Gut gewappnet für den Ernstfall

Key Facts

- Seit über 20 Jahren setzt sich die Verwaltungsberufsgenossenschaft (VBG) dafür ein, bei den Mitgliedsunternehmen das Bewusstsein für den Umgang mit Bedrohungen und Notfällen zu schärfen
- Die wichtigsten Präventionsinstrumente der VBG sind ein vollständig überarbeiteter Leitfaden zum Thema Notfallmanagement sowie ein begleitendes Seminar dazu
- Der neue Leitfaden legt den Fokus auf einen systematischen Ansatz zum Risiko- und Notfallmanagement

Autoren

↗ **Matthias Bludau**
↗ **Christof Radusch**
↗ **Hauke Burmann**

„Uns wird es schon nicht treffen“ – mit dieser Grundeinstellung wiegen sich viele Unternehmen in trügerischer Sicherheit. Unwetterlagen, Hackerangriffe, Pandemien, Stromausfälle oder Sabotageakte können Betriebe jäh vor große Herausforderungen stellen. Der VBG-Leitfaden „Umgang mit Bedrohungen und Notfällen“ hilft, Risiken frühzeitig zu erkennen und angemessen damit umzugehen.

Manche Ereignisse haben eine solche Tragweite, dass sie sich tief im kollektiven Bewusstsein einprägen. Dazu gehören unter anderem die Anschläge auf das New Yorker World Trade Center. Zu den Opfern des Terrorangriffs am 11. September 2001 zählten auch Beschäftigte deutscher Unternehmen, die sich damals in Auslandsbüros im südlichen Manhattan aufhielten.

Der dramatische Vorfall führte weltweit zu verstärkten Sicherheitsmaßnahmen an Flughäfen und öffentlichen Gebäuden wie etwa Konsulaten oder Militäreinrichtungen. Die Verwaltungs-Berufsgenossenschaft (VBG) reagierte ebenfalls umgehend auf die Vorfälle in den USA. Im ersten Schritt wurde eine zentrale Anlaufstelle (Hotline) eingerichtet, um eine optimale medizinische Behandlung und psychologische Betreuung der Betroffenen sowie sofortige finanzielle Hilfen für die Hinterbliebenen sicherzustellen. Im zweiten Schritt setzte die VBG eine bundesweite Arbeitsgruppe ein. Aufsichtspersonen aus verschiedenen Bezirksverwaltungen erarbeiteten gemeinsam Vorschläge, um Betriebe auch bei atypischen Gefährdungen durch die Prävention zu unterstützen.

Gezielte Beratung

Schnell wurde den Mitgliedern des VBG-Gremiums klar, dass kriegerische und terroristische Extremereignisse üblicherweise nicht Gegenstand der betrieblichen Betrachtung sein können. Dennoch wirken einschneidende Geschehnisse wie der 11. September, das Ahrtal-Hochwasser oder die Corona-Pandemie zumindest kurzfristig als Weckruf. Diese verdeutlichen den Unternehmen, dass auch sie direkt betroffen sein können, wie beispielsweise im Falle der Corona-Pandemie. Leider führt diese Erkenntnis oftmals jedoch nicht zu einer grundlegenden Bewusstseinsveränderung im Hinblick auf Bedrohungen. Ziel der Beratung für die Unternehmen soll es daher sein, Bedrohungen wie zum Beispiel Stromausfälle, Cyberangriffe, Starkregen, Spionage oder Pandemien (Zwischenfall und Notfall) immer wieder auf einem niederschwelligen Niveau anzusprechen.

Zu diesem Zweck erarbeitete die VBG einen Leitfaden für die Sicherheits- und Notfallorganisation, der im Jahr 2007 unter dem Titel „Zwischenfall, Notfall, Katastrophe“ erschien.

Inzwischen gibt es die dritte vollständig überarbeitete Auflage der Schrift mit dem neuen Titel „Umgang mit Bedrohungen und Notfällen – Risiken kennen und angemessen handeln“ sowie ein begleitendes Seminar dazu. Im Gegensatz zu den ersten beiden Auflagen, die eher maßnahmenorientiert waren (zum Beispiel hinsichtlich Security), legt der neue Leitfaden den Fokus auf einen systematischen Ansatz zum Risiko- und Notfallmanagement.

Der Nutzen liegt auf der Hand

Der erste Schritt in dieser Systematik ist, die Unternehmen für ein entsprechendes Risikobewusstsein zu sensibilisieren. Eigentlich liegt der Nutzen einer systematischen Vorgehensweise auf der Hand, denn ein Unternehmen kann auf diese Weise zum Beispiel

- wirtschaftliche Schäden begrenzen oder verhindern,
- Störungen im Arbeitsablauf vermeiden,
- Beschäftigte und Unternehmenswerte schützen,
- von günstigeren Konditionen bei Banken oder Sachversicherungen profitieren.

