VBG
Ihre gesetzliche Unfallversicherung

VBG-Fachwissen

Umgang mit Bedrohungen und Notfällen

Risiken kennen und angemessen handeln

Die in dieser Publikation enthaltenen Lösungen schließen andere, mindestens ebenso sichere Lösungen nicht aus, die auch in Regeln anderer Mitgliedstaaten der Europäischen Union oder der Türkei oder anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum ihren Niederschlag gefunden haben können.

VBG – Ihre gesetzliche Unfallversicherung

Die VBG ist eine gesetzliche Unfallversicherung und versichert bundesweit knapp 1,5 Millionen Unternehmen aus mehr als 100 Branchen – vom Architekturbüro bis zum Zeitarbeitsunternehmen. Ihr Auftrag ist im Sozialgesetzbuch festgeschrieben und teilt sich in zwei Hauptaufgaben: Die erste ist die Prävention von Arbeitsunfällen, Wegeunfällen, Berufskrankheiten und arbeitsbedingten Gesundheitsgefahren. Die zweite Aufgabe ist das schnelle und kompetente Handeln im Schadensfall, um die ganzheitliche Rehabilitation der Versicherten optimal zu unterstützen. Im Jahr 2020 wurden knapp 360.000 Unfälle und Berufskrankheiten registriert. Die VBG betreut die Versicherten mit dem Ziel, dass die Teilhabe am Arbeitsleben und am Leben in der Gemeinschaft wieder möglich ist. 2.300 VBG-Mitarbeiterinnen und -Mitarbeiter kümmern sich an elf Standorten in Deutschland um die Anliegen ihrer Kunden und Kundinnen. Hinzu kommen sieben Akademien, in denen die VBG-Seminare für Arbeitssicherheit und Gesundheitsschutz stattfinden. Verstärkt bietet die VBG auch Web-Seminare zur ortsunabhängigen Weiterbildung an.

Weitere Informationen: **www.vbg.de**

VBG
Ihre gesetzliche Unfallversicherung

Umgang mit Bedrohungen und Notfällen

Risiken kennen und angemessen handeln

Version 1.0/2022-01

Inhaltsverzeichnis

Abbildung 1: Bedrohung – was kann das sein?

Vorwort

Unvorhergesehene Ereignisse, Bedrohungen und Notfälle kommen oft schneller als erwartet und können Ihr Unternehmen plötzlich vor große Herausforderungen stellen. Dieser Leitfaden hilft Ihnen herauszufinden, wie Sie viele Risiken frühzeitig erkennen und wie Sie angemessen damit umgehen können. Die Informationen richten sich in erster Linie an Unternehmerinnen und Unternehmer in kleinen und mittleren Betrieben, bieten aber auch Führungskräften, Expertinnen und Experten sowie Interessenvertretungen in größeren Unternehmen eine Orientierung. Diese Schrift bietet eine Grundlage für ein Risikomanagement von Bedrohungen und Notfällen.

Der Leitfaden zeigt auf, wie Sie systematisch und präventiv vorgehen können, um auf Bedrohungen und Notfälle vorbereitet zu sein. Weitergehende Praxishilfen und Informationen, mit denen Sie die Hinweise des Leitfadens in Ihre betriebliche Planung und Ihre Abläufe integrieren können, finden Sie auf der Internet-Themenseite www.vbg.de/bedrohungen-und-notfaelle.

Die vorliegende Schrift konzentriert sich auf die Risiken sicherheitsrelevanter Bedrohungen und geht bewusst nicht auf Markt-, Finanz- und Vertragsrisiken ein.

Wussten Sie, …

… dass gerade kleinere Unternehmen von Angriffen betroffen sind? Zwei Drittel der Unternehmen mit zehn bis 99 Beschäftigten waren Opfer von Spionage, Sabotage und Datendiebstahl.

(Quelle[1]: Bitkom, siehe Quellenverzeichnis, Seite 70)

1

1 Der Umgang mit Unsicherheit

Beschäftigung mit dem Thema Bedrohung und Notfall für den Betrieb

1.1 Gefahren – plötzlich und unerwartet

„Uns wird es schon nicht treffen“ – diese gängige Meinung ist immer wieder von Unternehmen zu hören, wenn es um Bedrohungen unterschiedlicher Art geht. Doch die Realität spricht leider eine andere Sprache. Schlagzeilen aus verschiedenen Medien zeigen, wie vielfältig das Gefahrenpotenzial ist, dem Unternehmen und ihre Beschäftigten im Alltag ausgesetzt sind.

„Bundesweite Serie von Bombendrohungen“

Quelle: www.tagesschau.de, 13.03.2019

„Wie Cyberkriminelle Konzerne erpressen“

Quelle: www.tagesschau.de, 11.11.2020

SICHERHEIT AM LANDRATSAMT HAT OBERSTE PRIORITÄT

„Nach der Geiselnahme in Pfaffenhofen: Gesellschaft verroht zunehmend“

Quelle: www.merkur.de, 07.11.2017

„Lingen: Es brannte doch im nuklearen Bereich“

Quelle: www.ndr.de, 10.12.2018

BRAND IM CHEMPARK

„Explosion in Leverkusen: Risiken an allen Ecken und Enden in Deutschland“

Quelle: www.ingenieur.de, 30.07.2021

„Experten warnen vor Terrorangriff mit Biowaffen nach Corona-Vorbild“

Quelle: www.welt.de, 25.05.2020

„Flutschäden bei Unternehmen: Viele stehen vor den Trümmern ihres Lebenswerks“

Quelle: Redaktionsnetzwerk Deutschland (www.rnd.de), 22.07.2021

„Leitung gekappt: Vodafone-Kunden in SH haben keinen Empfang“

Quelle: www.shz.de, 09.11.2017

„Hamburgs Norden lahmgelegt: Grund für Mega-Strompanne gefunden“

Quelle: Hamburger Morgenpost (www.mopo.de), 30.05.2017

GEFAHR IM LUFTRAUM

„Drohnen flogen 88-mal zu dicht an Flugzeuge“

Quelle: www.spiegel.de, 10.01.2018

„Zugunglück in Meerbusch mit über 40 Verletzten: Gutachten deckt fatale Fehler auf“

Quelle: www.derwesten.de, 16.10.2018

„Bei Bauarbeiten: Blindgänger in Münster explodiert“

Quelle: Redaktionsnetzwerk Deutschland (www.rnd.de), 08.09.2020

„Schnee-Chaos: Lawinen treffen Bundesstraße und Hotel“

Quelle: www.abendzeitung-muenchen.de, 14.01.2019

DARMSTADT

„Menschen mutmaßlich an Universität vergiftet – Ermittlungen wegen versuchten Mordes“

Quelle: www.spiegel.de, 24.08.2021

„Wohl hoher Millionenschaden nach Tornado im Landkreis Aurich“

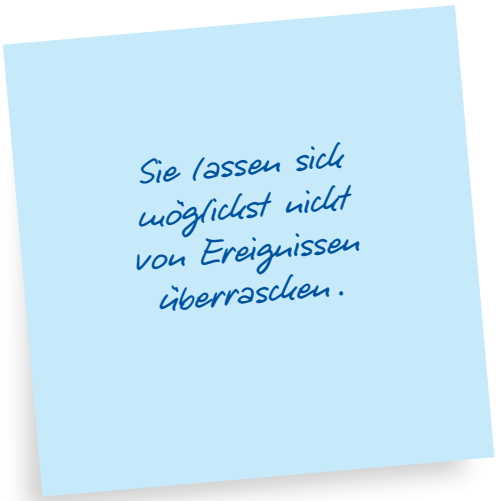
Quelle: www.ndr.de, 18.08.2021

AMOKLAUF MIT ELF TOTEN ERSCHÜTTERT HANAU

„Eine fassungslose Stadt“

Quelle: Gelnhäuser Neue Zeitung (www.gnz.de), 20.02.2020

1



1.2 Nutzen eines systematischen Umgangs mit Bedrohungen

Da Bedrohungen verschiedenster Art jedes Unternehmen praktisch immer treffen können, sollten Sie die damit verbundenen Risiken kennen und sich damit auseinandersetzen.

Im Mittelpunkt steht zunächst die Frage, welche Bedrohungen (siehe Kasten unten) für Sie relevant sein können. Die Vorteile einer solchen Risikobetrachtung sind unter anderem:

- Sie lassen sich möglichst nicht von Ereignissen überraschen.
- Sie bleiben immer „Herr und Frau des Verfahrens“, da Sie vorbereitet sind und auch in Ausnahmesituationen wissen, was zu tun ist.
- Sie kommen Ihrer Fürsorgepflicht gegenüber Ihren Beschäftigten nach, da Sie eventuellen Gesundheitsgefahren und Unfällen vorbeugen.
- Sie begrenzen oder verhindern vermeidbare wirtschaftliche Schäden und Störungen im Arbeitsablauf sowie schützen Beschäftigte und Unternehmenswerte.
- Sie sichern den Bestand Ihres Unternehmens, da Sie auf Bedrohungen und Notfälle vorbereitet sind – Sie haben zum Beispiel Maßnahmen zur Bewältigung der Auswirkungen von Pandemien eingeplant.
- Sie haben die Risikobetrachtungen in Ihr Führungshandeln integriert und haben so einen überschaubaren und kalkulierbaren Zusatzaufwand.
- Sie können weitgehend sicher sein, dass Sie auch im Bereich der Bedrohungen und Notfälle relevante Vorschriften zum Arbeitsschutz einhalten.
- Sie können gegenüber Banken und Versicherungen nachweisen, dass Sie auf Risiken durch mögliche Bedrohungen und Notfälle vorbereitet sind und etwaige Restrisiken im Blick haben. Dadurch können Sie auch mögliche Prämien der Versicherungen nutzen oder von Förderprogrammen profitieren (siehe Förderdatenbank des Bundeswirtschaftsministeriums, www.foerderdatenbank.de).
- Sie können in Versicherungsfällen leichter dokumentieren, dass Sie präventiv gehandelt haben und Ihren Sorgfaltspflichten nachkommen.

Wussten Sie, …

… dass in den vergangenen 40 Jahren in Deutschland die Anzahl der Starkniederschlagsereignisse und deren Intensität um 25 Prozent gestiegen ist?

(Quelle[2]: Deutscher Wetterdienst, siehe Quellenverzeichnis)

Begriffsklärungen

Bedrohung: Potenzielle Quelle eines Risikos, die zu einer ungünstigen Entwicklung führen kann. Das Gegenteil der Bedrohung ist die Chance.

Gefahr: Potenzielle Quelle eines Risikos, die zu einem plötzlich eintretenden Schadensereignis führen kann.

Gefährdung: Gefahr, die sich negativ auf Personen (auch Sachen oder Ziele) auswirken kann.

Risiko: Die Kombination aus der Wahrscheinlichkeit und Häufigkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit. Die Auswirkungen können positiv oder negativ sein.

Zwischenfall: Ein Zwischenfall ist ein Ereignis mit einem geringen Schadensausmaß (Störung). Zwischenfälle können in der Regel im allgemeinen Tagesgeschäft behoben werden. Sie können sich zu jedoch auch einem Notfall ausweiten. Zwischenfälle kommen relativ häufig vor.

Notfall: Ein Notfall ist ein Ereignis mit hohem Schadensausmaß. Notfälle können sich zu einer Katastrophe ausweiten. Notfälle treten nur selten auf.

Katastrophe: Eine Katastrophe ist ein Ereignis mit extremem Schadensausmaß, das stark über die Ausmaße von Schadensereignissen, wie zum Beispiel Notfälle, hinausgeht und dabei Leben, Gesundheit, Sachgüter oder wichtige Infrastrukturen erheblich gefährdet oder zerstört. Katastrophen kommen äußerst selten vor.

1

1.3 Was ist vorgeschrieben?

Um mögliche Bedrohungen und Notfälle sollten Sie sich nicht nur aus betriebswirtschaftlichen und ethischen Erwägungen kümmern, sondern natürlich auch aus rechtlichen Gründen. In den verschiedensten Regelungen zum Arbeitsschutz leiten sich bereits Anforderungen für Ihren Betrieb ab – wie zum Beispiel:

Arbeitsschutzgesetz (ArbSchG)

In §§ 5 und 6 wird das Unternehmen verpflichtet, eine dokumentierte Gefährdungsbeurteilung durchzuführen. Hierbei müssen die maßgeblichen mit der Arbeit verbundenen Gefährdungen für die Beschäftigten ermittelt und entsprechende Schutzmaßnahmen festgelegt werden.

In § 9 werden „besondere Gefahren“ behandelt. Die Beschäftigten müssen demnach über besondere Gefahren unterwiesen und in die Lage versetzt werden, Schutzmaßnahmen anzuwenden. Dabei sind die Kenntnisse der Beschäftigten sowie die vorhandenen technischen Mittel zu berücksichtigen.

In § 10 des ArbSchG werden Maßnahmen zur Ersten Hilfe, zum Brandschutz und zur Evakuierung vorgeschrieben – dies sind Kernthemen des Arbeitsschutzes. Dabei ist auch „… der Anwesenheit anderer Personen Rechnung zu tragen“, also zum Beispiel Kundinnen und Kunden oder Besucherinnen und Besucher.

Wussten Sie, …

… dass in Deutschland rund 60.000 Menschen pro Jahr einen Herz-Kreislauf-Stillstand außerhalb eines Krankenhauses erleiden? Nur etwa zehn Prozent der Betroffenen überleben. Ein Problem: In gerade einmal 40 Prozent aller Fälle beginnen zufällig Anwesende rechtzeitig mit Wiederbelebungsmaßnahmen. Würden mehr Menschen unverzüglich Erste Hilfe leisten, könnten sich die Überlebenschancen der Patientinnen und Patienten verdoppeln bis verdreifachen.

(Quelle[3]: Bundesgesundheitsministerium, siehe Quellenverzeichnis)

Betriebssicherheitsverordnung (BetrSichV)

In § 11 werden „besondere Betriebszustände, Betriebsstörungen und Unfälle“ behandelt. Hiernach müssen beim Umgang mit Arbeitsmitteln unter anderem folgende Punkte beachtet werden:

- Beschäftigte und andere Personen müssen bei einem Unfall oder bei einem Notfall unverzüglich gerettet und ärztlich versorgt werden können.
- Der Arbeitgeber hat dafür zu sorgen, dass die notwendigen Informationen über Maßnahmen bei Notfällen zur Verfügung stehen. Die Informationen müssen auch Rettungsdiensten zur Verfügung stehen.
- Zu den Informationen zählen eine Vorabmitteilung über einschlägige Gefährdungen bei der Arbeit sowie Informationen über einschlägige und spezifische Gefährdungen, die bei einem Unfall oder Notfall auftreten können, einschließlich der Informationen über die Maßnahmen.

Nach den **Empfehlungen zur Betriebssicherheitsverordnung (EmpfBS1115)** „Umgang mit Risiken durch Angriffe auf die Cyber-Sicherheit von sicherheitsrelevanten MSR-Einrichtungen“ (Mess-, Steuerungs- und Regelungstechnik) muss der Arbeitgeber im Rahmen der Gefährdungsbeurteilung ermitteln, welche Möglichkeiten bestehen, dass *„durch Manipulation eine sicherheitsrelevante MSR-Einrichtung ihre Sicherheitsfunktion nicht mehr ausüben kann und damit Gefährdungen nicht mehr verhindert beziehungsweise sogar herbeigeführt werden können“*.

Sicherheitsrelevante **MSR**-Einrichtungen dienen der sicheren Verwendung von Arbeitsmitteln.

1

DGUV Vorschrift 1 „Grundsätze der Prävention“

Die Unfallverhütungsvorschrift DGUV Vorschrift 1 „Grundsätze der Prävention“ beziehungsweise die DGUV Regel 100-001 – hier wird die Unfallverhütungsvorschrift anhand von Beispielen ausführlich erläutert und konkretisiert – fordert in § 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 der Terminus *„sonstige gefährliche Störungen des Betriebsablaufes“* ist dabei thematisch sehr weit gefasst. Es wird unter anderem die Aufstellung von Notfallplänen für *„****unerwartete Situationen****, zum Beispiel* ***Amokfall,“*** gefordert. Beispielhaft werden in der DGUV Regel als Notfälle ***„Brand, Unfall, Einbruch, Überfall …“*** genannt.

In § 23 werden **Maßnahmen gegen Einflüsse des Wettergeschehens** gefordert, die einerseits die Gesundheitsgefahren für die Beschäftigten beziehungsweise Dritte, andererseits auch Unfallgefahren in betrieblichen Einrichtungen, zum Beispiel Eisglätte auf Verkehrswegen oder an Anlagen und Betriebsmitteln, zum Beispiel die **Windlast** an einem Baukran, beinhalten.

