Ist die Sicherheit Ihres Unternehmens ausreichend geschützt?

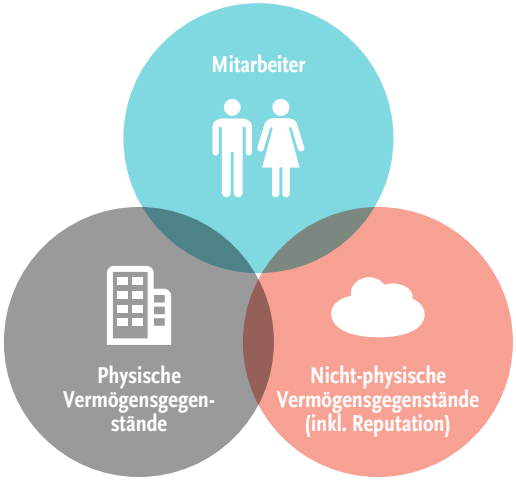
Sicherheits- und Krisenmanagement als Kern eines integrativen Risikomanagements

Die Komplexität externer und interner Bedrohungen für die Sicherheit von Unternehmen hat in den letzten Jahren stetig zugenommen. Nicht nur die gestiegene Terrorbedrohung, sondern auch Naturkatastrophen, Cyber-Attacken oder Compliance-Verstöße von Unternehmen oder Mitarbeitern stellen enorme Risiken für Unternehmen dar. Vorfälle in der Unternehmenspraxis haben gezeigt, dass ein ganzheitliches Risikomanagement den Schutz von Mitarbeitern, physischen und nicht-physischen Ressourcen sowie der Reputation des Unternehmens fokussieren muss. Allerdings haben diese Krisen auch bewiesen, dass falsche Handlungen und Reaktionen von Unternehmen diese Zieldimensionen häufig noch stärker gefährden. Derartige Verhaltensmuster verdeutlichen den Handlungsbedarf in der heutigen Unternehmenspraxis. Einzig durch ein integriertes Konzept, das alle Komponenten eines erfolgreichen Sicherheits- und Krisenmanagements abdeckt und über traditionelle Krisenkommunikation hinausgeht, kann diesen Entwicklungen vorgebeugt und im Krisenfall angemessen reagiert werden.

Warum ist Sicherheits- und Krisenmanagement aktuell relevant?

Obwohl Idee und Bedeutung von Sicherheits- und Krisenmanagement nicht neu sind, hat sich das Sicherheitsumfeld von Unternehmen in den letzten Jahren stark verändert. Somit rücken Sicherheitsmanagement und der Umgang mit Krisen auf die Agenda des Top-Managements. Nur durch den ganzheitlichen Schutz der Sicherheit von Mitarbeitern[1], physischen und nicht-physischen Vermögensgegenständen sowie der Reputation des Unternehmens **(► Abb. 01)**, können betroffene Unternehmen die steigenden Risiken aus Gesellschaft, Wirtschaft und Umwelt effektiv reduzieren. All dies darf jedoch nicht isoliert geschehen, sondern muss vielmehr in das übergreifende Risikomanagement integriert werden.

Abb. 01 Schutzobjekte eines ganzheitlichen Sicherheits- und Krisenmanagements



Der durch Terroranschläge verursachte weltweite wirtschaftliche Schaden ist seit 2010 um mehr als 300 Prozent gestiegen, wobei das Wachstum vor allem durch die Stärkung des Islamischen Staats (IS) im Irak und in Syrien vorangetrieben wurde [Vgl. Institute for Economics & Peace (IEP) 2017]. Besonders stark betroffen waren dabei die OECD-Mitgliedstaaten. Hier ist die Zahl der Todesfälle um 650 Prozent im Vergleich zum Jahr 2014 gestiegen, und die wirtschaftlichen Schäden haben sich seit 2011 verdreifacht [Vgl. Institute for Economics & Peace (IEP) 2017]. Folglich sind Sicherheitsfragen auch immer weiter in den Mittelpunkt der öffentlichen Diskussion gerückt. Vor allem aber die persönliche Haftung der Führungskräfte [Vgl. Werner 2017 zum Thema Dieselgate], sowie die steigenden Strafzahlungen und Reputationsschäden erhöhen den öffentlichen Druck auf Unternehmen, sich im unternehmerischem Sinn verantwortungsbewusst zu verhalten.