Aber nicht nur aus betriebswirtschaftlichen und ethischen Erwägungen ist diese Herangehensweise sinnvoll, sondern auch aus rechtlichen Gründen.

Bei der Recherche zu den rechtlichen Grundlagen stellte sich heraus, dass es neben den offensichtlichen Vorschriften, zum Beispiel den §§ 5, 9 und 10 des Arbeitsschutzgesetzes (ArbSchG), § 22 der DGUV Vorschrift 1 sowie der Störfall-Verordnung oder Managementsystemen in weiteren Gesetzen und Regelwerken, bereits eine Vielzahl von Anforderungen für den Umgang mit Bedrohungen und Notfällen gibt. Dazu zählen unter anderem:

DGUV Regel 100-001 „Grundsätze der Prävention“

Paragraf 22 (Notfallmaßnahmen): Der Unternehmer oder die Unternehmerin hat „die Maßnahmen zu planen, zu treffen und zu überwachen, die insbesondere für den Fall des Entstehens von Bränden, von Explosionen, des unkontrollierten Austretens von Stoffen und von sonstigen gefährlichen Störungen des Betriebsablaufs geboten sind“. Insbesondere die besagten Störungen sind dabei thematisch sehr weit gefasst. So wird unter anderem die Aufstellung von Notfallplänen für „unerwartete Situationen, zum Beispiel Amokfall“ gefordert. Beispielhaft werden in dieser DGUV Regel als Notfälle „Brand, Unfall, Einbruch, Überfall …“ genannt.

Technische Regel für Arbeitsstätten: ASR V3 „Gefährdungsbeurteilung“

Danach müssen in der Gefährdungsbeurteilung zur Nutzung von Arbeitsstätten auch „Situationen berücksichtigt werden, die vom Normalbetrieb abweichen, wie zum Beispiel Störungen, Stromausfälle oder extreme Witterungseinflüsse“. Darüber hinaus sind auch „Gefährdungen zu betrachten, mit denen zum Beispiel bei Bränden, Unfällen, Überfällen oder sonstigen Betriebsstörungen zu rechnen ist“. Auch in dieser Regelung findet sich mit der Formulierung „sonstige Betriebsstörung“ ein sehr weit gefasster Begriff.

VDI-Richtlinie 4062, Blatt 2, „Gefahrenabwehr bei lebensbedrohlichen Gewalttaten“

Die Richtlinie gilt für den Schutz von Menschen in Organisationen und Unternehmen sowie für Bildungseinrichtungen, Kindergärten und Veranstaltungen. Sie enthält Hinweise, die Verantwortliche in Unternehmen einhalten, vorhalten und organisieren sollten, wenn im Rahmen der Gefährdungsbeurteilung erkannt wird, dass die Gefahr von lebensbedrohlichen Gewalttaten besteht.

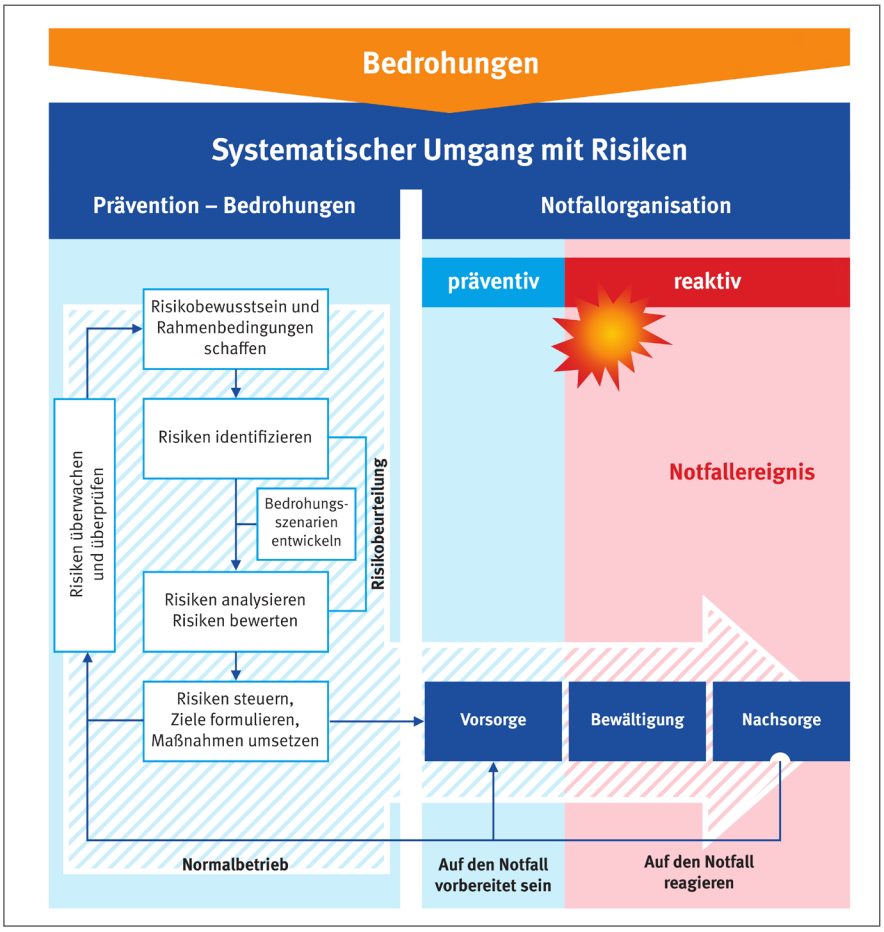
Die Auflistung zeigt das Dilemma für die Unternehmen, im Themenkomplex „Bedrohungen und Notfälle“ die relevanten Vorgaben zu überblicken und somit zu erfüllen.