Auch in Technischen Regeln, hier den Arbeitsstättenregeln (ASR), finden sich Regelungen zum Umgang mit Bedrohungen und Notfällen.

ASR A2.3 „Fluchtwege und Notausgänge, Flucht- und Rettungsplan“

Danach sind bei *„besonderen Gefährdungen oder aufgrund der örtlichen Gegebenheiten sowie der Nutzungsart und komplizierten Bedingungen im Gefahrenfall“* Maßnahmenpläne zu entwickeln, wie betriebliche Alarm- und Gefahrenabwehrpläne.

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.

Weitere Gesetze und Regelwerke

Das **Aktiengesetz (AktG)** und das **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)** fordern ein Überwachungssystem beziehungsweise Risikofrüherkennungssystem – im Wesentlichen für Aktiengesellschaften. Die Regelungen zu **Basel III** und die Mindestanforderungen an das **Risikomanagement bei Kreditinstituten (MaRisk)** für Banken und **Solvency II** für die Versicherungswirtschaft fordern ganz allgemein ein Risikomanagement.
In Managementsystemen, wie zum Beispiel der **DIN ISO 31000** zum „Risikomanagement“, finden sich naturgemäß weitere Anforderungen, da sich diese Norm sehr umfassend mit dem Umgang von Risiken im Betrieb beschäftigt. Hier heißt es unter anderem: *„Das Risikomanagement ist auf den internen und externen Kontext ausgerichtet. Dies erfordert eine Anpassung an alle relevanten rechtlichen und regulatorischen Anforderungen sowie an allgemein anerkannte Grundsätze von Sicherheit, Gesundheitsschutz und Umweltschutz.“*

In der **DIN ISO 45001**, einem *„Managementsystem für Sicherheit und Gesundheit bei der Arbeit“*, finden sich weitere Erläuterungen. So wird der Begriff der Gefährdung als *„Ursache, die potenziell zu Verletzung und Erkrankung führen kann“*, erklärt. Für den Prozess zur *„Ermittlung von Gefährdungen und Bewertungen von Risiken und Chancen“* wird unter anderem eine Betrachtung von *„zurückliegenden relevanten Vorfällen, innerhalb und außerhalb der Organisation, einschließlich Notfällen und ihren Ursachen“* sowie *„potenziellen Notfallsituationen“* gefordert.

Auch **AMS – Arbeitsschutz mit System**, mit dem die VBG ihren Mitgliedsunternehmen einen wirksamen und systematischen Arbeitsschutz bescheinigen kann, fordert Maßnahmen unter anderem für Notfallsituationen.

Die **VDI-Richtlinie 4062**, Blatt 2, „Gefahrenabwehr bei lebensbedrohlichen Gewalttaten“, gilt für den Schutz von Menschen in Organisationen und Unternehmen (auch Bildungseinrichtungen, Kindergärten und Veranstaltungen). Die Richtlinie 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. Solche Gewalttaten lassen sich mithilfe der Hinweise nicht verhindern. Ziel der Hinweise und empfohlenen Sicherungstechniken ist es, die Tatausübung zu erschweren und dadurch den Schadensumfang zu minimieren und Personen zu schützen.

Es gibt also bereits ein umfassendes Gesetzes- und Regelwerk, das eine Betrachtung zum Umgang mit Bedrohungen und Notfällen – welcher Art auch immer – im Unternehmen einfordert.

2

2 Risiken beachten ist Führungsaufgabe

Prävention und Risikobetrachtung

2.1 Prävention als Führungsaufgabe

Ihre Aufgabe als Unternehmer oder Unternehmerin besteht darin, Ihren Betrieb strategisch und wirtschaftlich gut aufzustellen sowie mit zufriedenen Führungskräften und Beschäftigten einen produktiven und gesundheitsgerechten Wertschöpfungsprozess zu gestalten. Damit Sie diese Aufgabe erfolgreich erfüllen können, müssen Sie zum einen die personellen, zeitlichen und finanziellen Ressourcen zur Verfügung stellen. Zum anderen müssen Sie die Risiken kennen, die mit diesen Prozessen verbunden sind: die Chancen, die sich ihrem Betrieb bieten, und die Gefahren, die drohen könnten.

Vorausschauende und vorsorgende Führung ist erfolgreiche Führung – mit einem Wort: präventive Führung. Wesentliche Bestandteile klassischer Führungsaufgaben sind:

- Die Bedrohungen (und auch Chancen) für das Unternehmen identifizieren.
- Die Risiken beurteilen und steuern.
- Die Handlungsziele unter Berücksichtigung der Risiken festlegen.
- Die Maßnahmen entsprechend der Handlungsziele gemeinsam mit den Führungskräften und Beschäftigten planen, umsetzen und jeweils kommunizieren.
- Die Maßnahmen und deren Anwendung vorleben.
- Die Wirksamkeit der Maßnahmen überprüfen und die Prozesse verbessern.

Bedrohungen und eventuell eingetretene Notfälle sind ein Bestandteil der Risiken für Ihr Unternehmen, die – wie beispielsweise die Coronakrise zeigt – existenzbedrohend sein können. Deswegen sollten Sie auch einschätzen, welche Bedrohungen für Ihr Unternehmen und Ihre Abläufe bestehen können, welche Risiken vorhanden sind und wie sie sinnvollerweise sowie angemessen damit umgehen können.

Dazu sollten sie vor allem zwei Aspekte beachten:

1. Informieren Sie sich, um entscheiden zu können: Verschaffen Sie sich einen Überblick über mögliche Bedrohungen und Notfälle für Ihr Unternehmen. Eignen Sie sich Handwerkszeug an, mit dem Sie die Situation im Unternehmen einschätzen und beurteilen können. Diese Schrift hilft Ihnen dabei.

2. Machen Sie im Unternehmen deutlich, dass das Thema Bedrohungen und Notfälle relevant ist: Wenn Sie wollen, dass Führungskräfte und Beschäftigte, aber auch Fremdfirmen, in Ihrem Unternehmen mitziehen, sollten Sie als Unternehmerin beziehungsweise Unternehmer betonen, dass Ihnen das Thema Bedrohungen und Notfälle wichtig ist. Formulieren Sie Ihre **Ziele und Erwartungen** konkret. Erklären Sie, worum es geht und warum Sie das Thema gemeinsam mit Führungskräften und Beschäftigten angehen. Beschreiben Sie, dass die Prävention im Hinblick auf Bedrohungen und Notfälle ein wichtiges Instrument und Bestandteil Ihrer Unternehmenskultur ist.

Sie sollten aus der Vielzahl der verfügbaren Informationen die für Sie relevanten heraussuchen und berücksichtigen.

2

2.2 Prozesse systematisch gestalten – der operative Aspekt

Zunächst einmal sollten Sie die Prozesse zum Umgang mit den Risiken durch Bedrohungen und Notfälle im Unternehmen festlegen. Dabei können Sie sich an den folgenden Prozessschritten zur systematischen Risikobetrachtung orientieren:

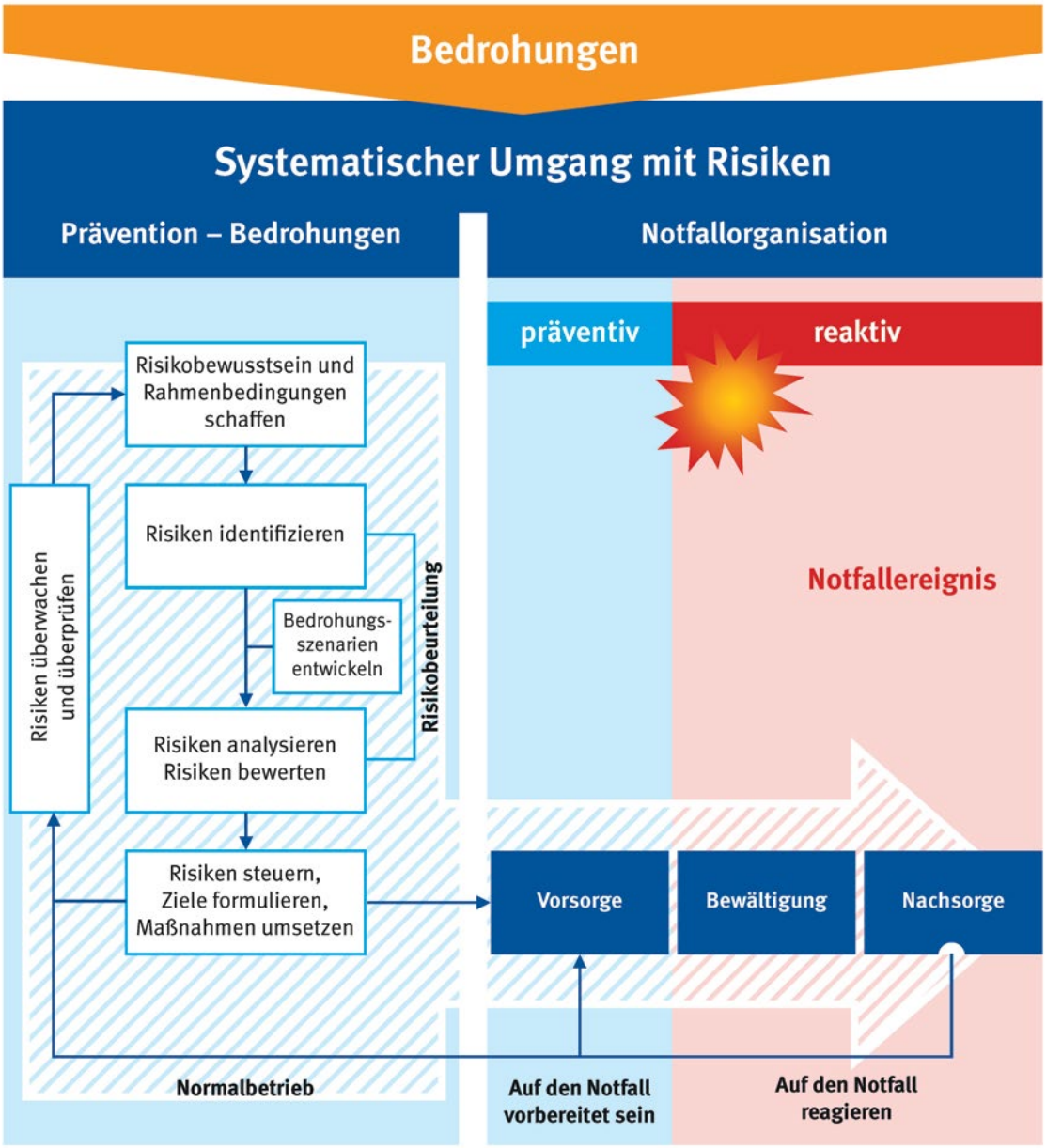
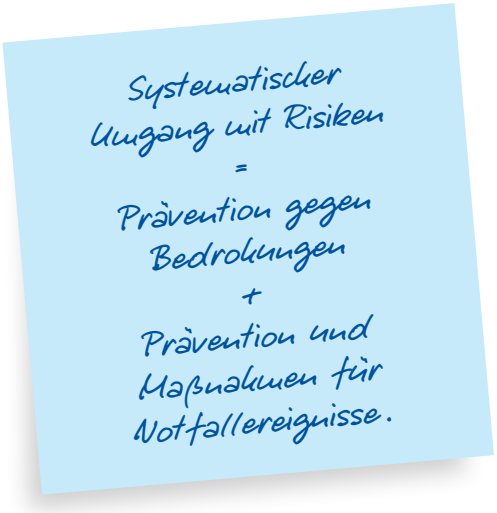


Abbildung 2: Systematischer Umgang mit Risiken

Wenn aus Notfällen Krisen werden

Aus eskalierenden Notfallereignissen oder Katastrophen können sich Krisen ergeben, die Leben bedrohen und zu einer existenzbedrohenden Extremsituation führen können. Die Notfallorganisation reicht in der Regel nicht dazu aus, Krisen bewältigen zu können. Krisen erfordern außerordentliche Maßnahmen. Größere Betriebe haben für diese Situation ein spezielles Krisenmanagement – siehe Kapitel 7.1.

Dieser Umgang mit Risiken im Sinne eines kontinuierlichen Verbesserungsprozesses (KVP) umfasst also zum einen die Prävention gegen Bedrohungen in Ihrem Unternehmen und zum anderen die Notfallorganisation.



Der systematische Umgang mit Risiken besteht aus folgenden Bausteinen:

- **Umgang mit Risiken als Führungsaufgabe** (Informationen in diesem Kapitel 2)
- **Risikoidentifikation und Bedrohungsszenarien:** Was könnte dem Unternehmen schaden (siehe Kapitel 3)?
- **Risikoanalyse und -bewertung:** Risiken analysieren und bewerten sowie präventive Maßnahmen für die wesentlichen Bedrohungen und Notfälle entwickeln (siehe Kapitel 4)
- **Risiken steuern** und **Maßnahmen** festlegen, umsetzen und **verbessern** (Kapitel 5)
- **Notfallorganisation** – gut organisiert den Ernstfall meistern (siehe Kapitel 6)
- **In großen Unternehmen: Krisen- und Kontinuitätsmanagement** (siehe Kapitel 7)

Zu diesem Prozess gehört auch, sich Gedanken zu machen, ob Sie ein betriebliches Notfallhandbuch (siehe Kapitel 6.3) benötigen. Überlegen Sie darüber hinaus, ob und wie Sie sich unterstützen lassen wollen beziehungsweise, was Sie im Betrieb selber machen können (siehe Kapitel 8).

Wussten Sie, ...

... dass im Jahr 2020 die weltweiten Schäden durch Naturkatastrophen rund 210 Milliarden US-Dollar betrugen, wovon etwa 82 Milliarden US-Dollar versichert waren? Damit lagen die Gesamtschäden ebenso wie die versicherten Schäden deutlich über denen des Vorjahres (166 Milliarden US-Dollar und 57 Milliarden US-Dollar).

(Quelle[4]: Münchener Rückversicherung, 2021, siehe Quellenverzeichnis)

3


Sturm
Evaku-ierung
Strom-Ausfall EDV-Ausfall
Schutz-gelderpres-sungen
Unwetter
Gefahr-stoff-austritt
Infektion bei Be-schäftig-ten
Bomben-drohung
Arbeits-unfall
Daten-diebstahl
Hoch-wasser
Amok-lauf

3 Risikoidentifikation – was kann Schäden verursachen?

Kompetenz zum Erkennen von Bedrohungen aufbauen

3.1 Bedrohungen erkennen

Der erste Schritt der Risikobewertung ist die Identifizierung der möglichen Bedrohungen, die auf Ihr Unternehmen einwirken können beziehungsweise zu Notfällen führen könnten.

Überlegen Sie, **welche Bedrohungen** für Ihr Unternehmen **infrage kommen**. Dazu können Naturereignisse, wie Hochwasser, Sturm oder starker Schneefall, genauso wie betriebliche Störungen, etwa ein längerer oder überregionaler Stromausfall, gehören. Auch durch Menschen verursachte Bedrohungen, wie Diebstahl oder Raub, Angriff auf die IT-Infrastruktur, Sabotage, schwere Gewalttaten und gesundheitliche Bedrohungen, stellen potenzielle Gefahren dar.

Sie müssen kein ausgewiesener Fachmann sein, um die offensichtlichen Bedrohungen zu identifizieren – Ihnen hilft zunächst gesunder Menschenverstand.

Dabei sollte Ihnen bewusst sein, dass Sie nicht immer alle für Sie relevanten Bedrohungen und Risiken zuverlässig oder vollständig erkennen können. Die Risikoidentifikation ist immer ein Annäherungsprozess und Sie können sich zunächst einmal ganz unbefangen erste Gedanken zu möglichen Bedrohungen und Notfällen machen.

Grundsätzlich gilt, dass dabei Ihre subjektive Wahrnehmung von Bedrohungen immer eine Rolle spielt. Deswegen ist es bereits in dieser Frühphase hilfreich, wenn Sie sich mit Ihren Führungskräften und Beschäftigten zusammensetzen und zum Beispiel ein „Brainstorming“ durchführen. Wichtig ist an dieser Stelle, dass alle Nennungen gesammelt werden. Eine Vorauswahl hinsichtlich Relevanz ist zu früh und nicht hilfreich.

Auch die subjektive Wahrnehmung von mehreren Personen führt noch nicht zur vollständigen Sicherheit, aber viele Perspektiven können unterschiedliche Aspekte berücksichtigen.