Diese Trends verdeutlichen, dass zeitgemäße Unternehmensführung auch bedeutet, sich kontinuierlich mit komplexen Sicherheitsfragen auseinanderzusetzen. Die Etablierung ganzheitlicher Präventions- und Reaktionsmaßnahmen ist zu einer unverzichtbaren Aufgabe für Unternehmen geworden, um Sicherheitsrisiken abzuschwächen, das Entstehen von Krisen zu vermeiden und diesen im Ernstfall angemessen gegenzusteuern. Dazu ist es notwendig, sich einer übergeordneten Risikostrategie zu verpflichten, die im Einklang mit der Unternehmensstrategie steht. Nur so kann Sicherheits- und Krisenmanagement nachhaltig in das übergreifende Risikomanagement integriert werden.

Viele aktuelle Praxisbeispiele zeigen, dass es zwar gute Ansätze im Bereich Sicherheits- und Krisenmanagement gibt, diese jedoch von diversen Schwachstellen, zumindest in der öffentlichen Wahrnehmung, überschattet werden. Bestimmte Verhaltensmuster können Umfang und Auswirkungen einer Krise noch verstärken. Zu diesen nachteiligen Verhaltensmustern in der Unternehmenspraxis zählen vor allem (1) langsame und inkonsistente Kommunikation in der Krisensituation selbst, (2) Silomentalität der Risikofunktionen, das heißt isoliertes Management von Sicherheitsrisiken, sowie (3) unklare Zuordnung von Rollen und Verantwortlichkeiten in der Organisation. Unternehmen ohne konkrete Sicherheitsvorfälle verzichten weitgehend auf die Einrichtung und Anwendung essentieller, präventiver Maßnahmen des Sicherheits- und Krisenmanagements. Dabei können Präventionen und der adäquate Umgang mit einer Krise letztendlich auch eine Chance für Unternehmen darstellen, positiv in der Öffentlichkeit und bei den Stakeholdern wahrgenommen zu werden.

Ziel dieses Artikels ist es, anhand von Fallbeispielen Komponenten eines effektiven Sicherheits- und Krisenmanagement abzuleiten und diese in ein einheitliches Risikomanagement-Framework zu überführen. Mithilfe dieses Frameworks können Sicherheitsfragestellungen ganzheitlich beantwortet und auch Chancen für das Unternehmen realisiert werden.

Wie erfolgt Sicherheits- und Krisenmanagement in der Praxis?

Amoklauf in Münchener Innenstadt

Während des Amoklaufs im Jahr 2016 im Münchener Olympia-Einkaufszentrum gab es mehrere Verletzte und neun Tote. Aufgrund des systematischen und effizienten Vorgehens der Polizei konnte das potenzielle Schadensausmaß jedoch frühzeitig minimiert und die Sicherheitslage kontrolliert werden. Bereits zu Beginn des Amoklaufs ging die Polizei von der höchsten Gefahrenstufe aus und koordinierte umgehend die Zusammenarbeit von Behörden, Unternehmen und öffentlichen Einrichtungen. Zudem bewahrte das zentrale Krisenmanagement-Team Ruhe und evaluierte systematisch Social-Media-Falschmeldungen zu angeblich zeitgleichen Terrorangriffen [Vgl. Oberhuber 2016].

Während des Amoklaufs führte die hohe Polizeipräsenz zu einer frühzeitigen

Deeskalation der Sicherheitslage. Regelmäßige Kommunikation und klare Argumentation von Kriseninterventionsmaßnahmen wirkten ferner der gesellschaftlichen Verunsicherung entgegen. Eine zentrale Krisenanlaufstelle (beziehungsweise Hotline) wurde eingerichtet und alle betroffenen Gruppen über zielgruppengerechte Kommunikationskanäle (beispielsweise Twitter) in verschiedenen Sprachen adressiert [Vgl. Oberhuber 2016].