Prozesse systematisch gestalten

Aber auch für die sonstigen betrieblichen Arbeitsschutzakteure, wie zum Beispiel Fachkräfte für Arbeitssicherheit oder Betriebsärztinnen und -ärzte scheint der Umgang mit den oben genannten Bedrohungen noch eher „Neuland“ zu sein. Bestätigt wird diese Wahrnehmung in der betrieblichen Beratung und Besichtigung der VBG. Im Rahmen der standardmäßigen Überprüfung der Arbeitsschutzorganisation wird auch die Gefährdungsbeurteilung überprüft. Dabei stellt sich in der Regel heraus, dass diese besonderen Bedrohungen keine Berücksichtigung finden. Es scheint den Unternehmen an konkreter Unterstützung für die Implementierung dieser Thematik in die betrieblichen Prozesse zu fehlen.

Bemerkenswert ist zudem, dass in der dritten GDA-Periode „Systembetrachtung“ unter dem Punkt „Notfallorganisation“ nur die Standardthemen „Erste Hilfe“, „Brandschutz“ und „Evakuierung“ abgefragt werden.

Mit der neuen Schrift hilft die VBG den Unternehmen herauszufinden, welche Risi-



Quelle: VBG

Abbildung 1: Systematischer Ansatz – Umgang mit Risiken

ken für sie relevant sein können und wie sie damit angemessen umgehen können.

Die Erfahrungen aus der Betriebsbetreuung und dem Seminar der VBG zu diesem Thema zeigen, dass die Betriebe schnell den Fokus auf die Notfallorganisation inklusive der Erstellung eines Notfallhandbuches legen. Dieser Ansatz greift zu kurz, da wichtige Prozessschritte fehlen.

Abbildung 1 erläutert die systematische Vorgehensweise.

Der Umgang mit Risiken im Sinne eines kontinuierlichen Verbesserungsprozesses (KVP) erfordert im ersten Schritt die Prävention gegen Bedrohungen und erst im zweiten Schritt die Notfallorganisation.

Nachfolgend werden die einzelnen Handlungsschritte erläutert.

Risikobewusstsein schaffen

Nachdem das entsprechende Risikobewusstsein bei der Unternehmensführung geweckt wurde, muss das Thema auch an Führungskräfte und Beschäftigte adressiert werden.

Rahmenbedingungen schaffen

Vom Unternehmen müssen personelle, finanzielle und zeitliche Ressourcen zur Verfügung gestellt werden.

Risiken identifizieren

Schlagwortartig sollen zunächst ergebnisoffen verschiedene Bedrohungen zum Beispiel mithilfe der Brainstorm-Methode benannt werden. Eine anschließende Clusterung ist sinnvoll.

Erfahrungen aus dem Seminar zeigen, dass tatsächliche Bedrohungslagen wie auch die subjektive Wahrnehmung sich ändern.

Bedrohungsszenarien entwickeln

Unter einem Szenario ist gemeinhin die bildhafte Darstellung/Beschreibung eines Risikos mit Annahmen über Abläufe und Auswirkungen von möglichen künftigen Ereignissen zu verstehen. Es zeigt in Kurzform auf, wie sich eine Bedrohung in einem Unternehmen auswirken kann.

Wozu braucht man Szenarien?