Beginnen können Sie die Identifikation möglicher Bedrohungen beispielsweise mit Fragen wie:

- Welche Bedrohungen oder Notfälle hat es bereits im Betrieb gegeben?
- Kann sich jemand an Vorfälle in anderen Unternehmen oder aus den Medien erinnern, die auf den eigenen Betrieb zutreffen könnten?
- Gibt es besondere Anlässe, sich mit Bedrohungen zu befassen? Diese können zum Beispiel aus neuen Produktions- und Arbeitsverfahren, Änderungen im betrieblichen Umfeld, behördlichen Regelungen, der Umstellung von Abläufen oder Beinahe-Vorfällen resultieren.
- Welche besonderen Bedrohungen von innen sind denkbar? Zum Beispiel ungenügender Brandschutz, Datendiebstahl durch Beschäftigte, Sabotage.
- Welche besonderen Bedrohungen von außen sind denkbar? Dies sind zum Beispiel Energieausfall, Hochwasser, Sturm, Gewalteinwirkungen, Pandemien, Sabotage, Hackerangriffe.

Bei diesen ersten Überlegungen und Gedanken zur Risikoidentifikation helfen beispielhafte Listen mit möglichen Bedrohungen. Diese können Anregungen und Hinweise geben, an die Sie selber vielleicht nicht gedacht haben.

Eine solche Liste finden Sie im folgenden Kapitel 3.2.

3

3.2 Beispielhafte Liste möglicher Bedrohungen

Im Folgenden finden Sie eine beispielhafte Liste von Bedrohungen, die es Ihnen erleichtern kann, im eigenen Unternehmen entsprechende Risiken zu identifizieren.

Die Begrifflichkeiten sind hier umgangssprachlich zu verstehen. Die Ursache der Bedrohung ist an dieser Stelle noch nicht Gegenstand der genauen Betrachtung, sondern erfolgt später. Die Zuordnung zu den Bedrohungskategorien in dieser beispielhaften Aufzählung kann nicht immer trennscharf sein.

Wussten Sie, ... dass in den vergangenen Jahren das Risiko für Datendiebstahl, Industriespionage und Sabotage dramatisch gestiegen ist? In einer Studie des Digitalverbands Bitkom gaben drei Viertel aller befragten Unternehmen an, in den zurückliegenden zwei Jahren davon betroffen gewesen zu sein. In den Jahren 2015 und 2017 war nur rund jedes zweite Unternehmen betroffen. Hinzu kommt eine hohe Dunkelziffer. Denn nicht immer lässt sich solch ein Angriff zweifelsfrei feststellen.

(Quelle[5]: Bitkom, siehe Quellenverzeichnis)

„Technische“ Bedrohungen	Bedrohungen durch Naturereignisse	Bedrohungen der Gesundheit	Bedrohung von Personen (durch Menschen)	Bedrohung von Sachwerten (durch Menschen)
Brandereignis	Hochwasser/ Sturmflut	Lebensmittel-vergiftung	Amoklauf	Diebstahl
Stromausfall	Starkregen/Hagel	Epidemie/Pande-mie (zum Beispiel Grippe)	Bomben-/Brand-anschlag	Einbruch
Freisetzung von Chemikalien	Sturm/Tornado	Hitze-/Kältewelle	Geiselnahme	Hackerangriff
Explosion	Blitzeinschlag		Säureanschlag	Datendiebstahl
Flugzeugabsturz/ Zugentgleisung in Betriebsnähe	Hangrutsch/ Lawine		Erpressung	Spionage
Tagesbruch (in Bergbaugebieten)	Erdbeben		Raubüberfall	Sabotage
Ausfall der Wasserversorgung			Vergiftung/ Anthrax	Vandalismus
			Terroranschlag	Gezielte Zerstörung
			Mord	Erpressung (zum Beispiel IT)
			Körperverletzung	Raubüberfall
			Bestechung	Manipulation von Daten/Fälschung
			Mobbing	

4

4 Risikoanalyse und -bewertung

Die Risiken systematisch erfassen und beurteilen

4.1 Identifizierte Bedrohungen näher untersuchen, Szenarien entwickeln

Nachdem Sie die möglichen Bedrohungen Ihres Unternehmens identifiziert haben, sollten Sie diese systematisch analysieren und bewerten. Dies zusammen ist die **Risikobeurteilung**.

Diese hat das Ziel, die **relevanten Bedrohungen** zu ermitteln, die die Sicherheit und Gesundheit Ihrer Beschäftigten beziehungsweise auch Ihre Kundinnen und Kunden oder Lieferfirmen beeinträchtigen können oder die möglicherweise zu einer Unterbrechung von Geschäftsprozessen führen können. Die Funktion dieser Risikobeurteilung ist

- die wesentlichen Risiken realistisch zu erkennen,
- als Unternehmer oder Unternehmerin sich selbst sowie den Führungskräften und Beschäftigten diese Risiken transparent zu machen,
- eine Grundlage zu haben, wie Sie mit den Risiken umgehen wollen – zum Beispiel, welche Risiken Sie akzeptieren wollen beziehungsweise in welchen Fällen Sie konkrete Maßnahmen einleiten wollen.

Nachdem Sie die möglichen Bedrohungen Ihres Unternehmens identifiziert haben, sollten Sie diese systematisch analysieren und bewerten. Dies zusammen ist die Risikobeurteilung.

Nachdem Sie die möglichen Bedrohungen Ihres Unternehmens identifiziert haben, sollten Sie diese systematisch analysieren und bewerten. Dies zusammen ist die Risikobeurteilung.

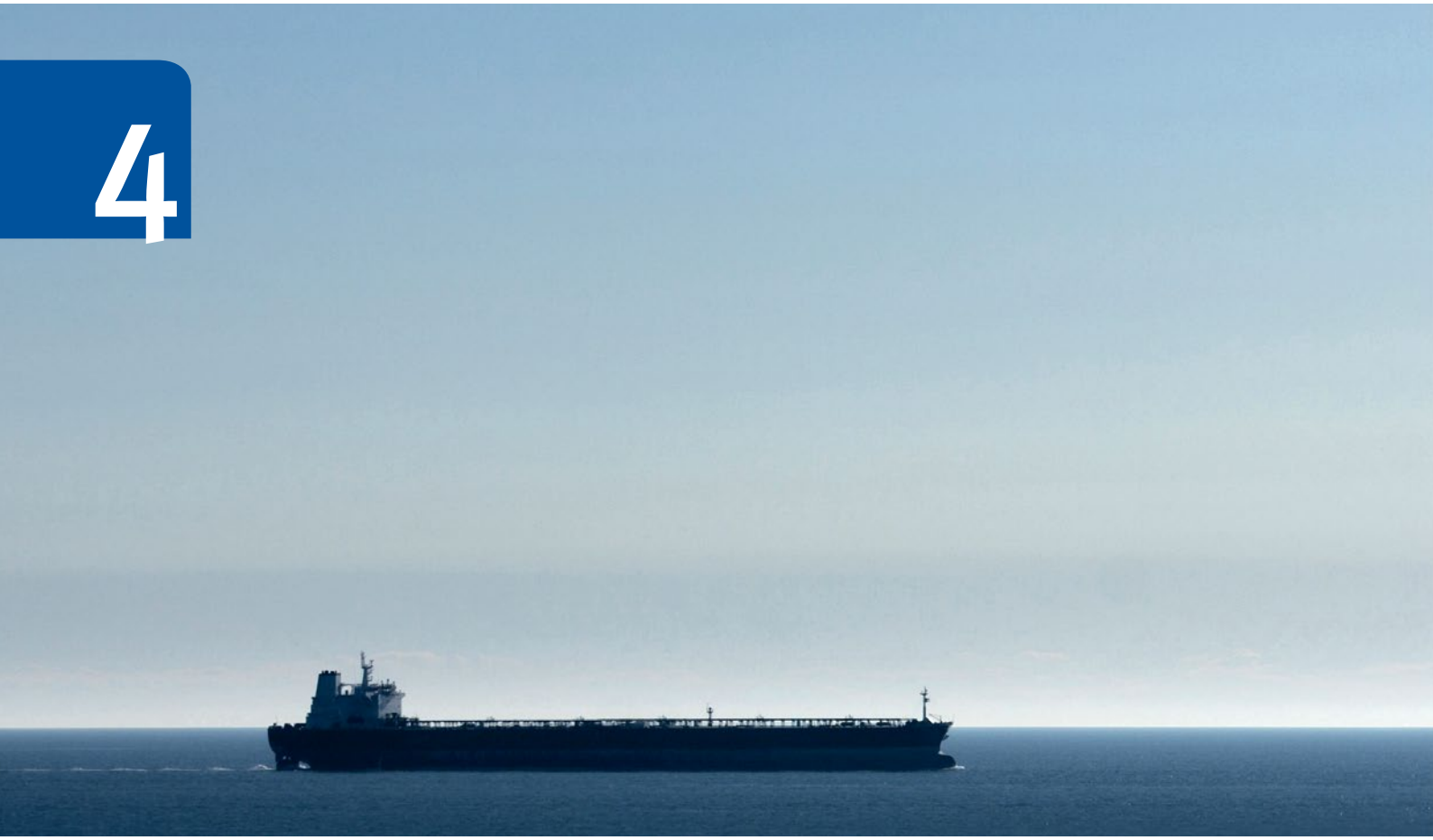
Zunächst kann es sein, dass die Zahl Ihrer identifizierten Bedrohungen relativ groß ist. Um diese für das weitere Vorgehen handhabbar zu machen, sollten Sie diese näher untersuchen, zum Beispiel durch nachfolgende Abwägungen (siehe Seite 26/27).

Wussten Sie, ...

... dass der Eigentümer oder die Eigentümerin eines Bauwerks dafür verantwortlich ist, die Gefahr durch eine Schneelast zu prüfen? Das gestaltet sich in der Praxis mitunter kompliziert. Denn Schnee ist nicht gleich Schnee. Lockerer Pulverschnee ist deutlich leichter als nasser Schnee. Grundsätzlich gilt: In schwierigen Fällen sollten Hausbesitzerinnen und Hausbesitzer lieber Fachkräfte beauftragen und nicht selbst auf den verschneiten Dächern herumklettern. So verfügt etwa das Technische Hilfswerk über Schneelastmesstrupps, die von Einsatzkräften bei starkem Schneefall angefordert werden können.

(Quelle[6]: Spiegel Online, siehe Quellenverzeichnis)

4



Wussten Sie, ...

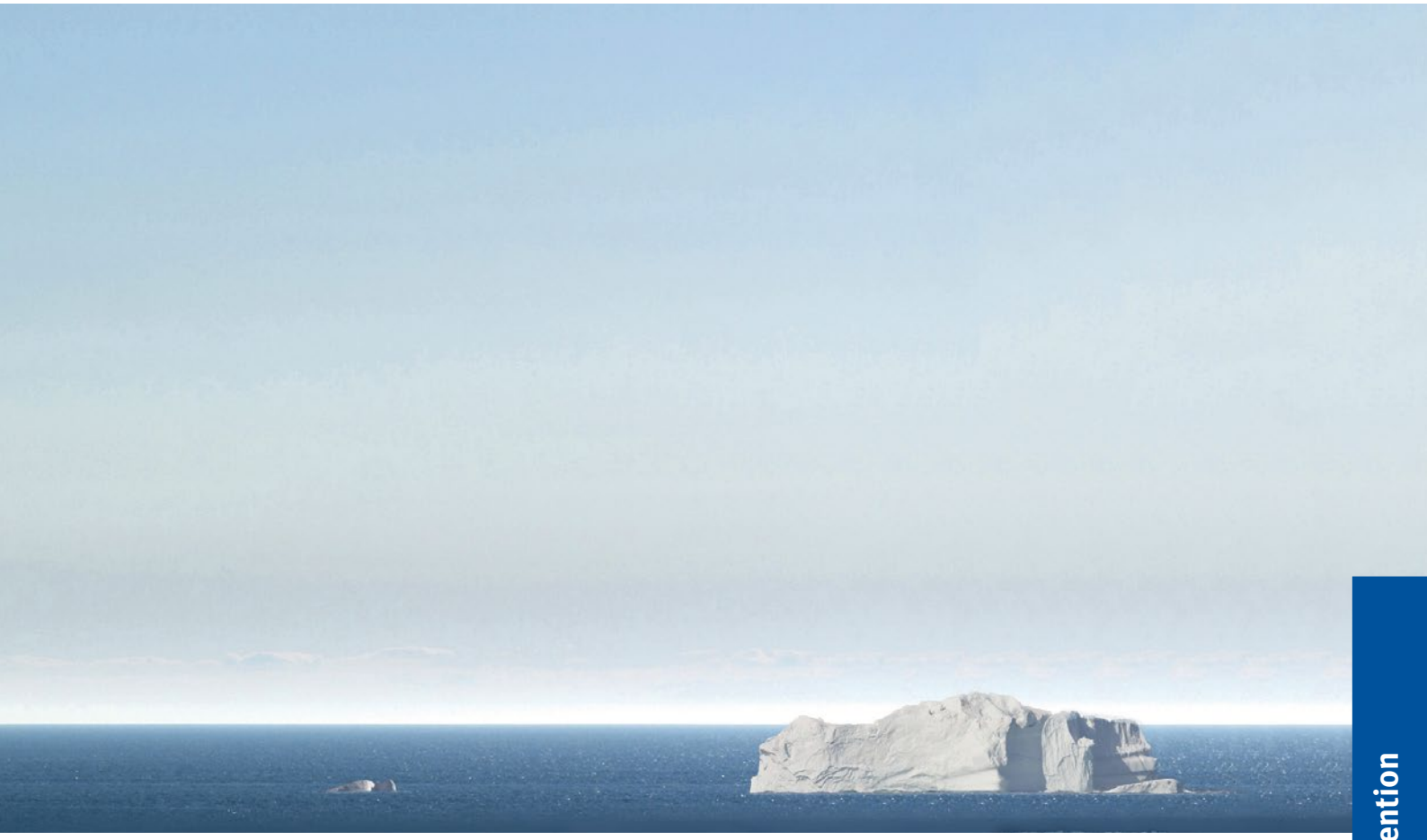
... dass die meisten Meteoriten aus dem All in der Erdatmosphäre verglühen beziehungsweise vollständig verdampfen, bevor sie die Oberfläche unseres Planeten erreichen? Immer wieder erreicht jedoch auch ein nicht verdampfter Rest eines solchen Himmelskörpers die Erdoberfläche. Eine Abschätzung aus fotografisch aufgezeichneten Meteorbahnen geht pro Jahr weltweit von insgesamt 5.800 Meteoritenfällen mit einem Gewicht über 0,1 Kilogramm auf Landflächen aus. Ein großer Teil davon fällt jedoch auf unbesiedelte Gebiete.

(Quelle[7]: Schweizer Bundesamt für Bevölkerungsschutz, BABS, siehe Quellenverzeichnis)

Abwägung 1 – Eintrittswahrscheinlichkeit

Ist die identifizierte Bedrohung durchaus vorstellbar und sollte deshalb genauer analysiert werden oder ist sie praktisch unmöglich? So tritt zum Beispiel ein Meteoriteneinschlag so selten ein, dass Sie sich damit nicht weiter befassen sollten (siehe Infokasten links). Aus diesem Grund sollten vergleichbare Bedrohungen nicht weiter betrachtet werden, auch wenn das Schadensausmaß bei einem tatsächlichen Eintreten extrem hoch wäre.

Bedrohungen, deren Eintreten für Ihren Betrieb nahezu ausgeschlossen ist, sollten nicht weiter betrachtet werden.



Abwägung 2 – Schadensschwere

Ist bei einer Bedrohung mit durchaus vorstellbarer Eintrittswahrscheinlichkeit ein mindestens mäßiges (mittleres) Schadensausmaß für Ihre Beschäftigten, Lieferfirmen und Kunden beziehungsweise Kundinnen sowie die kritischen Geschäftsprozesse und Ressourcen anzunehmen? So werden zum Beispiel durch einen für die Region normalen Schneefall mit etwas Glatteis keine maßgeblichen Auswirkungen zu erwarten sein, sodass Sie in den allermeisten Fällen diese „Bedrohung“ nicht berücksichtigen müssen.

Richten Sie Ihr Augenmerk auf die wesentlichen Bedrohungen mit durchaus vorstellbarer Eintrittswahrscheinlichkeit und einem mindestens mittleren Schadensausmaß für Ihren Betrieb.

4

Begriffsklärung: Szenario

Ein Szenario ist die bildhafte Darstellung/ Beschreibung eines Risikos mit Annahmen über Abläufe und Auswirkungen von Ereignissen. Es zeigt auf, wie sich eine Bedrohung in einem Unternehmen auswirken kann.

Entwicklung von Szenarien

Bei der Beurteilung der Arbeitsbedingungen (Gefährdungsbeurteilung) nach dem Arbeitsschutzgesetz gilt: Nach der Ermittlung der Gefährdungen schließt sich deren Bewertung an. Dieses Vorgehen ist aber bei der Bewertung von Bedrohungen nicht zielführend. Zum Beispiel lässt sich die Bedrohung „Hochwasser“ nicht ohne weiteres bewerten, denn häufig fehlen wichtige Hintergrundinformationen für die Bewertung der Bedrohungen.