Darüber hinaus nutzte die Polizei nach Beendigung des Amoklaufs weitere technische Methoden, auf die sie in ihrer Berichterstattung kontinuierlich hinwies. So konnten Betroffene z. B. über Social-Media-Kanäle anzeigen, dass sie in Sicherheit waren [Vgl. Oberhuber 2016].

Ölkrise im Golf von Mexiko

Die Explosion der Ölplattform Deepwater Horizon von British Petroleum (BP) im Jahr 2010 hatte mehrere Verletze, zehn tote Mitarbeiter sowie irreparable Umweltschäden zur Folge [Vgl. Valvi & Fragkos 2013]. Es entstand ein finanzieller Schaden von 20 Milliarden US-Dollar inklusive Sanierungskosten, Entschädigungen, Schadensersatz und Geldbußen [Vgl. Crooks 2010].

Die vermeintlichen Hauptgründe für die Krise waren regulatorische Verstöße zwischen 2005 und 2009, insbesondere die Nichteinhaltung verschiedener US-amerikanischer Umwelt-, Sicherheits- und Arbeitsschutzgesetze [Vgl. Qumer & Purkayastha 2010].

In der Krise führten bestimmte Verhaltensweisen, wie die Aussage „Betrachtet man die Größe des Golfs von Mexiko und seine gesamte Wassermenge, ist die Menge an ausgetretenem Öl winzig“ zu einer Zuspitzung der Krise und schadeten der Reputation des Unternehmens zusätzlich [Vgl. Valvi & Fragkos 2013]. Anstatt Verständnis und Stabilität zu vermitteln, entstand der öffentliche Eindruck eines rein profitorientierten Unternehmens, das 50 Millionen US-Dollar für Werbekampagnen ausgab, anstatt diese in die Reduzierung der Umweltschäden zu investieren [Vgl. Valvi & Fragkos 2013]. Zudem wurden Anregungen und Diskussionen von Mitarbeitern unterdrückt [Vgl. Valvi & Fragkos 2013]. Auch Gesundheitsprobleme der eigenen Mitarbeiter, die nachweislich durch die Beseitigung des Ölteppichs entstanden, wurden verharmlost.

Untersuchungen der Krisenursache ergaben, dass effiziente und erfolgreiche Eindämmungsmaßnahmen zusätzlich durch veraltete Technologien und Ausrüstungen erschwert wurden [Vgl. Crooks 2010]. Nach einem CEO-Wechsel und dem Eingeständnis der eigenen Versäumnisse hat BP die Einsichten genutzt, um ein wirkungsvolles und effizientes Sicherheits- und Krisenmanagement aufzubauen.

Brandkatastrophe Grenfell Tower

Der Großbrand im Londoner Grenfell Tower kostete 71 Bewohner ihr Leben und machte ein 24-stöckiges Wohngebäude unbewohnbar. Diese Katastrophe warf wichtige Fragen zur Planung, Bauweise und Sicherheit von Wohngebäuden auf [Vgl. Kahlweit 2017].

Als Ursache für den Brand wurde identifiziert, dass die Sicherheitsinspektionen und Brandrisikobewertungen über mehrere Jahrzehnte nicht den geforderten Mindeststandards von Industrieexperten entsprachen. Die Gründe hierfür waren zum einen die angestrebten Kostenersparnisse des Bauträgers und zum anderen die unzureichenden Brandschutzvorschriften der Behörden. Zwar forderte das Parlament mehrmals schärfere Auflagen, diese wurden vom Gesetzgeber jedoch nicht ausreichend umgesetzt [Vgl. Kirkpatrick, Hakim, & Glanz 2017]. So wurden feuergefährliche Materialien in den Gebäudefassaden verwendet und keine feuerhemmenden Türen im Gebäude installiert. Bei den Untersuchungen der Krisenursache stellte sich heraus, dass Bewohner wiederholt Bedenken bezüglich der Sicherheit des Gebäudes geäußert hatten. Diese wurden aber von der Mieterorganisation und den Behörden ignoriert [Vgl. Bertrand 2017]. Es fand somit keine ausreichende Überwachung statt, inwieweit der Bauträger seinen Pflichten nachkam.