Zu vielen Bedrohungen gibt es kein Regelwerk im Vergleich zum normalen Arbeitsschutz. So lässt sich eine im Brainstorming erkannte Bedrohung, zum Beispiel „Hochwasser“, nicht ohne Weiteres bewerten. Häufig fehlen wichtige Hintergrundinformationen für die Bewertung der Bedrohungen und somit auch für die richtigen Maßnahmen. Zum Beispiel ist von entscheidender Bedeutung, die tatsächliche Ursache eines Hochwassers zu kennen: Starkregen, Schneeschmelze, Staudammbruch.

Ebenso spielt der zeitliche Verlauf eine entscheidende Rolle. Im Falle eines regionalen Starkregens kann ein Flusspegel sehr schnell – innerhalb von Stunden – steigen, während sich bei einer Schneeschmelze normalerweise ein Hochwasser über mehrere Tage entwickelt.

Zudem ist von Bedeutung, welche Bereiche im Unternehmen betroffen sein können. So kann beispielsweise das Wasser lediglich tiefer gelegene Areale oder Kellerbereiche überfluten oder sich auch auf Werkshallen ausdehnen.

Außerdem gilt noch abzuschätzen, welche Auswirkungen die Bedrohung auf betriebliche Prozesse hätte. Zum Beispiel: Welche möglichen Folgen hätte die Bedrohung für den betrachteten Betriebsbereich, wenn durch ein Starkregenereignis die Produktion für zwei Wochen ausfällt?

In der Praxis gestaltet sich dieser Prozess beispielsweise in den VBG-Seminaren für die Teilnehmenden schwieriger als gedacht. Teilweise fällt es schwer, ein konkretes zukünftiges Ereignis mit den dazugehörigen Abläufen für die bildhafte Szenariobeschreibung prägnant zu formulieren.

Verschiedene Ursachen, zeitliche Verläufe, Bereiche sowie Auswirkungen können zu einer Fülle von unterschiedlichen Szenarien führen. Diese führen wiederum zu sehr unterschiedlichen präventiven Maßnahmen, die im jeweiligen Fall zu ergreifen wären.

Es gibt in diesem Fall kein Richtig oder Falsch. Als praktikabler Weg hat sich die Beschreibung eines Worst-Case-Szenarios erwiesen. Darunter versteht man ein schlimmstmögliches, aber dennoch plausibles Szenario. Zum Beispiel:

Bei einem sommerlichen Starkregenereignis über mehrere Stunden steigt der Pegel eines nahe gelegenen Flusses um drei Meter. Das Wasser überflutet einen Betrieb im Uferbereich. Dort laufen die Keller voll und in der Produktionshalle steht das Wasser einen Meter hoch. Die hoch technisierte Produktion fällt für vier Monate aus, da Maschinen schwer beschädigt wurden und es keinen Ausweichstandort für die Produktion gibt.

Die Szenarien müssen berücksichtigen, welche Erfahrungen das Unternehmen bereits mit früheren Bedrohungen gesammelt hat und welche Schutzmaßnahmen aktuell vorhanden sind.

- **Problem 1:** Eine genaue Beschreibung der Auswirkungen wird nicht durchgeführt. Zum Beispiel: Wie lange genau ist die Produktion in dem Unternehmen unterbrochen?
- **Problem 2:** Mögliche komplexe Ereignisfolgen – auch „Kaskadeneffekte“ genannt – sollten nicht in einem Szenario gebündelt werden. Stattdessen empfiehlt es sich, diese in einzelnen Szenarien zu betrachten.

Ansonsten ist es nicht möglich, den nächsten Schritt der Risikoanalyse sinnvoll durchzuführen.

Subjektive Einschätzung

Bei der Risikoanalyse geht es darum, die Eintrittswahrscheinlichkeit und Schadensschwere einzuschätzen. Dies ist wichtig, um die Relevanz der einzelnen beschriebenen Szenarien für das Unternehmen erkennen zu können. Dafür ist als Hilfsmittel die Risikomatrix geeignet.

Bei der Einschätzung der Eintrittswahrscheinlichkeit helfen entweder Statistiken oder Branchenkenntnis. Bei der Schadens-

schwere gilt es in erster Linie zu verhindern, dass durch Ereignisse Menschen zu Schaden kommen.

In der Systematik dieser Schrift kann die Schadensschwere hingegen sowohl monetär (Produktionsausfall, Unterbrechung von Lieferketten et cetera) wie auch als Imageschaden (Unternehmen kann seine Leistungen nicht mehr erbringen) betrachtet werden.

Die Risikomatrix bezieht sich immer auf das im Betrieb schon vorhandene Sicherheitsniveau in Bezug auf die jeweilige Bedrohung. Wenn in einem Unternehmen beispielsweise ein Notstromaggregat vorhanden ist, das die Stromversorgung für zwei Stunden sichert, muss dies für das Szenario eines möglichen Stromausfalls in der Bewertung der Schadensschwere entsprechend berücksichtigt werden.