Damit Sie die Bedrohungen besser verstehen können, um diese dann analysieren und bewerten zu können, ist die Entwicklung von konkreten Bedrohungsszenarien hilfreich. Dort werden zum Beispiel je nach Ursache der Bedrohungen die zu erwartenden Risiken für einen definierten Arbeitsbereich oder eine Tätigkeit beschrieben.

Mit der Szenario-Technik können Sie die unterschiedlichen zeitlichen Entwicklungen und Eskalationsmöglichkeiten der Ereignisse (vom positiven bis zum negativen Extrem) bildhaft beschreiben. Sie ermöglicht es, die mit dem jeweiligen Bedrohungsszenario zusammenhängenden Risiken zu identifizieren.

Fünf hilfreiche Schritte

Um welche Bedrohung handelt es sich?
Beschreiben Sie die Bedrohung, für die das Szenario gelten soll – zum Beispiel Hackerangriff auf IT, Infektionswelle, Hochwasser, Stromausfall, Extremwetter, Brandgefahr.

Was ist die Ursache?
Bei einem Stromausfall ist es für Ihr Unternehmen beispielsweise ein entscheidender Unterschied, ob die Ursache eine großflächige Überlastung des regionalen Netzes (Blackout) ist, ob ein Baggerfahrer bei Bauarbeiten vor Ort ein Erdkabel beschädigt hat oder ob das betriebliche Stromnetz nicht für die zunehmende Anzahl von Verbrauchern ausgelegt ist.

Wie ist der Verlauf?
Zeigen Sie die zeitliche Entwicklung des Verlaufes auf – zum Beispiel: Bei einem einstündigen Starkregen kommt es zur Überflutung auf dem Betriebsgelände.

Welche Bereiche sind betroffen?
Beschreiben Sie, welche Bereiche im Unternehmen maßgeblich betroffen sind – zum Beispiel eine Lagerhalle.

Welche Auswirkungen hat diese Bedrohung?
Überlegen Sie, welche möglichen Folgen die Bedrohung für Ihren Betrieb haben kann – zum Beispiel: Die Produktion steht aufgrund eines Stromausfalls drei Tage still.

Achten Sie bei den Szenarien darauf, dass die Beispiele keine zu umfassenden aufeinander folgenden Ereignisse (Kaskaden-Effekt) beinhalten, da ansonsten später aufgrund der Komplexität keine vernünftigen Bewertungen zur Schadensschwere möglich sind.

Auch die Beschreibung eines Szenarios mit geringen Auswirkungen auf den Betrieb hilft Ihnen nicht weiter. Entwickeln Sie deshalb ein schlimmstmögliches, aber dennoch plausibles Szenario (Credible Worst Case) für Ihr Unternehmen. Allerdings sollten Sie bedenken, dass derartige Worst-Case-Szenarien oft zu einer pessimistischen Sichtweise tendieren, die eine extreme Ausnahmesituation beschreiben.

Wenn Sie dies aber berücksichtigen, kann ein solches Szenario für den ungünstigsten Fall bei der Einschätzung helfen, welche Relevanz die identifizierten Risiken tatsächlich für das Unternehmen haben, und dabei, sich auf die zentralen Risiken zu konzentrieren.

Wussten Sie, ...

... dass Infektionskrankheiten sich wegen der Vernetzung unserer modernen Welt heute viel schneller verbreiten als früher? Während sich im 14. Jahrhundert die Pest mit einer Geschwindigkeit von vier bis fünf Kilometern pro Tag ausbreitete, sind es bei aktuellen Epidemien durchschnittlich zwischen 100 und 400 Kilometer pro Tag.

(Quelle[8]: DKKV, siehe Quellenverzeichnis)

4 Wie viele Szenarien sollten für jeweils eine Bedrohung erstellt werden?

Diese Frage kann nicht pauschal beantwortet werden. So viele, wie aus betrieblicher Sicht sinnvoll sind. So können zum Beispiel für die Bedrohung „Hochwasser“ aufgrund von verschiedenen Ursachen des Hochwassers (wie Dammbruch, Starkregen, Sturmflut, Schneeschmelze) auch unterschiedliche Szenarien beschrieben werden.

Wussten Sie, ...

... dass Ransomware eine Hacker-Software ist, die den Zugriff zu sämtlichen Daten auf dem Rechner sperrt? Cyberkriminelle erpressen auf diese Weise Unternehmen und fordern in der Regel hohe Beträge, bevor sie ihren Opfern wieder freien Zugriff auf ihre Daten ermöglichen. Der Digitalverband Bitkom spricht von Schäden in Höhe von insgesamt 10,5 Milliarden Euro in den Jahren 2018 und 2019.

(Quelle[9]: Bitkom, siehe Quellenverzeichnis)

Beispiele für Szenarien zu einzelnen Bedrohungen

Starker dreitägiger Schneefall:

Durch einen starken und über drei Tage andauernden Schneefall kommt es zu Schneehöhen von bis zu einem Meter. Dadurch werden der öffentliche Verkehr sowie der Gütertransport auf der Straße fast komplett lahmgelegt. Erforderliche Rohstoffe und Vorprodukte können nicht mehr oder nur mit größer Verzögerung angeliefert werden. Schon ab dem zweiten Tag muss die Produktion um 50 Prozent heruntergefahren werden, weil die Lagerbestände nicht ausreichen. Ein großer Teil der Beschäftigten kann nicht mehr zur Arbeit kommen. Die Statik der Gebäude ist durch die Schneelast nicht gefährdet.

Hackerangriff:

Ein unzufriedener Beschäftigter aus der IT greift auf interne Daten einer neuen Produktentwicklung zu und stellt diese öffentlich auf eine Online-Plattform ein. Die wertvollen internen Informationen stehen somit auch den Mitbewerbern und -bewerberinnen zur Verfügung. Dadurch wird die Entwicklungsarbeit von zwei Jahren zunichte gemacht und der Marktvorsprung gefährdet.

Infektionskrankheit:

Im Winter infiziert sich ein Fünftel der Belegschaft mit einem Grippevirus (Influenza) und fällt krankheitsbedingt durchschnittlich für jeweils zwei Wochen aus. Sämtliche Abteilungen sind betroffen. Ein wichtiger Termin mit einem Schlüsselkunden kann dadurch nicht fristgerecht eingehalten werden, eine Vertragsstrafe droht.

Vertiefendes Wissen

Werden Szenarien entwickelt, ist bei komplexeren Betriebsstrukturen eine prozessorientierte Herangehensweise sinnvoll. Die notwendigen Schritte können wie folgt lauten:

Um welche Bedrohung handelt es sich?

Was ist die Ursache?

Wie ist der Verlauf?

Welche Prozesse sind betroffen?

Beschreiben Sie, welche Prozesse im Unternehmen maßgeblich betroffen sind.

Welche Auswirkungen hat diese Bedrohung?

Überlegen Sie, welche möglichen Folgen die Bedrohungen für die Faktoren des Prozesses/ Teilprozesses im Unternehmen haben können. Zu berücksichtigen sind hierbei beispielsweise:

- **Menschen**
  Personal, Fremdfirmen, Besucherinnen und Besucher, ...
- **Gebäude**
  Produktion, Verwaltung, Lager, Tiefgaragen, ...
- **Gelände**
  Verkehrswege, Parkflächen, Grünanlagen, ...
- **Daten**
  IT, Unterlagen in Papierform, ...
- **Versorgungsanlagen**
  Strom, Gas, Wasser, ...
- **Betriebsmittel**
  Maschinen, Fahrzeuge, ...

4

4.2 Risiken einschätzen und bewerten – ein Hilfsmittel ist die Risikomatrix

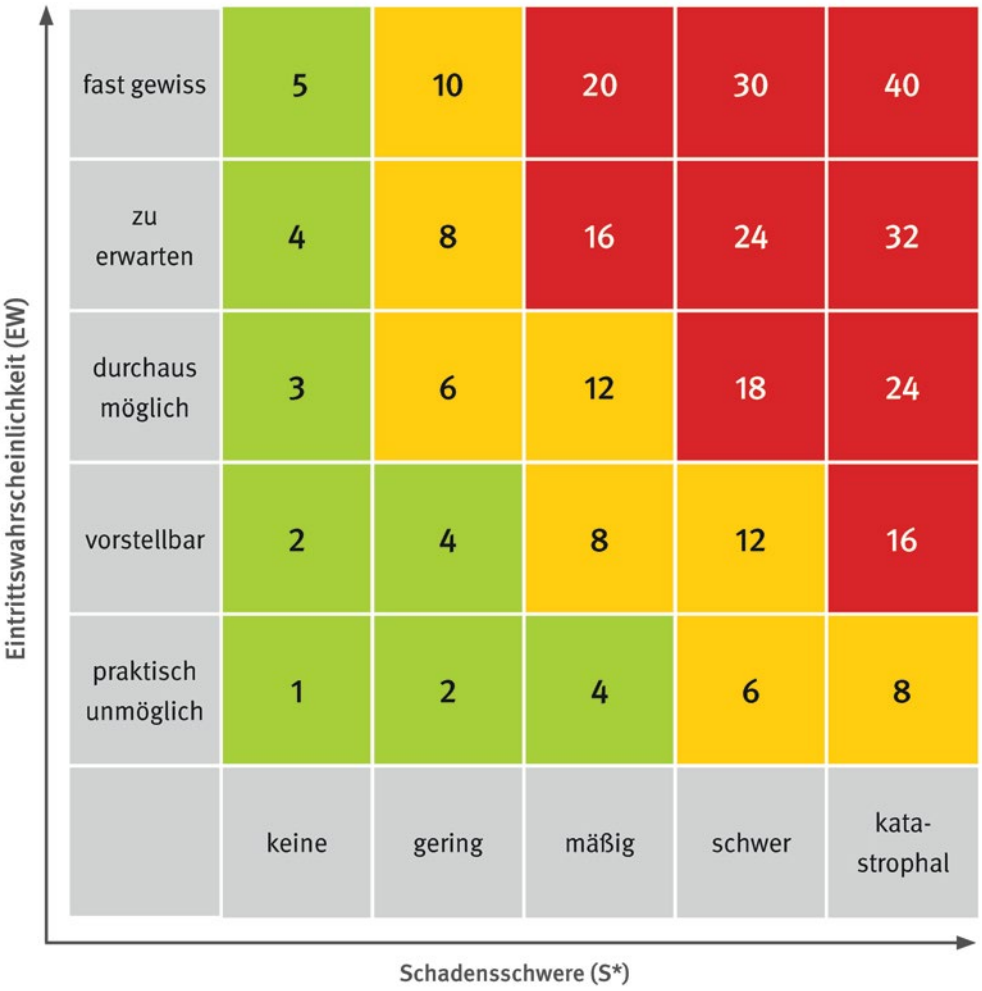


Abbildung 3: Risikomatrix in Anlehnung an die VBG-Software zur Gefährdungsbeurteilung „GEDOKU“ (* höhere Gewichtung der Schadensschwere)

Die Risikomatrix hilft Ihnen, durch Einschätzung der Eintrittswahrscheinlichkeit und der Schadensschwere das Risiko des Bedrohungsszenarios zu bewerten.

Um die **Relevanz** der einzelnen identifizierten Bedrohungen Ihres Unternehmens erkennen zu können, schließt sich als nächster Schritt die Risikoanalyse an. Wählen Sie dazu jeweils ein von Ihnen entwickeltes Bedrohungsszenario aus und schätzen Sie die **Eintrittswahrscheinlichkeit** dieses Szenarios sowie das Ausmaß des **zu erwartenden Schadens** bei den beschriebenen Auswirkungen ein. Dazu kann eine Risikomatrix – siehe Abbildungen 3 und 4 – hilfreich sein, die es in verschiedenen Ausführungen gibt.

Es gibt viele Varianten einer Risikomatrix. Eine 8 x 8 Matrix lässt eine höhere Genauigkeit vermuten. Fraglich ist jedoch, wie exakt die Angaben für die Eintrittswahrscheinlichkeit und Schadensschwere überhaupt gemacht werden können. Für welche Variante Sie sich entscheiden, bleibt Ihnen selbst überlassen. Sie sollte allerdings zu Ihrem Betrieb passen und auch durchgängig verwendet werden. Die unterschiedliche Farbgebung hilft dabei, das für Sie noch akzeptable Risiko festzulegen, beziehungsweise konkreten Handlungsbedarf zu identifizieren (Risikobewertung).

Die Beschriftung der Achsen sollte möglichst neutral und einheitlich gefasst werden. So kann unter der Bezeichnung der höchsten Schadensschwere „katastrophal“ sowohl ein Körperschaden mit tödlichen Folgen als auch eine „Firmenpleite“ verstanden werden.

Die Risikomatrix hat jedoch auch ihre Tücken. So ist Ihre Einschätzung der Eintrittswahrscheinlichkeit und der Schadensschwere fast immer nur subjektiv und relativ grob. Auch Wechselwirkungen zu 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.

Wenn Sie jedoch diese Einschränkung Ihrer Bewertung mitberücksichtigen, bietet die Risikomatrix dennoch eine hilfreiche Orientierung dafür, auf welche wesentlichen Bedrohungen Sie sich konzentrieren sollten.

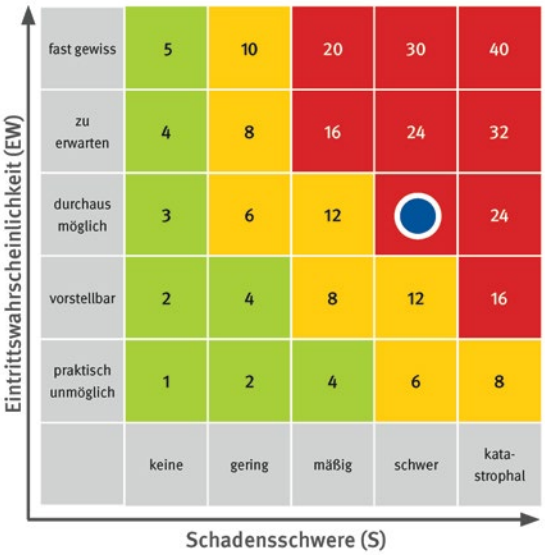


Abbildung 4: Beispiel für eine Risikoanalyse und -bewertung (Risikobeurteilung)

Bedrohungsszenario

Ein Beispiel für die Arbeit mit der Matrix (siehe Abbildung 4): Durch einen Hackerangriff in einem mittelständischen Produktionsbetrieb werden alle Firmendaten verschlüsselt (Ransomware), ein Zugriff ist nicht mehr möglich. Die Hacker verlangen ein Lösegeld in sechsstelliger Höhe. Ergebnis: Die Eintrittswahrscheinlichkeit wird als „durchaus möglich“ (EW = 3) eingeschätzt, die Schadensschwere mit „schwer“ (S = 6) bewertet. Das Risiko R = 18 liegt im roten, nicht akzeptablen Bereich und sollte weiter betrachtet werden.

Wussten Sie, ...

... dass die „Juli-Flut“ 2021 so viele Großschäden angerichtet hat, wie keine andere Naturkatastrophe in Deutschland zuvor? So gab es durch die Flut an Ahr und Erft rund 400 Großschäden mit einer Schadenshöhe von jeweils über einer Million Euro. Schäden in dieser Höhe entstehen vor allem im gewerblichen und industriellen Bereich durch beschädigte Gebäude, Maschinen oder Geräte.

(Quelle[10]: GDV, siehe Quellenverzeichnis)

4 Vertiefendes Wissen

Beachten Sie weiterhin, dass bei der Betrachtung der möglichen Schadensschwere von Sachschäden nicht nur unmittelbare monetäre Auswirkungen eine Rolle spielen. So kann zum Beispiel bei einem Hackerangriff auf eine Softwarefirma mit Schwerpunkt IT-Sicherheit der Imageschaden sehr viel höher sein als der kurzfristige monetäre Schaden durch den Ausfall der IT. Möglicherweise können auch Vertragsstrafen drohen, wenn beispielsweise Sicherheitsgarantien nicht gewährleistet werden können. Es empfiehlt sich somit, für verschiedene Geschäftsprozesse eine Gewichtung hinsichtlich eines möglichen Schadens vorzunehmen.

Wussten Sie, ...

... dass der Golfstrom derzeit so schwach ist, wie nie zuvor in den letzten 1.000 Jahren? Der Grund dafür ist der Klimawandel. Dieser sorgt für mehr Schmelzwasser, einen geringeren Salzgehalt und eine niedrige Oberflächendichte im Atlantik. Dadurch hat sich die sensible Nordatlantische Umwälzströmung seit den 1950er-Jahren um 15 Prozent verlangsamt – eine bislang beispiellose Abschwächung. Hält dieser Trend an, könnte das zu mehr Extremwetterlagen in Europa führen.