Im Gegensatz zum fahrlässigen Sicherheitsmanagement von Bauträger und Behörden, wurde das schnelle und effiziente Krisenmanagement der Feuerwehr während des Großbrands gelobt. Trotz der mangelnden Sicherheitsinstallationen, wie fehlender Sprinkleranlagen oder Fluchtwege, konnten viele Bewohner gerettet werden [Vgl. Knapton & Dixon 2017]. Die intransparente und langsame Reaktion und Koordination von Behörden und Bauträgern Vor Ort sorgte jedoch zunehmend für Empörung in der Gesellschaft und bei den Opfern.

Obwohl dem Bauträger die Lizenz für Gebäudemanagement nach dem Großbrand entzogen wurde, entstand der öffentliche Eindruck, dass sich dieser und die Behörden der Verantwortung bzw. Haftung entziehen. Die Opfer und deren Angehörige wurden bis heute weder finanziell noch psychologisch ausreichend entschädigt bzw. behandelt [Vgl. Knapton & Dixon 2017].

Was sind die Erfolgsfaktoren und Elemente für ein smartes Sicherheits- und Krisenmanagement?

Die Praxisbeispiele zeigen, dass es bestimmte Erfolgsfaktoren für ein wirkungsvolles und effizientes Sicherheits- und Krisenmanagement gibt. Die klassischen Fallstricke sind in ► **Abb. 02** zusammenfassend dargestellt.

Die Beispiele verdeutlichen, dass Krisen- und Sicherheitsmanagementansätze häufig nicht über den heute erforderlichen Reifegrad verfügen und nicht regelmäßig auf der Agenda des Top-Managements auftauchen. Augenfällig ist, dass die meisten Krisen mit einem fehlenden Risikobewusstsein des Top-Managements einhergehen.

Es bedarf eines ganzheitlichen Ansatzes, der alle relevanten Stakeholder innerhalb einer Organisation einbezieht sowie in das bestehende Risikomanagement und dessen Strukturen integriert ist.

Um Sicherheitsrisiken ganzheitlich identifizieren, analysieren und mitigieren zu können, müssen Top-Management und beteiligte Risikofunktionen die Kernkomponenten eines Sicherheits- und Krisenmanagements aufeinander abstimmen sowie entlang eines klar definierten unternehmensweiten Risikoappetits gestalten. Nur so können Fallstricke vermieden und das Schadensausmaß von Sicherheitsrisiken minimiert werden. **(► Abb. 03)**

1. **Strategie und Reichweite** – Aus der übergeordneten Risikostrategie gilt es, die Rahmenbedingungen für das Steuern

von Sicherheitsrisiken abzuleiten. Diese Sicherheitsstrategie definiert nicht nur Ausmaß, sondern auch Zieldimensionen der Maßnahmen zum Schutz von Mitarbeitern, Reputation sowie Ressourcen des Unternehmens. Durch die Definition relevanter Schutzobjekte und Risikoquellen wird die Ausgestaltung der restlichen Dimensionen des Sicherheitskonzepts bestimmt. Um die strategischen Ziele nicht zu gefährden, muss die Sicherheitsstrategie aus der individuellen Unternehmensstrategie abgeleitet werden und in sich konsistent sein.