Die Risikomatrix hat jedoch auch ihre Tücken. So ist die Einschätzung der Eintrittswahrscheinlichkeit und der Schadensschwere fast immer nur subjektiv und relativ grob. Auch Wechselwirkungen mit anderen Risiken werden nicht unbedingt berücksichtigt. Nur für wenige Bedrohungen existieren fundierte und belastbare Erfahrungen und Erkenntnisse hinsichtlich der Eintrittswahrscheinlichkeit. Ein weiteres Problem ist, dass sich aus Ereignissen in der Vergangenheit häufig keine absolut zuverlässigen Schlussfolgerungen für die Zukunft ableiten lassen, da sich die Rahmenbedingungen sehr schnell ändern können.

Die Unternehmensgröße und Komplexität der Unternehmensprozesse bestimmen hierbei den Aufwand und die Vorgehensweise bei der Risikoanalyse.

Ein kleines Unternehmen mit wenigen Angestellten – zum Beispiel aus der IT-Branche – wird in der Regel keine ausgefeilte Risikoanalyse machen, sondern sofort entsprechende Maßnahmen zur Cybersicherheit umsetzen. Dabei werden wesentliche Handlungsschritte übersprungen mit dem Risiko, relevante Bedrohungen außer Acht zu lassen.

Umgang mit dem Risiko

Bevor (Schutz-)Ziele festgelegt und Maßnahmen abgeleitet werden, sollten Überlegungen zum Umgang mit dem jeweiligen Risiko im Betrieb angestellt werden. Dies entspricht der Risikosteuerung, wobei verschiedene Möglichkeiten bestehen.

Risikovermeidung

Beispiel: Das Unternehmen zieht aus der hochwassergefährdeten Flussaue in einen höher gelegenen Bereich um.

Risikoakzeptanz

Beispiel: Das letzte „Jahrhundert-Hochwasser“ war vor über 20 Jahren. Das Unternehmen verlässt sich darauf, dass das nächste Hochwasser dieser Art in absehbarer Zeit wohl nicht eintreten wird. Außerdem soll der Betrieb in drei Jahren ohnehin an einen anderen Ort umziehen.

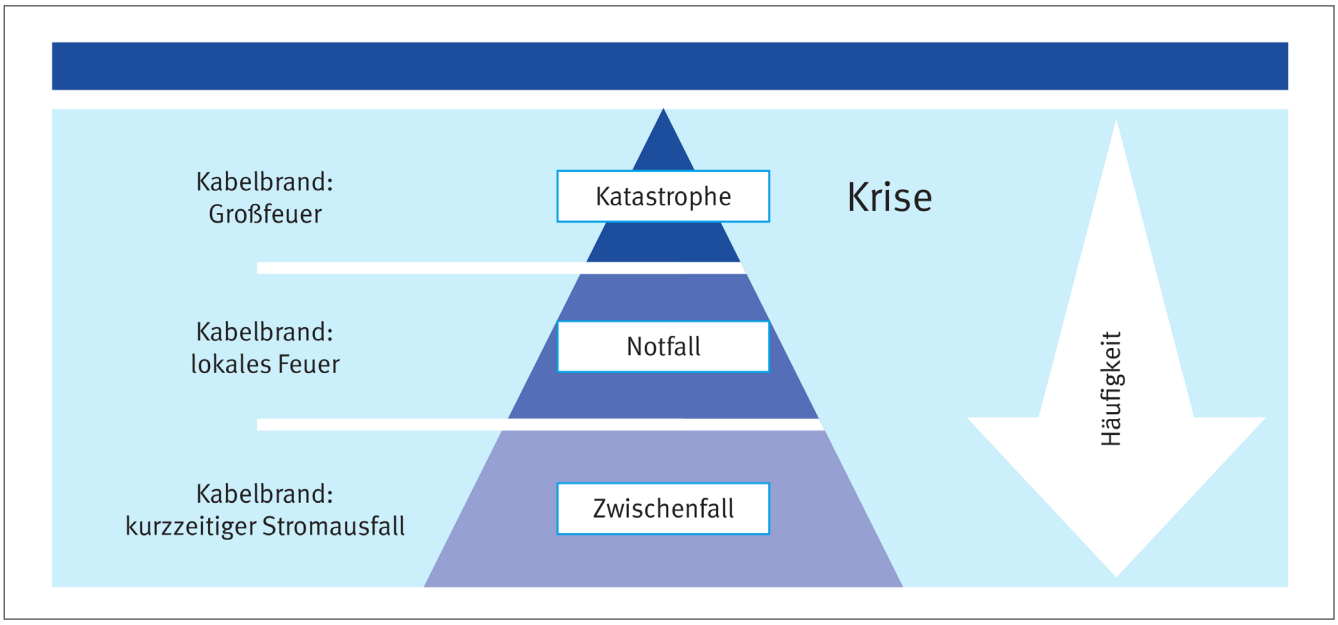
Hierin besteht ein Unterschied zum Arbeitsschutzrecht. In einem Bereich, der nicht gesetzlich geregelt ist, hat das Unternehmen die Wahl, sich individuell zu entscheiden – sofern dadurch Beschäftigte nicht gefährdet werden.

