potenzielle Krisen bereits frühzeitig identifiziert und die Reaktion darauf angemessen vorbereitet werden kann. Die damit einhergehende Befähigung zu datenbasierten Entscheidungen über alle Hierarchieebenen hinweg erhöht die operationelle Resilienz von Organisationen und unterstützt so deren erfolgreiches Krisenmanagement.

Der Autor

***Steven Richardson** ist Chief Resilience Innovation Officer bei Fusion Risk Management. **Fusion RM** ist laut Gartner und Forrester Wave Marktführer für Operational Resilience und Business Continuity Software.*