2. **Governance** – Im Rahmen des unternehmensweiten Risikomanagements müssen Rollen und Verantwortlichkeiten eindeutig funktionsübergreifend definiert und zugewiesen werden. Vor allem die konsistente Definition von Grundsätzen und Richtlinien, insbesondere Kommunikations- und Eskalationsrichtlinien, sowie die Integration multidisziplinärer Teams erleichtern die spätere Umsetzung deutlich.
3. **Präventions- und Reaktionsprozesse** – Definition und Abstimmung von Präventions- (beispielsweise Szenarioanalysen) und Reaktionsprozessen (beispielsweise Eskalationsmechanismen und Krisenkommunikation) können nicht nur die Wahrscheinlichkeit des Auftretens einer Unternehmenskrise, sondern auch ihr potenzielles Schadensausmaß minimieren. Beide Prozesse sind nicht vollständig voneinander trennbar. So können beispielsweise Lern- und Adaptionsprozesse nach überstandenen Krisen gleichzeitig als Input für die Prävention zukünftiger Krisen dienen.
4. **Enablers & Tools** – Effektive Enablers sind wirkungsvolle Mittel, um physische und Cyber-Risiken zu reduzieren. Auf technischer Ebene gehören hierzu vor allem IT-Systeme. Diese erleichtern den Informationstransfer sowie die Kommunikation zwischen sicherheitsrelevanten Organisationseinheiten und helfen, Unternehmensrisiken bereichsübergreifend zu identifizieren, zu analysieren und zu bewerten. Zu den effektivsten physischen Enablers und Tools zählen neben Überwachungs-, Alarm- und Zugangskontrollsystemen auch Sicherheitskontrollzentren oder Reaktions- und Eskalationshandbücher. Diese Maßnahmen maximieren die Effektivität und Effizienz von Sicherheitsmaßnahmen.
5. **Unternehmenskultur** – Die erfolgreiche Umsetzung des Sicherheits- und Krisenmanagements ist vor allem von der sicherheitsorientierten Mentalität bzw. dem Verhalten der Mitarbeiter abhängig. Durch entsprechende Schulungen und Coachings muss das Bewusstsein für die Notwendigkeit eines Verhaltenswandels im aktuellen Sicherheitsumfeld gestärkt werden. So können Silos zwischen verschiedenen Risikofunktionen aufgebrochen und auftretende Risiken ganzheitlich erfasst werden. Gleichzeitig muss der Verhaltenswandel durch entsprechende Anreizsysteme unterstützt werden.

Abb. 02 Klassische Fallstricke eines ganzheitlichen Sicherheits- und Krisenmanagements

Klassische Fallstricke

- Fehlende oder inkonsistente **Sicherheitsstrategie** sowie Unklarheit über zu priorisierende Sicherheitsquellen und Schutzgüter.
- Silo-Mentalität der Risikofunktionen sowie unklare Rollen und Verantwortlichkeiten in der **Organisation.**
- Isolierte und ineffiziente **Risikoprozesse** sowie Ableitung und Durchführung von Mitigierungsmaßnahmen.
- Inkonsistente Kommunikation mit internen und externen Stakeholdern und unzureichende **technische Unterstützung.**
- Geringe **Risikokultur** sowie erratische Schuldzuweisungen.

Abb. 03 Elemente eines ganzheitlichen Sicherheits- und Krisenmanagements

Unternehmen, die die aufgeführten Erfolgsfaktoren entlang der fünf Kernkomponenten beachten, können Krisen vorbeugen oder das Schadensausmaß deutlich reduzieren. Eine ganzheitliche Betrachtungsweise ist bei der Anwendung des Konzepts entscheidend, da einzelne Komponenten voneinander abhängig sind und nur in ihrer Gesamtheit eine effektive Wir-

kung erzielen. Letztlich müssen bei der Implementierung und Durchführung fortgeschrittener Präventionsmaßnahmen auch die zeitliche und finanzielle Effizienz des Sicherheits- und Krisenmanagements sowie die Integrierbarkeit in bestehende Geschäftsprozesse sichergestellt werden.

Ausblick: Was kommt auf Unternehmen in Zukunft zu?

Die Beispiele aus der Unternehmenspraxis verdeutlichen, dass die Bedrohung von Mitarbeitern, physischen und nicht-physischen Vermögensgegenständen sowie der Reputation stetig steigt. Dabei entstehen neben bekannten Risikoquellen (beispielsweise Terror oder Umweltkatastrophen) im Zeitalter der Digitalisierung viele neue Risiken, wie Cyber oder Data Security Risks. Gleichzeitig sind neben der steigenden Komplexität eines ganzheitlichen Sicherheits- und Krisenmanagements auch zunehmende Transparenzanforderungen sowie gesellschaftlicher und politischer Druck zu beobachten, sich im unternehmerischen Sinn verantwortungsbewusst zu verhalten. Bereits die aufgeführten Praxisbeispiele zeigen, dass gesetzliche Verstöße sowie fehlerhaftes Management von Risiken vermehrt zu hohen Strafen und Reputationsschäden von Unternehmen führen. Aufgabe der Zukunft wird sein, diese Herausforderungen und Risiken frühzeitig zu erkennen und entsprechende unternehmenskritische Entwicklungen zu verhindern. Die Funktion des Risikomanagements als zentrale Steuerungsfunktion wird immer wichtiger für Unternehmen, da Risiken komplexer werden, bereichs- und funktionsübergreifend auftreten und damit einer entsprechenden ganzheitlichen Steuerung bedürfen. Insbesondere ist eine kontinuierliche Überprüfung und Bewertung des Risikokatalogs und des Risikoappetits hinsichtlich neuer Risiken essentiell, um als Unternehmen auf das veränderte Umfeld stets adäquat vorbereitet zu sein. Hierfür ist es unabdingbar, im Vorfeld Maßnahmen zu definieren, um Risiken zu verhindern oder bei Eintritt dieser optimal und mit möglichst geringem Schadensausmaß zu reagieren. Darüber hinaus wird vor allem der „tone from the top“ beziehungsweise das sicherheitsorientierte Bewusstsein und Verhalten des Top-Managements weiter an Bedeutung gewinnen, um entsprechende Verhaltensweisen vorzuleben und im Unternehmen über alle Hierarchieebenen hinweg umzusetzen.