Risikoüberwälzung

Beispiel: Das Unternehmen schließt für die Bedrohung durch Hochwasser eine geeignete Elementarschadenversicherung ab, sofern diese im jeweiligen Gebiet verfügbar ist.

Risikoverminderung

Beispiel: Das Unternehmen wird mit speziellen Maßnahmen gegen Hochwasser bis zu einer bestimmten Höhe gesichert (zum Beispiel durch den Einsatz von Sandsäcken).



Quelle: VBG

Abbildung 2: Ereignishorizont – Darstellung der Ereignisstufen

Nach der Risikosteuerung wird im nächsten Schritt geprüft, inwiefern die Notfallorganisation zum Einsatz kommt.

Auf den Notfall vorbereitet sein

Bei der Notfallorganisation gilt grundsätzlich: Risiken sind nicht immer oder vollständig beherrschbar und meist verbleiben Restrisiken. Diese können trotz aller Maßnahmen zur Risikovermeidung oder -minimierung bei geringer Eintrittswahrscheinlichkeit erhebliche Auswirkungen haben.

Denkbar ist auch, dass einzelne Bedrohungen unzureichend eingeschätzt oder diese bis dato gar nicht erkannt wurden. Somit muss trotzdem damit gerechnet werden, dass es in einem Unternehmen zu unerwünschten Ereignissen kommt. Diese können – je nach Schwere des Ereignisses – prinzipiell in drei verschiedene Kategorien eingeteilt werden: Zwischenfall, Notfall und Katastrophe. Dieses Spektrum kann als Ereignishorizont bezeichnet werden.

Dieser Ereignishorizont ist in jedem Unternehmen und in jeder Branche spezifisch und muss deswegen an die Situation angepasst festgelegt werden. Auch die Dauer des Ereignisses kann eine Rolle spielen – ein längerfristiger Systemausfall hat umfassendere Auswirkungen als ein kurzfristiger.

Notfallvorsorge

Bei der Notfallorganisation gilt es, gut vorbereitet zu sein, falls ein Notfallereignis doch stattfinden sollte (Notfallvorsorge). In gewissen Bereichen wie Brandschutz, Erste Hilfe oder Evakuierung sind die erforderlichen Maßnahmen bereits gesetzlich geregelt. Die dort zugrunde liegende Systematik gilt es auch auf die Bereiche zu übertragen, für die es noch keine verbindlichen Vorgaben gibt. So kommt es beispielsweise im Bereich der IT-Sicherheit auch bei kleinen und mittleren Unternehmen vermehrt zu Hackerangriffen. Für einen solchen Fall gilt es Vorbereitungen zu treffen, um im entscheidenden Moment schnell handeln zu können. So müssen im Vorfeld beispielsweise Überlegungen zu folgenden Maßnahmen angestellt werden:

- Umgang mit potenziell betroffenen IT-Systemen
- Information von Beschäftigten, Kunden, Kundinnen und Behörden
- Aufrechterhaltung der Handlungsfähigkeit des Unternehmens

Bei vielen Notfällen ist die Zeitschiene ein wesentlicher Faktor, der beispielsweise bei längeren Zeit- und Ereignishorizonten auch eine längere Reaktionszeit für koordinierte Handlungen lässt. Dies gilt allerdings nicht für plötzlich eintretende Ereignisse ohne Vorwarnzeit. Bei der Notfallvorsorge gilt es Folgendes zu beachten:

- Abläufe detailliert beschreiben
- Informationsfluss und Alarmierungswege festlegen und sicherstellen
- verantwortliche Personen benennen
- notwendige Qualifizierung sicherstellen
- Personal zur Notfallbewältigung einplanen
- mit externen Partnern abstimmen
- Einrichtungen und Einsatzmittel zur Verfügung stellen
- Information und Training von Führungskräften und Beschäftigten einplanen
- Thema „Notfälle“ regelmäßig im Unternehmen ansprechen
- Maßnahmen zur Notfallorganisation in vorhandene Betriebsabläufe integrieren (wie Unternehmenspolitik, Personal-, Technologie-, Gebäudemanagement, Beschaffung, Prozess- und Projektmanagement)
- psychische Hilfe bei Extremsituationen einplanen

Notfallbewältigung

Voraussetzung für eine erfolgreiche Notfallbewältigung ist es, die entsprechenden Abläufe für das jeweilige Ereignis regelmäßig im Unternehmen zu üben. Hierfür gibt es verschiedene Methoden, wie zum Beispiel Unterweisungen, Planspiele oder Praxisübungen.