(Quelle[11]: Scinexx.de, siehe Quellenverzeichnis)

Darüber hinaus haben Sie die Möglichkeit, die Auswirkungen der identifizierten Bedrohung noch detaillierter zu analysieren und zu bewerten. Dadurch erhalten Sie verlässlichere Informationen über die Zusammenhänge, Wechselwirkungen und Prozesse. Dabei hilft Ihnen die **Abbildung 5 „Risikofelder“.**

Diese zeigt die Auswirkungen jeweils einer Bedrohung (wie beispielsweise „Schneefall“) auf Teilprozesse in Ihrem Betrieb (wie „Herstellung des Produkts“). Hierbei wird berücksichtigt, dass jeder Teilprozess von verschiedenen Faktoren abhängig sein kann, wie beispielsweise Menschen, Gebäuden, Gelände, Daten, Versorgunganlagen, Betriebsmitteln und anderen.

Führen Sie zu jedem Faktor des Teilprozesses eine Risikobewertung mit Hilfe der Risikomatrix durch.

Ein Beispiel für eine derartige Tabelle finden Sie in der nachstehenden Abbildung.

Das Ergebnis für das gewählte Bedrohungsszenario zeigt, dass die Teilprozesse im Wesentlichen durch die fehlende Verfügbarkeit von Fremdfirmen und Beschäftigte sowie die mangelnde Statik der alten Produktionshalle beeinträchtigt sind.

Diese Vorgehensweise bietet somit eine Orientierung, um zu beurteilen, bei welchen Bedrohungen vorrangig Handlungsbedarf bestehen. Dabei sind auch die gesetzlichen Vorgaben mit zu beachten.

Bedrohung:		**Starker Schneefall**					
Bedrohungsszenario:		Ein starker Schneefall erstreckt sich über einen Zeitraum von fünf Tagen. Es kommt zu Schneehöhen von einem Meter, bei Schneeverwehungen von zwei Metern.					
Eintrittswahrscheinlichkeit:		Durchaus möglich.					
		Faktoren der Teilprozesse					
		Menschen Personal, Fremdfirmen, Besucherinnen und Besucher	**Gebäude** Verwaltung, Produktion, Tiefgarage	**Firmen-gelände** Verkehrswege, Parkflächen, Grünanlagen	**Daten** IT, Dokumente, ...	**Versorgungs-anlagen** Strom, Gas, Wasser, Abwasser	**Betriebsmittel** Maschinen, Arbeitsmittel
Anlieferung der Ware	Beschreibung	Ware kann nicht geliefert werden (1 Tag Puffer)					
	Risiko	R = 12					
Herstellung des Poduktes	Beschreibung	Beschäftigte kommen nicht zur Arbeit	Schneelasten alte Produk-tionshalle	Parkflächen eingeschränkt			
	Risiko	R = 12	R = 18	R = 6	R = 3		
Auslieferung des Poduktes	Beschreibung						
	Risiko						

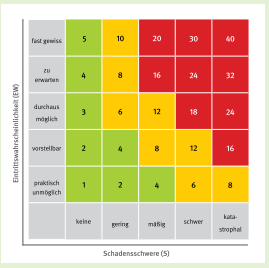


Abbildung 5: Risikofelder

5

5 Risiken steuern, Ziele festlegen, Maßnahmen ableiten und verbessern

Präventive Maßnahmen gegen Bedrohungen

5.1 Ziele und Maßnahmen

Bevor Sie zunächst (Schutz-)Ziele festlegen und dann Maßnahmen ableiten, sollten Sie abwägen, wie Sie mit dem jeweiligen Risiko in Ihrem Betrieb umgehen wollen (Risikosteuerung):

- **Kann das Risiko vollständig vermieden werden?**
  Beispiel: Sie ziehen mit Ihrem Unternehmen aus der hochwassergefährdeten Flussaue in einen höher gelegenen Bereich um.

- **Soll das Risiko akzeptiert werden, ohne tätig zu werden?**
  Beispiel: Das letzte „Jahrhundert-Hochwasser" war vor über 20 Jahren. Sie gehen davon aus, dass das nächste Hochwasser dieser Art in absehbarer Zeit nicht eintritt und das Unternehmen in drei Jahren ohnehin an einen anderen Ort umzieht.

- **Soll das Risiko auf andere übertragen werden (Risikoüberwälzung)?**
  Beispiel: Für die Bedrohung durch Hochwasser wird eine geeignete Elementarschaden-Versicherung abgeschlossen.

- **Kann das Risiko vermindert werden?**
  Beispiel: Um das Firmengelände wird ein geeigneter Hochwasserschutz errichtet.

Bei diesen Abwägungen sollten Sie auch berücksichtigen, dass die verschiedenen Varianten kombiniert werden können. Zudem sind die Maßnahmen des Arbeitsschutzes mit zu berücksichtigen.

Wenn Sie Risiken vermindern wollen, legen Sie zunächst die Ziele Ihrer Maßnahmen fest. Gehen Sie hierbei möglichst systematisch vor (zum Beispiel nach der SMART-Methode): Die Ziele sollten **s**pezifisch, **m**essbar, **a**usführbar, **r**ealistisch und **t**erminiert sein. So ist zum Beispiel die Verhinderung eines Stromausfalls ein ungeeignetes Ziel. Besser ist: *„Für den Fall eines regionalen Stromausfalls ist bis zum [Datum X] sicherzustellen, dass die Produktion mindestens drei Stunden weiterlaufen kann."*

Wussten Sie, ...

... dass ein 100-jährliches Hochwasser nicht zwangsläufig nur einmal in 100 Jahren auftreten muss? So kam es beispielsweise in Köln sowohl 1993 als auch 1995 zu einem „Jahrhundert-Hochwasser". Im Abstand von nur 13 Monaten erreichte der Pegel des Rheins jeweils eine Marke von über 10,60 Metern.

(Quelle[12]: Stadtentwässerungsbetriebe Köln, siehe Quellenverzeichnis)

5

T-O-P:
Technische Maßnahmen
vor organisatorischen
vor personenbezogenen
Maßnahmen

Überprüfen Sie, ob rechtliche und andere Vorgaben für die Ziele zu berücksichtigen sind, wie zum Beispiel:

- Gesetze und Verordnungen mit Technischen Regeln
- Regelungen der Unfallversicherungsträger
- Normen
- Auflagen, zum Beispiel aus Genehmigungsbescheiden
- Vorgaben, zum Beispiel von Sachversicherern
- Herstellerinformationen
- Informationen von Bundesämtern, wie dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), dem Umweltbundesamt (UBA) oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Hinweise der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), der Bundesanstalt für Geowissenschaften und Rohstoffe (BGR), der Feuerwehr, der Polizei oder gegebenenfalls des Technischen Hilfswerks (THW)
- Hinweise von Behörden/Ministerien
- Mögliche Anforderungen von Kunden

Aus den von Ihnen festgelegten Zielen leiten Sie die konkreten Maßnahmen ab. Dabei sollten Sie systematisch vorgehen, um die Wirksamkeit zu erhöhen – zum Beispiel nach dem T-O-P-Prinzip: Technische Maßnahmen vor organisatorischen vor personenbezogenen Maßnahmen.

Die Maßnahmen sollten auf die Ursache der Bedrohung abzielen. So kann beispielsweise ein Stromausfall verschiedene Ursachen haben. Je nach Ursache sind unterschiedliche Maßnahmen zu ergreifen.

Überprüfen Sie auch, ob sich aus der vorhandenen Gefährdungsbeurteilung Auswirkungen auf die Maßnahmen ergeben. Umgekehrt sollten die Maßnahmen zu den Bedrohungen auch in die Gefährdungsbeurteilung mit aufgenommen werden.

Zum Beispiel verlangt der Arbeitsschutz, dass auch in Sicherheitsbereichen die Flucht- und Rettungswege jederzeit frei zugänglich sind, während die Maßnahmen der Zugangskontrolle erfordern, dass Zutrittsbeschränkungen vorhanden sind. Hier sind scheinbar widersprüchliche Ziele in Einklang zu bringen, zum Beispiel durch eine elektronische Zugangsregelung in Verbindung mit Panikschlössern.

Nach Festlegung der Maßnahmen sollten Sie überprüfen, inwieweit das Risiko gesenkt wurde.

Wussten Sie, ...

... dass zwei Drittel der in Deutschland durch Betriebssabotage betroffenen Industrieunternehmen von unzufriedenen eigenen Beschäftigten geschädigt wurden?

(Quelle[13]: Bitkom, siehe Quellenverzeichnis)

5

Vertiefendes Wissen

Nach Festlegung der Maßnahmen sollten Sie überprüfen, inwieweit das Risiko gesenkt wurde.

Prüfen Sie erneut mit Hilfe der Risikomatrix, inwiefern das Risiko nach der Risikominderung (Umsetzung der Maßnahmen) gesenkt wurde und ob Sie dadurch Ihr angestrebtes Risikoniveau (akzeptables Risiko) erreicht haben.

Bedenken Sie, dass sich einige Maßnahmen auf eine Verringerung der Schadensschwere auswirken, andere dagegen auf die Verringerung der Eintrittswahrscheinlichkeit. Eine Verringerung beider Faktoren wäre erstrebenswert, ist aber nur in seltenen Fällen möglich. Zum Beispiel lässt sich die Eintrittswahrscheinlichkeit eines starken Schneefalls oder anderer Naturereignisse auch durch Maßnahmen nicht verringern.

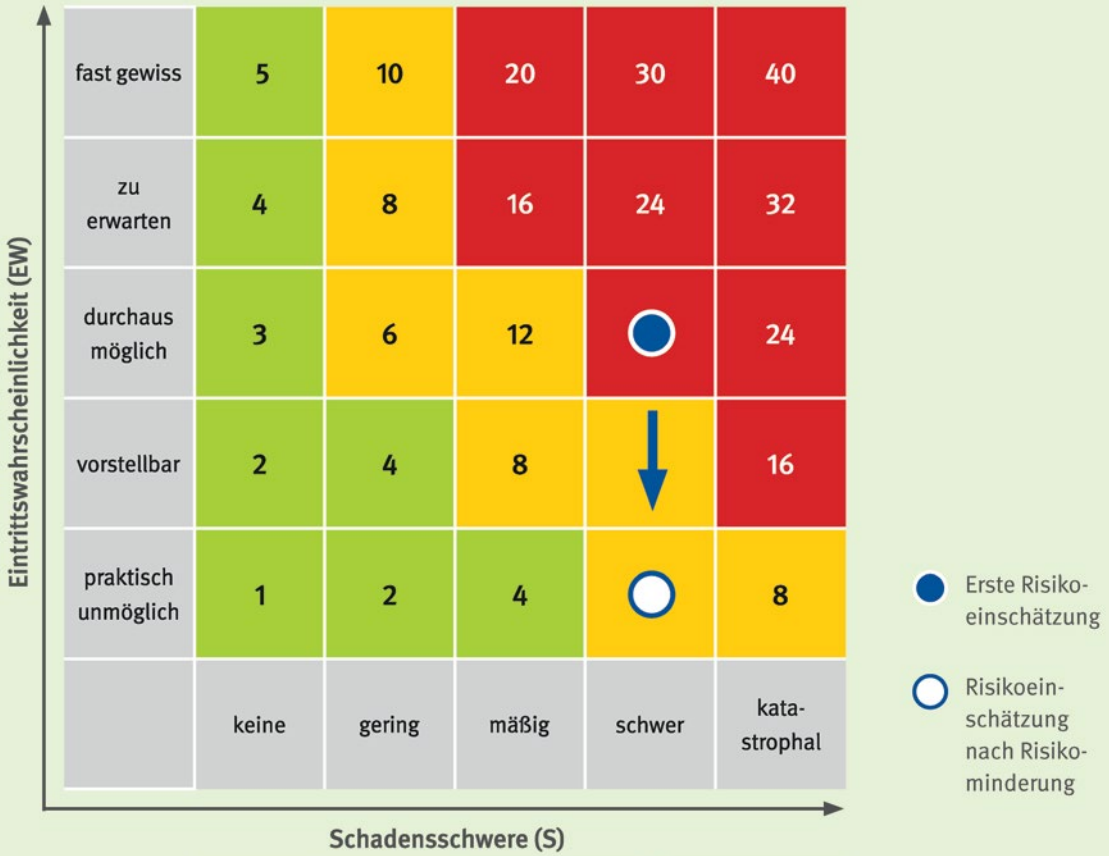


Abbildung 6: Risikoeinschätzung nach Risikominderung, Schadensschwere (S, höhere Gewichtung gegenüber EW)

Bedrohungsszenario

Durch einen Hackerangriff (Beispiel aus Kapitel 4.2) in einem mittelständischen Produktionsbetrieb werden alle Firmendaten verschlüsselt (Ransomware), ein Zugriff ist nicht mehr möglich. Die Hacker verlangen ein Lösegeld in sechsstelliger Höhe.

Die Schadenschwere (S) wurde mit 6 beziffert, die Eintrittswahrscheinlichkeit (EW) mit 3, dies ergibt eine Risikozahl von R = 18.

Risikosteuerung (Maßnahmen)

Es wurden umfangreiche technische, organisatorische und verhaltensbezogene Maßnahmen zur Erhöhung der IT-Sicherheit im Hinblick auf die Bedrohung durchgeführt. Die zuvor eingeschätzte Schadensschwere „schwer“ (S = 6) kann aus präventiver Sicht nicht beeinflusst werden, bleibt somit weiterhin bestehen. Die Eintrittswahrscheinlichkeit wird aber neu bewertet und „nur noch“ mit „vorstellbar“ (EW = 2) eingeschätzt. Das Risiko wurde somit von R = 18 auf R = 12 reduziert.

5

5.2 Verbesserung der Präventionsmaßnahmen zu den Bedrohungen

Damit Ihre Ziele und Maßnahmen zur Prävention der identifizierten Bedrohungen aktuell bleiben, sollten Sie deren Wirksamkeit regelmäßig überprüfen. Nutzen Sie dazu die Risikobeurteilung beziehungsweise auch die Gefährdungsbeurteilung.

Überlegen Sie, wie Sie den **Ablauf der Wirksamkeitskontrolle** gestalten wollen. Zu empfehlen ist, Ihre Führungskräfte, Ihre Beschäftigten, die Interessenvertretung und die Fachkräfte für Arbeitssicherheit sowie die Betriebsärzte und Betriebsärztinnen mit einzubeziehen. Hilfreich können auch Fachleute zum Risiko- und Notfallmanagement sein. Die Wirksamkeitskontrolle sollte regelmäßig – zum Besispiel einmal im Jahr oder bei besonderen Anlässen – durchgeführt werden. Besondere Anlässe können beispielsweise neu identifizierte Bedrohungen, neue Gebäude und Standorte, neue Software oder neue Arbeitsabläufe sein. Auch Vorfälle in anderen Unternehmen oder verwandten Branchen können Anlass für eine Wirksamkeitskontrolle sein.

Bei der Wirksamkeitskontrolle sollten Sie die nachfolgend aufgeführten Aspekte berücksichtigen:

Wie haben die festgelegten Maßnahmen funktioniert?

Ziel dieser Frage ist, Verbesserungsmöglichkeiten zu identifizieren und die Erfahrungen aus der Vergangenheit zu nutzen – als Ausdruck einer gelebten Fehlerkultur. Denn aus Fehlern lässt sich lernen, wie es besser geht. Führen Sie eine Ursachenforschung gemeinsam mit Ihren Beschäftigten durch. Schuldzuweisungen sollten Sie bei diesen Gesprächen und Untersuchungen vermeiden. Konkret sind unter anderem folgende Aspekte zu überprüfen:

- Wie effektiv haben die verantwortlichen Personen gehandelt?
- Sind spezielle Qualifizierungsmaßnahen erforderlich?
- Haben die Unterweisungen der Beschäftigten stattgefunden?
- Haben Führungskräfte und Beschäftigte ihre Erfahrungen in die Prozesse der Risikobewältigung eingebracht?
- In welchem Zustand sind die für die Risikobewältigung benötigten Arbeitsmittel, Anlagen und Einrichtungen? Wurden die Prüffristen eingehalten?
- Wurden die externen Partner (wie Feuerwehr, Rettungsdienst) kontaktiert und welche Erfahrungen gab es dabei?
- Stehen ausreichende personelle und materielle Ressourcen für die Risikobewältigung zur Verfügung?
- Wie haben bei einer Übung die festgelegten Maßnahmen und der Informationsfluss funktioniert?

Waren die Schutzziele und Maßnahmen angemessen? Hat sich die Bedrohungslage verändert?