Die Integration des Sicherheits- und Krisenmanagements in das übergreifende Risikomanagement ist dabei notwendig, um eine angemessene und effiziente Steuerung aller relevanten Risiken zu erreichen. Durch den professionellen Umgang mit einer Krise kann ein Unternehmen nicht nur als Positivbeispiel in der Gesellschaft wahrgenommen werden, sondern vielmehr gestärkt aus der Krise hervorgehen. Nicht ohne Grund setzt sich das chinesische Schriftzeichen für Krise (危机) auch aus den Elementen „Gefahr“ und „Chance“ zusammen [Vgl. Ostasieninstitut 2017].

Quellenverzeichnis sowie weiterführende Literaturhinweise

Bertrand, P. (2017): Residents repeatedly warned Grenfell Tower management of fire risks. Abgerufen von http://www.euronews.com/2017/06/14/london-tower-fire-residentwarnings.

Crooks, E. (2010): BP „not prepared“ for deep-water spill. Abgerufen von https://www.ft.com/content/e1e0e21c-6e53-11df-ab79-00144feabdco.

Institute for Economics & Peace (IEP) (2017): Global Terrorism Index - Measuring and understanding the Impact of Terrorism.

Kahlweit, C. (2017): Untersuchungen zum Grenfell Tower kommen nicht voran. 1. Januar 2018, Süddeutsche Zeitung.

Kirkpatrick, D./Hakim, D./Glanz, J. (2017): Why Grenfell Tower Burned: Regulators Put Cost Before Safety. Abgerufen von https://www.nytimes.com/2017/06/24/world/europe/grenfell-tower-london-fire.html.

Knapton, S./Dixon, H. (2017): Eight failures that left people of Grenfell Tower at mercy of the inferno. Abgerufen von http://www.telegraph.co.uk/news/2017/06/15/eightfailures-left-people-grenfell-tower-mercy-inferno.

Oberhuber, N. (2016): Eine gute Figur. 23. Juli 2016, Zeit.

Ostasieninstitut (2017): Hochschule Ludwigshafen am Rhein. Ostasienlexikon, Krise Abgerufen von http://www.oai.de/de/wissen/ostasienlexikon/56-kkk/1569-krise.html.

Qumer, S./Purkayastha, D. (2010): BP's Continuing Safety Problems: The Gulf of Mexico Crisis. Abgerufen von http://icmrindia.org/casestudies/catalogue/Business%20Ethics/BECG116.htm.

Valvi, A./Fragkos, K. (2013): Crisis communication strategies: a case of British Petroleum. Industrial and Commercial Training(7), S. 383-391.

Autoren

Dr. Kai Brühl, Director im Bereich Strategic & Reputation Risk, Risk Advisory, **Maximilian Johnen**, Risk Advisory, **Steffen Eisele**, Risk Advisory, **Jennifer Groß**, Risk Advisory, alle Deloitte.

1 Hierbei lässt sich grundlegend zwischen Sicherheit [Security] vor externen, weniger kontrollierbaren Entwicklungen und internem Arbeitsschutz [Safety] unterscheiden. Im vorliegenden Artikel wird der Begriff Sicherheit für beide Aspekte verwendet.