Notfallnachsorge

Ist es zu einem Notfallereignis im Betrieb gekommen, sollte überprüft werden, ob die Maßnahmen der Notfallvorsorge und -bewältigung gegriffen beziehungsweise welche Schwachstellen sich ergeben haben. Das Prinzip ist vergleichbar mit der Wirksamkeitsprüfung bei der Gefährdungsbeurteilung.

Aus eskalierenden Notfallereignissen oder Katastrophen können sich Krisen ergeben, die Leben bedrohen und/oder zu einer existenzbedrohenden Extremsituation führen können (siehe Abbildung 2). Die Notfallorganisation reicht in vielen Unternehmen oft nicht aus, um Krisen zu bewältigen.

Der Umgang mit Krisen erfordert üblicherweise eine besondere Organisationsstruktur, die aber in der Regel nur in größeren Betrieben möglich und sinnvoll ist. Kleinere Firmen können auch in Krisen geraten. Sie haben aber wegen fehlender Ressourcen oft nicht die Möglichkeit, eine eigene Organisationsstruktur zur Bewältigung der Krise aufzubauen. Da bei ihnen die Entscheidungswege oft kurz sind, ist dies in der Regel auch nicht erforderlich. In kleinen Betrieben übernehmen oft der Unternehmer oder die Unternehmerin und Führungskräfte diese Aufgabe. Je nach Komplexität und Schwere des Ereignisses sind diese aber ohne Expertise den Aufgaben möglicherweise nicht gewachsen.

Neben der Notfallorganisation und dem Krisenmanagement ist es wichtig, wie der Betrieb nach Ereignissen mit erheblicher Schadensschwere möglichst schnell verlorene kritische Betriebsfunktionen wiederherstellen und somit zum Normalbetrieb zurückkehren kann. Hiermit befasst sich das Kontinuitätsmanagement oder auch Business Continuity Management (BCM).

Dazu gehören folgende Schritte:

- Auswahl der kritischen Geschäftsprozesse
- Schadensanalyse
- Festlegung der Wiederanlaufparameter
- Festlegung der Ressourcen für den Normalbetrieb und den Schadensfall (Notbetrieb)

Nach der intensiven und präventiven Auseinandersetzung mit den möglichen Bedrohungen und der Notfallorganisation ist es sinnvoll, die wesentlichen Informationen in einem Notfallhandbuch zu bündeln. Dieses hilft dabei, die Prozesse weiter zu systematisieren, idealerweise einen schnellen Überblick zu gewinnen und eine zügige Reaktion zu ermöglichen. Das Notfallhandbuch unterstützt Führungskräfte und die für die Notfallbewältigung verantwortlichen Personen. Das Notfallhandbuch ergänzt und präzisiert die Gefährdungsbeurteilung.