Überprüfen Sie, ob sich die identifizierten Bedrohungen für das Unternehmen verändert haben oder ob neue Bedrohungen entstanden sind. Folgende Fragen sind dabei beispielsweise hilfreich:

- Gibt es neue Softwareanwendungen im Unternehmen, durch die neue Angriffspunkte möglich werden?
- Gibt es eine veränderte Cloud- und Social-Media-Nutzung, die neue Gefahren mit sich bringt?
- Gibt es neue smarte Arbeitsmittel und Arbeitsverfahren, die Dritten einen Zugriff auf betriebsinterne Abläufe ermöglichen?
- Haben neue Extremwetterlagen Auswirkungen auf die Prozesse im Unternehmen?
- Hat die Gefährdung durch Infektionserkrankungen zugenommen und muss die Pandemieplanung entsprechend anpasst werden?
- Gibt es verstärkt verärgerte Kundinnen und Kunden, Lieferantinnen und Lieferanten und ehemalige Beschäftigte, von denen eine Gefährdung ausgeht?
- Haben sich gesellschaftliche Rahmenbedingungen verändert und haben diese Auswirkungen auf unser Unternehmen – zum Beispiel Extremismus, Terrorismus, Vandalismus, Provokateure, Shit-Storm?
- Wie hätte sich ein Ereignis, das bei einem anderen Unternehmen vorgekommen ist, bei uns ausgewirkt?

5

5.3 Risikobeurteilung mit der Gefährdungsbeurteilung verbinden

Auf den ersten Blick scheint die Risikobeurteilung ein zusätzliches Verfahren neben der gesetzlich geforderten Beurteilung der Arbeitsbedingungen (Gefährdungsbeurteilung) nach dem Arbeitsschutzgesetz zu sein.

Versuchen Sie, Ihren Aufwand dafür zu minimieren. Integrieren Sie die Risikobeurteilung idealerweise in die bereits vorhandene Gefährdungsbeurteilung. Dies bietet sich insbesondere deswegen an, weil die Systematik vergleichbar ist:

- Identifizieren von Gefährdungen oder Bedrohungen,
- Analyse und Bewertung,
- Festlegung von Maßnahmen,
- Umsetzung der Maßnahmen und
- Wirkungskontrolle.

Unterschiede gibt es nur in der Entwicklung von Szenarien und der Risikosteuerung.

Zeile bearbeiten

Bedrohungen
Musterunternehmen

Arbeitsbereich/Anwendungsbereich:
Produktion

Arbeitsumgebung/-mittel/-bedingung:

Teilbereich/Betrachtungsgegenstand/Tätigkeit:
Flachglas – Isolierglas

Gefährdung/Belastung:

Bedrohungsszenario:
Durch einen Fehler in dem nahe gelegenen Umspannwerk kommt es zu einem überregionalen Stromausfall mit einer Dauer von sechs Stunden. Das Notstromaggregat ist nur für die Sciherheitsbeleuchtung ausgelegt. Die Produktion steht still.

Risikobewertung

Risikobewertung | Risikobewertung mit Schutzmaßnahmen

Risikomaßzahl: 9
Koordinate: C3

	Keine erheblichen Verletzungen	Leichte Verletzungen	Mittel-schwere Verletzungen	Schwere Verletzungen	katastrophale/ tödliche Verletzungen
Fast ausgeschlossen	gering	gering	gering	gering	gering
sehr unwahrscheinlich	gering	gering	mittel	mittel	mittel
unwahrscheinlich	gering	mittel	**mittel**	hoch	hoch
wahrscheinlich	gering	mittel	hoch	hoch	hoch
sehr wahrscheinlich	gering	mittel	hoch	hoch	hoch

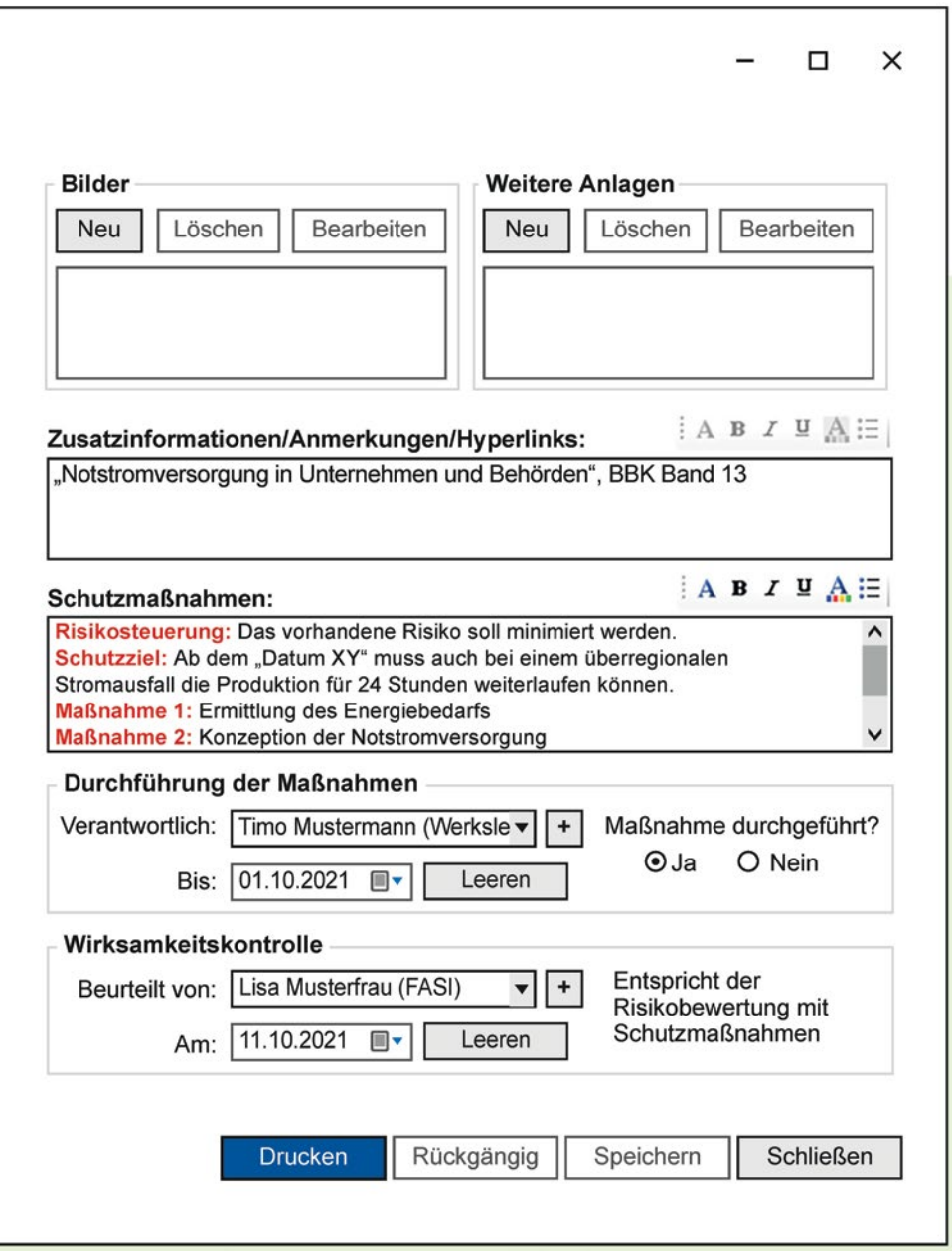
Abbildung 7: Gefährdungsbeurteilung – Software GEDOKU der VBG

In vielen Fällen lassen sich Risiken von Bedrohungen auch kaum von Gefährdungen aus den Arbeitsbedingungen trennen.

Wenn zum Beispiel die Bedrohung „starker Schneefall“ heißt, müssen Sie sich aus Sicht des Arbeitsschutzes die Fragen stellen:

- Wie kann die Schneelast sicher von den Dächern beseitigt werden?
- Welche Hilfsmittel benötigt der Betrieb dafür und wer setzt die Maßnahmen um?

Zur Gefährdungsbeurteilung können Sie beispielsweise die Software GEDOKU der VBG nutzen. Erweitern Sie die vorhandenen Gefährdungsfaktoren durch die identifizierten Bedrohungen – siehe Abbildung 7.



Vertiefendes Wissen

Für die Risikobeurteilung von Bedrohungen und Notfällen gibt es auch weitere systematische Verfahren, die allerdings für kleine und mittlere Unternehmen oft zu komplex sind. Dazu gehören beispielsweise:

- das **PAAG**-Verfahren (Prognose-Auffinden-Abschätzen-Gegenmaßnahmen),
- das **HAZOP**-Verfahren (Hazard and Operability),
- die **SWOT**-Analyse (Strengths, Weaknesses, Opportunities and Threats),
- die **FMEA** (Fehlermöglichkeits- und Einflussanalyse),
- die **Fehlerbaumanalyse** oder
- die **Delphi**-Methode.

6

6 Notfallorganisation: Gut organisiert den Ernstfall meistern

Die Notfallvorsorge und Notfallnachsorge

Während wir uns in dieser Schrift bisher mit der Prävention von möglichen Bedrohungen befasst haben, kommen wir jetzt zum Umgang mit Notfällen. Dies bedeutet, auf mögliche Notfälle vorbereitet zu sein sowie eingetretene Notfälle erfolgreich bewältigen und aufarbeiten zu können oder mindestens ihre Auswirkungen zu reduzieren (Notfallorganisation).

Die Auswirkungen können unterschiedlich groß sein. So kann es im betrieblichen Alltag zu kleineren **Zwischenfällen** kommen, zu schwereren **Notfällen** oder zu **Katastrophen**, die sich zu existenzbedrohenden Krisen ausweiten können. In diesem Kapitel, das sich mit der Notfallorganisation befasst, betrachten wir in erster Linie den Notfall. Aber auch ein Zwischenfall kann zu einem Notfall eskalieren.

6.1 Den Notfall einplanen

Fakt ist: Risiken sind nicht immer beherrschbar, meist verbleiben Restrisiken. Eventuell haben Sie einzelne Bedrohungen unzureichend eingeschätzt oder diese bis dato gar nicht erkannt.

Beispiele:

- Restrisiko: Sie haben beispielsweise weitreichende Maßnahmen zur Verhinderung von Hackerangriffen festgelegt und umgesetzt. Dennoch müssen Sie mit einem Angriff rechnen, der Ihre Sicherheitssysteme überwindet.
- Falsche Einschätzung: Ein Ereignis kann schneller als erwartet eintreten und es können Reaktionen innerhalb kurzer Zeit erforderlich werden – zum Beispiel bei einem Hochwasser durch Starkregen.

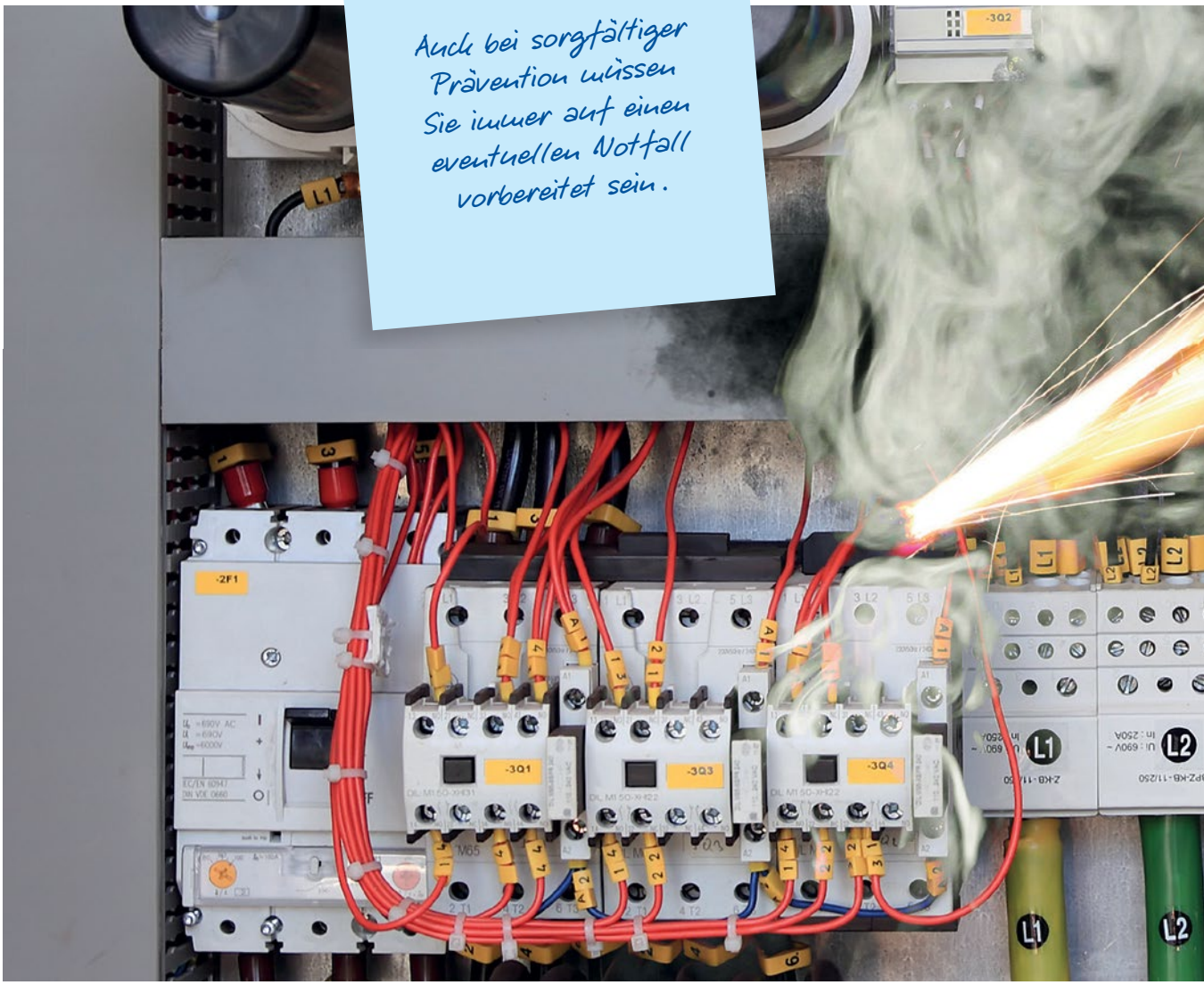
Wussten Sie, ...

... dass Cyberangriffe auf Unternehmen in den vergangenen Jahren stark zugenommen haben? In einer Befragung des Digitalverbands Bitkom gaben 2019 rund drei Viertel der Unternehmen an, Cyberattacken hätten stark beziehungsweise eher zugenommen. Besonders betroffen waren Unternehmen aus dem Sektor der Kritischen Infrastrukturen. 82 Prozent aller Befragten rechneten auch für die nähere Zukunft mit einer weiter wachsenden Gefahr von Cyberangriffen auf ihr Unternehmen.

(Quelle[14]: Bitkom, siehe Quellenverzeichnis)

6

Auch bei sorgfältiger Prävention müssen Sie immer auf einen eventuellen Notfall vorbereitet sein.



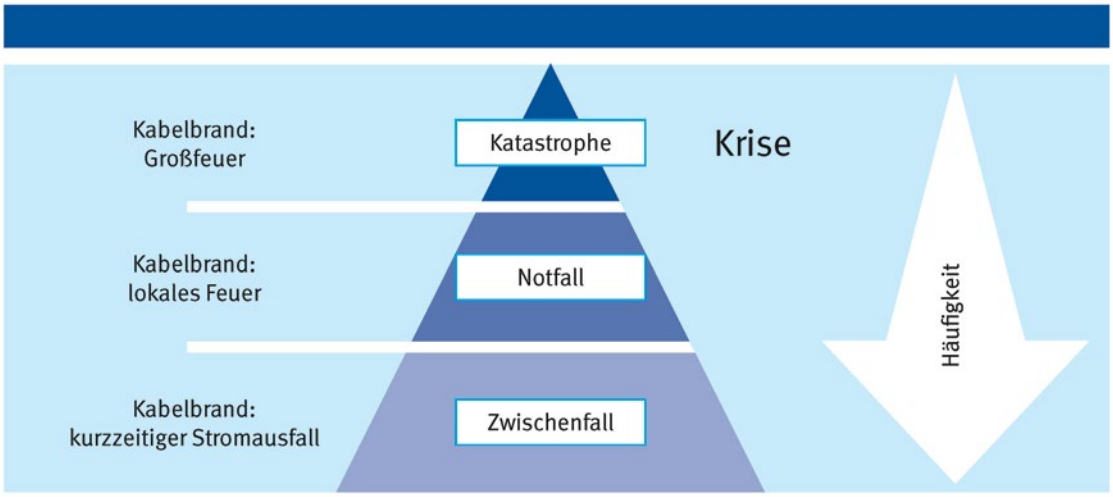
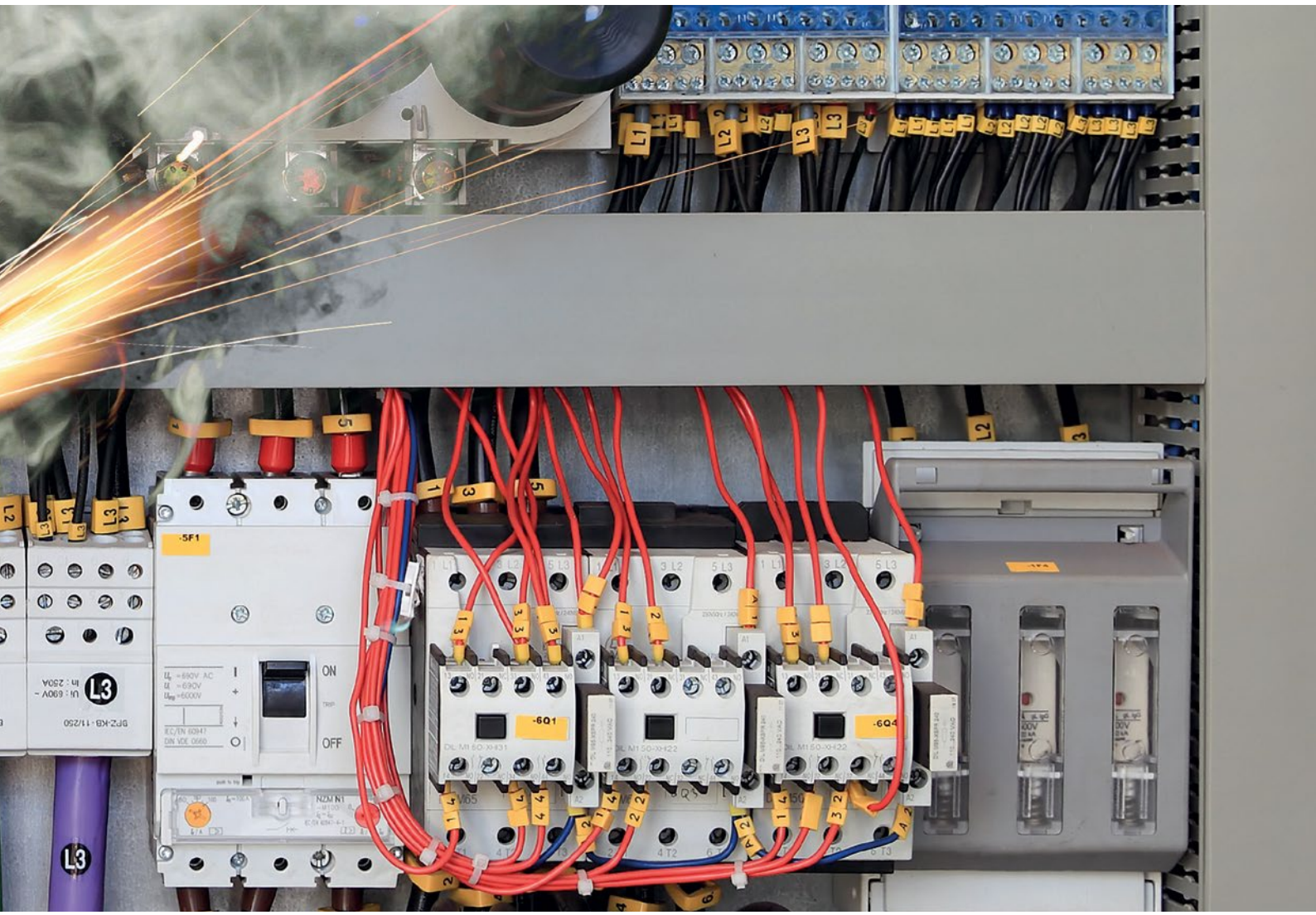


Abbildung 8: Stufen der Ereignisse – Beispiel: Kabelbrand



Es ist erforderlich, dass Sie zunächst den Ereignishorizont für Ihr Unternehmen bestimmen. Legen Sie bei einem Schadensereignis fest, ob es sich um einen Zwischenfall, einen Notfall oder eine Katastrophe handelt – siehe Abbildung 8. Der Ereignishorizont ist in jedem Unternehmen und in jeder Branche spezifisch und muss deswegen auf die Situation angepasst festgelegt werden. Auch die Dauer des Ereignisses kann eine Rolle spielen – ein längerfristiger Systemausfall hat umfassendere Auswirkungen als ein kurzfristiger.

Die Risikowahrnehmung ist individuell und von der Branche abhängig.

Beispielsweise kann ein Kabelbrand

- einen Zwischenfall darstellen, wenn es dadurch vorübergehend zu einem Stromausfall kommt und Arbeitsabläufe für einen kurzen Zeitraum unterbrochen werden,
- zu einem Notfall führen, wenn sich der Kabelbrand zu einem lokalen Feuer entwickelt, bei dem einige Beschäftigte Rauchvergiftungen erleiden und in den betroffenen Bereichen mehrere Tage lang nicht gearbeitet werden kann,
- eine Katastrophe auslösen, wenn sich der Kabelbrand zu einem Großfeuer entwickelt, bei dem Produktionsanlagen in erheblichem Umfang zerstört werden und darüber hinaus auch Beschäftigte schwer oder gar tödlich verletzt werden.

Eskalation vom Zwischenfall zur Katastrophe: siehe auch Kapitel 7.

6

6.2 Die erforderlichen Abläufe der Notfallorganisation sicherstellen

Bei der Notfallorganisation sollten Sie gut vorbereitet sein, falls ein Notfallereignis doch stattfinden sollte. In gewissen Bereichen, wie Brandschutz, Erste Hilfe oder Evakuierung, sind diese Maßnahmen bereits durch gesetzliche Regelungen vorgeschrieben. Beachten Sie bei der Vorsorge, dass Ereignisse sich sehr schnell entwickeln können – zum Beispiel ein Starkregen – oder andere sich über einen längeren Zeitraum entwickeln – wie zum Beispiel Schneefall. Die Zeitschiene ist ein wesentlicher Faktor, der Ihnen beispielsweise bei längeren Zeit- und Ereignishorizonten auch eine längere Reaktionszeit für koordinierte Handlungen lässt. Bei der Notfallvorsorge sollten sie folgendes beachten:

- **Die Abläufe detailliert beschreiben**

  Aus Ihren Bewertungen der Bedrohungen für Ihr Unternehmen und aus den Szenarien leitet sich ab, welche Notfälle Sie betrachten und berücksichtigen wollen. Auf diese Notfälle sollten Sie vorbereitet sein. Legen Sie die Abläufe fest, die bei einem eventuellen Notfall einzuhalten sind. Erstellen Sie beispielsweise einen Evakuierungsplan, dem die Maßnahmen und Abläufe bei einem Verlassen des Gebäudes zu entnehmen sind. Diese einheitlichen Informationen, welche Maßnahmen dann greifen und wie sich alle zu verhalten haben, sind die Grundlage einer erfolgreichen Notfallbewältigung. Diese Informationen können beispielsweise in Arbeitsanweisungen, Beschreibungen von Abläufen und Prozessen, Alarm- und Notfallplänen und in Checklisten vermittelt werden.

  Berücksichtigen Sie im Notfall auch die Anwesenheit von Fremdfirmen im Gebäude sowie von Besucherinnen und Besuchern – zum Beispiel bei einer Evakuierung.

- **Den Informationsfluss festlegen und sicherstellen**

Sie sollten die Meldekette sowie die Erreichbarkeit von Funktionsträgerinnen und -trägern sowie Einsatzkräften festlegen und sicherstellen. Bedenken Sie, die Abläufe auch in Papierform festzuhalten (beispielsweise in einem Notfallhandbuch, siehe Kapitel 6.3), um bei einem eventuellen Stromausfall handlungsfähig zu bleiben. Zu empfehlen ist eine festgelegte Notfallnummer im Unternehmen, unter der immer eine Person mit Entscheidungsbefugnis zu erreichen ist. Beschreiben Sie für eine jeweilige Bedrohung und den Notfall,
– wer informiert,
– wer informiert wird,
– wie informiert wird,
– mit wem kommuniziert wird (zum Beispiel externe Stellen).

Dies können Sie etwa mithilfe einer Meldematrix, im Alarm- und Meldeplan und im Rufnummernverzeichnis umsetzen.

Legen Sie auch fest, wie die Beschäftigten zu informieren sind. Dabei sind auch abwesende Beschäftigte und Beschäftigte von Fremdfirmen mit zu berücksichtigen. Für die identifizierten Notfallereignisse sollten Sie eine Erstinformation für die Beschäftigten zum Verhalten im Notfall vorbereiten – zum Beispiel einen Vordruck.

Sie sollen auch Regeln für die Notfall-Kommunikation vorgeben, idealerweise in kurzen und unmissverständlichen Anweisungen. Berücksichtigen Sie dabei auch den möglichen Ausfall beziehungsweise die Störung von Kommunikationsnetzen.

Planen Sie auch, wer die Öffentlichkeit informiert: Information an Behörden, Nachbarschaft, Presse, Social Media. Legen Sie auch vorab fest, wie dies geschieht. So stellen Sie sicher, dass nur abgestimmte und gesicherte Informationen herausgegeben werden.

Lassen Sie die für den Notfall erforderlichen Kommunikationseinrichtungen regelmäßig auf Funktionsfähigkeit überprüfen (zum Beispiel Batterien von Kommunikationsgeräten).

6

- **Verantwortliche Personen benennen**

  Bestimmen Sie die Personen, die für die Abläufe und die Maßnahmen im Notfall verantwortlich und weisungsbefugt sind. In kleinen und mittleren Unternehmen sollten dies die jeweils zuständigen Führungskräfte in ihrem jeweiligen Bereich sein. Sie sollten auch Vertretungen für die Verantwortlichen benennen, sodass auch im Falle von Urlaub, Krankheit, Dienstreise oder Wechselschicht die Abläufe gesichert sind.

- **Notwendige Qualifizierung sicherstellen**

  Gewährleisten Sie, dass die verantwortlichen und beteiligten Personen die entsprechenden Kompetenzen für die Vorsorge und Bewältigung einer Notfallsituation besitzen. Einen guten Einstieg bietet etwa das VBG-Seminar mit dem Kürzel „RINOA“.

Wussten Sie, ...

... dass das europäische Verbundsystem zu den sichersten Stromnetzen der Welt zählt? Dennoch steigen auch hierzulande die Risiken für großräumige und lang andauernde Stromausfälle (Blackouts). Die Faktoren, die ein stabiles Stromnetz gefährden, sind aufgrund von Klimawandel, Cyberattacken und Energiewende größer denn je. Fiele der Strom in mehreren Bundesländern über einen Zeitraum von drei Tagen oder länger aus, würde das in unserer hochentwickelten Gesellschaft zu katastrophalen Zuständen führen.

(Quelle[15]: Deutschlandfunk, siehe Quellenverzeichnis)

- **Personal zur Notfallbewältigung einplanen**

  Legen Sie fest, welche weiteren betrieblichen Personen in einer Notfall- beziehungsweise Bedrohungssituation spezielle Aufgaben übernehmen sollen: Ersthelferinnen und -helfer, Brandschutzhelferinnen und -helfer, Betriebsärztinnen und -ärzte, Fachkräfte für Arbeitssicherheit, Sicherheitspersonal, IT-Administratorinnen und -administratoren etc. Auch bei diesen Personen sollten Sie die jeweilige Eignung und Qualifikation für die Notfallbewältigung sicherstellen und gegebenenfalls Weiterbildungsmaßnahmen vorsehen.

  Je nach Betriebsgröße, Branche und Bedrohungslage kann es auch sinnvoll sein, einen qualifizierten **Risikomanager** beziehungsweise eine **Risikomanagerin** (beispielsweise nach ONR 49003) zu benennen, der oder die die Prozesse kontinuierlich analysiert und entsprechende Maßnahmen auf den Weg bringt. Manche Unternehmen setzen zusätzlich einen **Notfallmanager** beziehungsweise eine **Notfallmanagerin** ein, der oder die im Notfall die notwendigen Entscheidungen trifft. Die Begriffe „Risikomanager“ und „Notfallmanager“ sind keine fest definierten Funktionen, sondern werden sehr unterschiedlich verstanden.

- **Mit externen Partnern abstimmen**

  Legen Sie fest, mit welchen externen Stellen Sie zusammenarbeiten sollten beziehungsweise müssen: Feuerwehr, Polizei, Rettungsdienste, Unfallversicherungsträger, staatliche Arbeitsschutzbehörden, Gesundheitsämter, Wach- und Sicherheitsdienstleister, Sachverständige von Versicherungen, externe Fachleute sowie THW etc. Organisieren Sie ein Treffen mit wichtigen externen Partnern wie den genannten. Die Anforderungen und Erwartungen sollten mit diesen Institutionen abgestimmt werden. Hilfreich ist es, wenn sich die jeweiligen Kontaktpersonen aus dem eigenen Unternehmen und der Institution des wichtigen externen Partners persönlich kennen.

- **Einrichtungen und Einsatzmittel zur Verfügung stellen**

  Stellen Sie sicher, dass die Einrichtungen und Einsatzmittel, die zur Bewältigung des Notfalls und der Bedrohung notwendig sind, im Betrieb vorhanden und funktionsfähig sind: Erste-Hilfe-Material, Löscheinrichtungen, Warn- und Signaleinrichtungen, Rettungseinrichtungen und -geräte, Kennzeichnungen, Überwachungseinrichtungen, technische Zugangskontrollen, Einbruchmeldeanlagen (EMA), Überfallmeldeanlagen (ÜMA), Brandmeldeanlagen (BMA), Störmeldeanlagen und -einrichtungen, Biometrische Systeme, Sicherheitstüren und -fenster (Drehtüren, Drehschleusen, Drehsperren), Notstromersatzanlagen etc.

- **Information und Training von Führungskräften und Beschäftigten**

  Sorgen Sie dafür, dass Ihre Führungskräfte und Beschäftigten über die festgelegten Schutzziele und Maßnahmen für das Verhalten im Notfall informiert sind. Diese Informationen sollten in regelmäßigen Abständen wiederholt werden beziehungsweise in Zusammenhang mit anderen Unterweisungen erfolgen. Bei Veränderungen im Ablauf sollten Ihre Führungskräfte die Beschäftigten anlassbezogen über die neuen Anforderungen informieren. Anlässe könnten neue Bedrohungen, eine neue Software, Änderungen in Arbeitsprozessen, ein Wechsel des Arbeitsbereiches, bauliche Veränderungen im Unternehmen oder Ähnliches sein. Neue Beschäftigte müssen im Rahmen ihrer allgemeinen Ersteinweisung über die Maßnahmen zur Notfallbewältigung informiert werden.

„Übung macht den Meister“: Lassen Sie auch einzelne Abläufe praktisch trainieren und üben.

Bei den Informationen und Unterweisungen sollten Sie über die möglichen Auslöser für Notfälle informieren. Hilfreich sind hier die ermittelten Notfallszenarien.

Lassen Sie auch einzelne Abläufe praktisch trainieren und üben, wie zum Beispiel den Aufbau von Hochwasserwänden, die Handhabung von Alarmierungseinrichtungen und Feuerlöschern sowie den Ablauf von Evakuierungen und Informationsflüssen. Nur durch regelmäßige Übungen kann im Ereignisfall ein weitgehend reibungsloser Ablauf der Notfallbewältigung erzielt werden. Durch Training und Übungen überprüfen Sie schließlich auch die Funktion von Prozessen, Einrichtungen und Einsatzmitteln. Üben Sie Notfallsituationen auch mit externen Stellen, damit im Ereignisfall alle wissen, wie die Zusammenarbeit funktioniert. Bewerten Sie Trainings und Übungen, um ein etwaiges Verbesserungspotenzial zu erkennen.

6

- **Thema Notfälle regelmäßig ansprechen**

  Sprechen Sie die Maßnahmen zur Notfallbewältigung regelmäßig in Gesprächen mit Ihren Führungskräften an. Diese sollten wiederum in den Team-Besprechungen mit den Beschäftigten das Thema Notfallorganisation turnusmäßig auf die Agenda setzen. Dabei sollten die Beschäftigten die Möglichkeit haben, eventuelle neue Erfahrungen und Erkenntnisse über Schwachstellen und im Rahmen einer offenen Fehlerkultur Mängel mitzuteilen.

- **Schnittstellen und Integration in die Gesamtprozesse**

  Integrieren Sie die Maßnahmen zur Notfallorganisation in die vorhandenen Betriebsabläufe: Unternehmenspolitik, Personal-, Technologie-, Gebäudemanagement, Beschaffung, Prozess- und Projektmanagement etc. Die Notfallmaßnahmen sollten Bestandteil der alltäglichen Abläufe werden.