Interne und externe Unterstützung

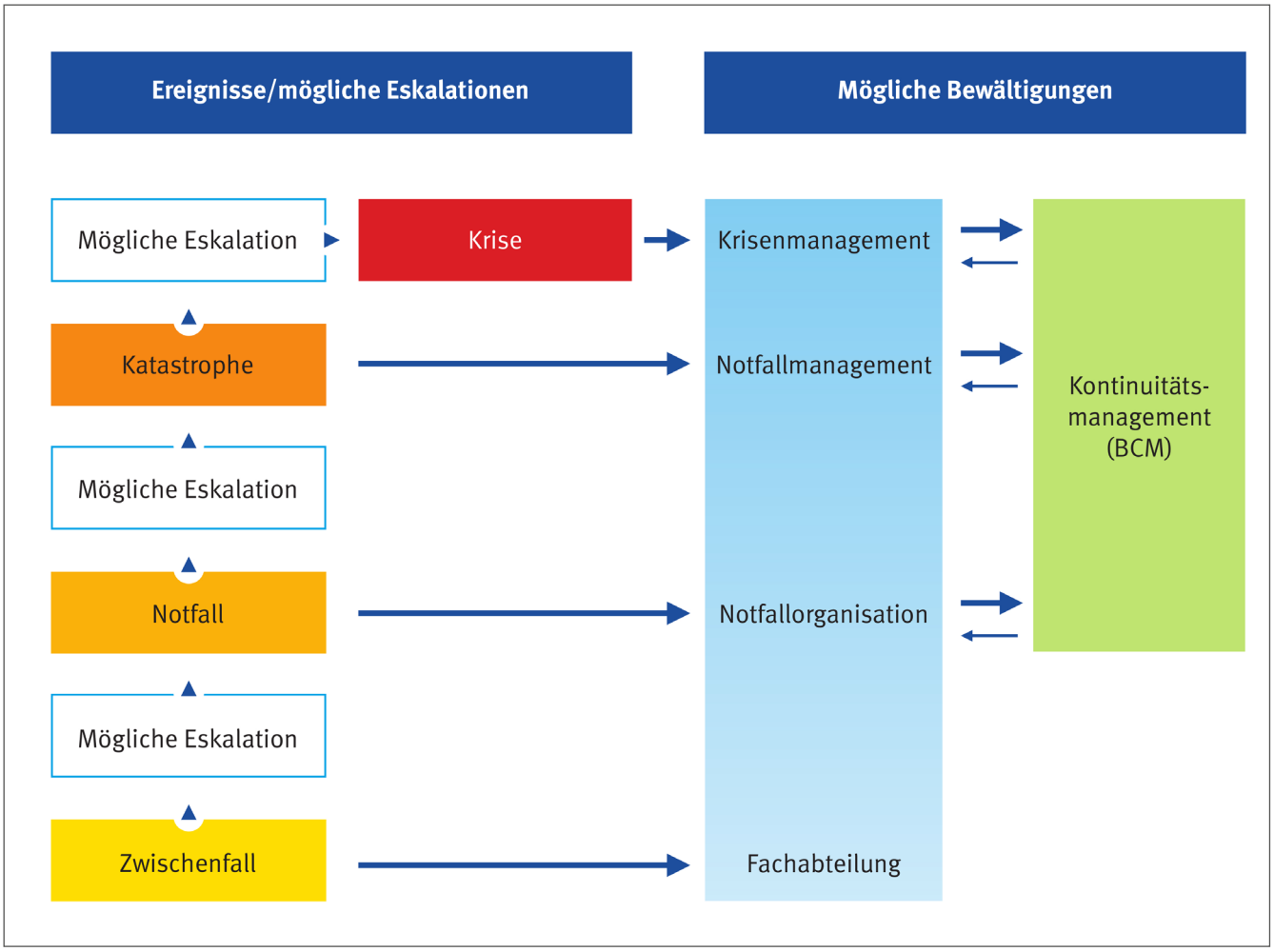
Aufgrund der Vielzahl möglicher Bedrohungen können Unternehmerinnen und Unternehmer nicht alle relevanten Fakten selbst zusammentragen und entsprechende Maßnahmen ableiten. Die üblichen Akteurinnen und Akteure des Arbeitsschutzes verfügen hierfür meist nicht über die entsprechende Expertise. Deshalb kann es sinnvoll sein, im Unternehmen auch die Funktion eines Risiko- und Notfallmanagers beziehungsweise einer Risiko- und Notfallmanagerin zu schaffen. Zudem kann es ratsam sein, zusätzlich fachliche Unterstützung bei Behörden und Organisationen zu suchen. In der VBG-Publikation werden beispielhaft Institutionen benannt.

Fazit

Extreme Wetterereignisse infolge des Klimawandels und sonstige Naturgefahren, Cyberangriffe, Pandemien, Sabotageakte, Spionagevorfälle, Stromausfälle und Gewalttaten: Hinter all diesen Bedrohungen verbergen sich sehr komplexe Themenfelder, mit denen sich Unternehmen – je nach Branche – systematisch auseinandersetzen sollen.

Die betriebliche Praxis im Aufsichtsdienst zeigt jedoch, dass es den Unternehmen dabei oft noch am Wissen, an der Motivation und Unterstützung fehlt. Die Unfallversicherungsträger können hier im Rahmen ihrer Präventionsleistungen einen wichtigen Beitrag leisten, um die Unternehmen branchenspezifisch bei dieser Aufgabe zu unterstützen.

Die VBG liefert mit der aktualisierten Schrift „Umgang mit Bedrohungen und Notfällen“ sowie dem Seminar zu dieser Thematik einen Beitrag im Bereich der Präventionsleistungen „Information“ und „Qualifizierung“.



Quelle: VBG

Abbildung 3: Vom Zwischenfall zur Katastrophe – Bewältigungsstrategien in Abhängigkeit der Eskalationsstufe