- **Psychische Hilfe bei Extremsituationen planen**

  Bei Überfällen, kriminellen Handlungen, Naturereignissen, schweren Personenunfällen (Suizide im ÖPNV) und ähnlichen Ausnahmesituationen kann es zu extremen psychischen Belastungen (posttraumatisches Belastungssyndrom) von Beschäftigten kommen. Planen und organisieren Sie entsprechende Betreuung für Beschäftigte, die durch traumatische Ereignisse belastet sein können.

Wussten Sie, …

… dass es im Jahr 2020 in Deutschland 678 Schienensuizide gab? Statistisch gesehen erlebt nahezu jeder Lokführer oder jede Lokführerin im Laufe seines oder ihres Berufslebens mindestens einmal einen Schienensuizid.

(Quelle[16]: Eisenbahn-Bundesamt, siehe Quellenverzeichnis)

Stellen Sie sicher, dass Führungskräfte und Beschäftigte sich um die Betroffenen kümmern und sie angemessen unterstützen (Erstbetreuerinnen und -betreuer bei Notfällen). Wenn Beschäftigte durch Extremsituationen psychisch belastet werden, sollte auf jeden Fall ärztliche Hilfe in Anspruch genommen werden. Erste Anlaufstellen sind beispielsweise zuständige Betriebs- oder Durchgangsärzte beziehungsweise -ärztinnen. Außerdem sollten Sie eine Unfallanzeige erstellen. Die VBG unterstützt Sie in solchen Fällen durch spezielle Reha-Managerinnen und -manager.

Wussten Sie, …

… dass ein traumatisches Ereignis wie ein Banküberfall im betrieblichen Zusammenhang als Arbeitsunfall gemeldet werden kann?

(Quelle[17]: VBG, siehe Quellenverzeichnis)

Organisieren Sie, dass der Umgang mit traumatischen Ereignissen in der Gefährdungsbeurteilung berücksichtigt wird. Bei einem traumatischen Ereignis hilft Ihnen die VBG bei der weiteren psychologischen Betreuung der Betroffenen (mehr Informationen: DGUV Information 206-017). Überlegen Sie gemeinsam mit den betroffenen Beschäftigten, wie diese nach Notfällen und Katastrophen im Unternehmen eingesetzt werden wollen und können. Ziehen Sie dabei den Betriebsarzt beziehungsweise die Betriebsärztin hinzu.

In Branchen mit Kundenverkehr (zum Beispiel ÖPNV, Freizeitparks, Bildungseinrichtungen, Banken) und in größeren Unternehmen sowie für Hilfsorganisationen und Einsatzkräfte kann es sinnvoll sein, Beschäftigte als **psychologische Erstbetreuer und Erstbetreuerinnen** (DGUV Information 206-023) auszubilden beziehungsweise zu qualifizieren. Diese Personengruppe hilft nach belastenden Ereignissen bei der psychosozialen Notfallversorgung und sie kümmert sich um die Betroffenen.

In Bildungseinrichtungen kommt häufig auch ein **„Krisenteam“** oder ein **„Krisen-Interventions-Team (KIT)“** zum Einsatz, dessen Mitglieder aus der Belegschaft stammen. KITs sind auch bei den Rettungs-/Hilfsorganisationen oder im seelsorgerischen Bereich vorhanden, die bei schweren Unfällen zum Einsatz kommen.

- **Aktualisierung der Dokumente**

  Legen Sie fest, wer für die Erstellung beziehungsweise Aktualisierung, Freigabe und Weitergabe von Dokumenten über die Maßnahmen bei Bedrohungen und Notfällen zuständig ist: Zugangsberechtigungen, Passwörter, Unterlagen zur Anlagen- und IT-Sicherheit etc.

6

6.3 Hilfreich: das Notfallhandbuch

Eine Hilfe zur Notfallorganisation ist ein Notfallhandbuch. Es hilft, einen **schnellen Überblick** zu gewinnen und die Prozesse zu systematisieren. Das Notfallhandbuch dient als Informationsquelle für alle erforderlichen Prozesse und Maßnahmen. Es unterstützt somit die Führungskräfte und die für die Notfallbewältigung verantwortlichen Personen. Es soll im Notfall eine schnelle Reaktion und idealerweise eine reibungslose Bewältigung für die jeweils betrachteten Szenarien sicherstellen.

Das **Notfallhandbuch** kann je nach Zielrichtung zum Beispiel folgende **Inhalte** haben:

1. Geltungsbereich und Ziele
2. Definitionen
3. Rollen, Verantwortlichkeiten und Kompetenzen
4. Alarmierungs- und Eskalationswege
5. Im Notfall zu berücksichtigende Schnittstellen
6. Notfalltreffpunkte und benötigte Ressourcen
7. Notfallpläne
8. Notfallkommunikation
9. Ergänzende Informationen und Pläne

Ein Notfallhandbuch ist ein individuelles Dokument und beschreibt Ihr Unternehmen sehr detailliert. Die Inhalte sind unternehmensbezogen zu erarbeiten und beispielsweise in die oben vorgeschlagene Gliederungsstruktur einzufügen. Das Notfallhandbuch sollte regelmäßig geprüft und bei Bedarf aktualisiert und ergänzt werden.

Beachten Sie für Notfälle unbedingt, dass das Notfallhandbuch auch in gedruckter Form (mehrere Exemplare) vorliegt, damit bei einem System- oder Stromausfall darauf zurückgegriffen werden kann.

Vorlagen und Muster für Notfallhandbücher finden Sie im Internet, zum Beispiel unter www.wirtschaftsschutz.info.

Für Schulen stellen unter anderem die jeweiligen Bundesländer entsprechende Vorlagen für Notfallhandbücher zur Verfügung. Diese können auch von Bildungseinrichtungen genutzt und auf ihre Bedürfnisse angepasst werden.

6.4 Die Notfallnachsorge

Ist es zu einem Notfallereignis im Betrieb gekommen, sollten Sie überprüfen, ob die Maßnahmen der **Notfallvorsorge und -bewältigung** gegriffen beziehungsweise welche Schwachstellen sich ergeben haben.

Wenn beispielsweise ein Brand eines Papierkorbs in einem Büro mit einem älteren ABC-Pulver-Feuerlöscher gelöscht wurde, könnten durch das fein verteilte Feuerlöschmittel Computer, Möbel und Akten verunreinigt und beschädigt worden sein. Der Sachversicherer würde in diesem Fall möglicherweise den Schaden durch das ungeeignete Löschmittel nicht übernehmen. Mit einem geeigneten Schaumlöscher wären diese Folgeschäden nicht entstanden. Als Lehre aus dieser Erfahrung beschließt das Unternehmen anschließend, die Feuerlöschmittel im Büro auf Schaum-/Wasserlöschmittel umzustellen.

Bei der Überprüfung der Maßnahmen zur Notfallvorsorge und -bewältigung können unter anderem folgende Fragen helfen:

- Sind die Abläufe der Notfallbewältigung generell wie geplant umgesetzt worden?
- Hat die Meldekette funktioniert und war der Informationsfluss reibungslos?
- Haben die verantwortlichen Personen und Führungskräfte effektiv handeln können?
- Konnten die festgelegten Maßnahmen wirksam umgesetzt werden?
- Wie haben die Einsatz- und Unterstützungskräfte gearbeitet?
- Haben die Führungskräfte und Beschäftigten gewusst, wie sie sich verhalten müssen?
- Wie war die Zusammenarbeit mit den externen Stellen? Wie hat die Kommunikation mit diesen externen Stellen funktioniert (auch die Öffentlichkeitsarbeit)?
- Wie war der Umgang mit den Beschäftigten von Fremdfirmen im Gebäude sowie mit Besucherinnen und Besuchern?
- Haben die Einrichtungen, Einsatzmittel und Materialien für den Notfall funktioniert und haben sie sich bewährt?
- Sind einzelne Personen psychisch besonders belastet worden, sodass Unterstützungsmaßnahmen erforderlich wurden?
- Hätte der eingetretene Schaden durch andere Maßnahmen wirkungsvoller eingedämmt werden können beziehungsweise war die Risikosteuerung richtig?
- Gibt es andere Unternehmen (wie benachbarte Firmen), die auch von dem Ereignis betroffen waren, und mit denen ein Erfahrungsaustausch hilfreich sein kann?
- Muss das Notfallhandbuch angepasst werden?

7

7 Krisen- und Kontinuitätsmanagement: Bewältigung von Extremsituationen

Aus eskalierenden Notfallereignissen oder Katastrophen können sich Krisen ergeben, die Leben bedrohen und zu einer existenzbedrohenden Extremsituation führen können. Die Notfallorganisation reicht in der Regel nicht dazu aus, derartige Krisen zu bewältigen.

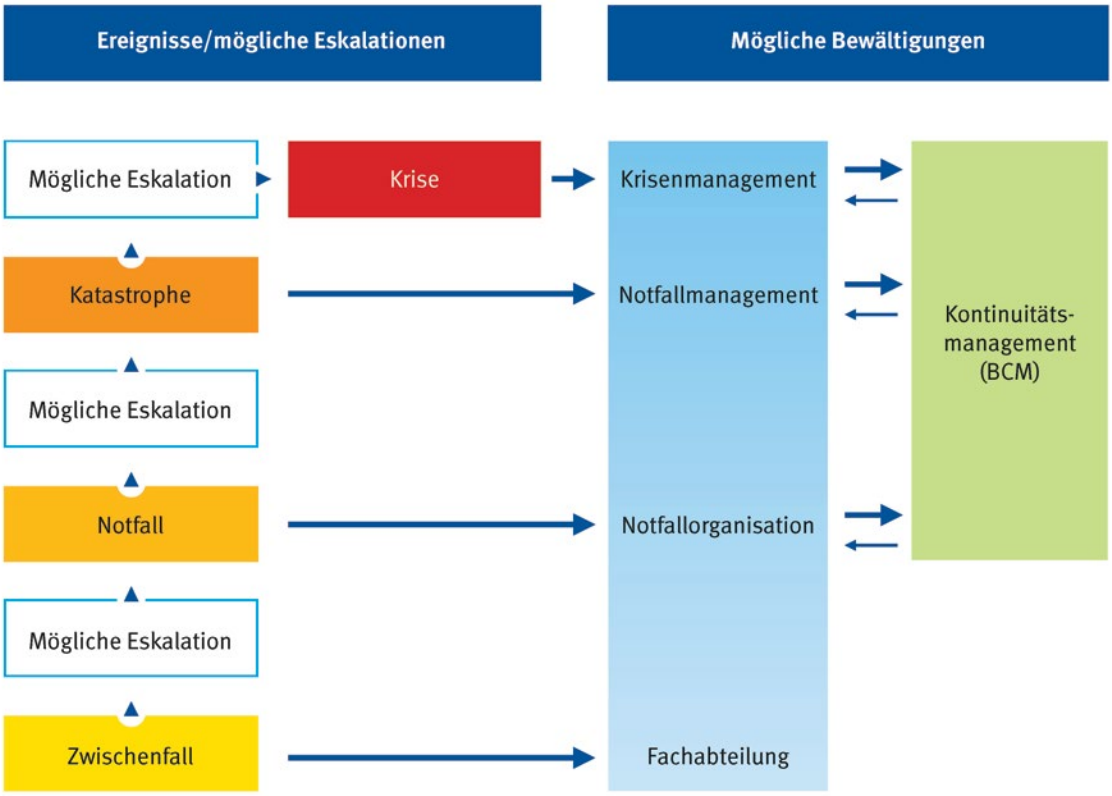


Abbildung 9: Bewältigungsstrategien in Abhängigkeit der Eskalationsstufe

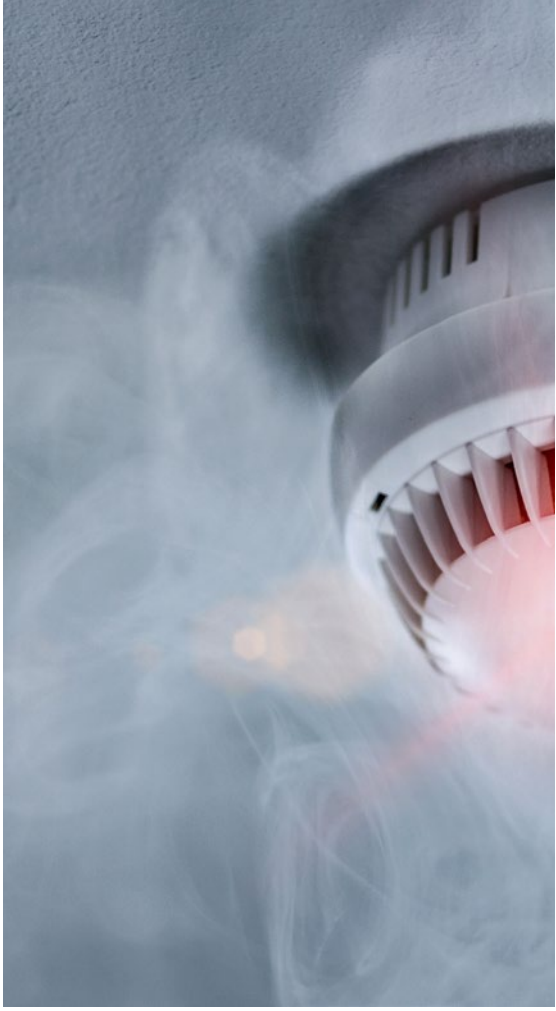
Der Umgang mit Krisen erfordert üblicherweise eine besondere Organisationsstruktur, die aber in der Regel nur in größeren Betrieben möglich und sinnvoll ist. Kleinere Firmen können auch in Krisen geraten. Sie haben aber wegen fehlender Ressourcen oft nicht die Möglichkeit, eine eigene Organisationsstruktur 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 der Unternehmer oder die Unternehmerin und seine/ihre Führungskräfte diese Aufgabe.

Sinngemäß gelten diese Überlegungen auch für das sogenannte Kontinuitätsmanagement (siehe 7.2).

Begriffsklärung: Krise

Eine Krise ist eine komplexe Situation, die für eine Organisation existenzgefährdend sein kann. Die Krisenbewältigung erfordert organisationsweit außerordentliche Maßnahmen, weil bestehende Organisationsstrukturen und Prozesse (zum Beispiel eine Notfallorganisation) nicht ausreichen.
Die Krise kann durch einen eskalierten Notfall oder direkt durch eine Katastrophe ausgelöst werden.

7



7.1 Krisenmanagement

Trotz aller Maßnahmen zur Risikovermeidung oder -minimierung verbleiben in jedem Unternehmen Restrisiken, die bei geringer Eintrittswahrscheinlichkeit erhebliche Auswirkungen haben können. Aus eskalierenden Notfallereignissen oder Katastrophen können sich Krisen ergeben, die zu einer existenzbedrohenden Extremsituation führen können.

Beispiel 1: Notfall

Ausgelöst durch ein defektes Arbeitsmittel, kommt es in einem Unternehmen zu einem Brand, bei dem eine Lagerhalle zerstört wird. Die Notfallbewältigung erfolgt im Rahmen der festgelegten Abläufe und Alarmpläne. Personen wurden nicht verletzt. Die Auswirkungen für den Betrieb sind erheblich, können aber in Grenzen gehalten werden, weil durch Schutzmaßnahmen die Ausbreitung des Brandes auf andere Betriebsbereiche verhindert werden konnte.

Das Notfallereignis konnte mit der vorhandenen Notfallorganisation bewältigt werden.

Beispiel 2: Katastrophe

In einem Unternehmen fängt aufgrund eines defekten Arbeitsmittels zunächst nur ein einzelnes Lagergebäude Feuer. Durch ungünstige Windverhältnisse greift das Feuer anschließend auf benachbarte Produktionshallen über. Dabei werden auch Gefahrstoffe freigesetzt.

Nachdem der Brand gelöscht wurde, ergeben Messungen, dass Anwohner nicht gefährdet wurden. Da das Unternehmen nachweisen konnte, dass alle notwendigen Arbeitsmittelprüfungen durchgeführt wurden, wird der Schaden durch den Sachversicherer reguliert. Trotzdem entsteht dem Unternehmen aufgrund des Produktionsausfalls ein Millionenschaden.

Ein Notfallereignis eskaliert zur Katastrophe. Eine existenzbedrohende Situation konnte noch abgewendet wird.

Beispiel 3: Krise infolge einer Katastrophe

In einem Unternehmen der Feuerwerksindustrie brennt aufgrund eines defekten Arbeitsmittels eine Lagerhalle ab. Die Notfallbewältigung läuft nicht wie geplant, sodass das Feuer auf weitere Gebäude übergreift. Da ein Notausgang versperrt war, kommen drei Beschäftigte ums Leben. Nach diesem katastrophalen Ereignis wird – auch durch eine schlechte Öffentlichkeitsarbeit der Verantwortlichen – die gesamte Feuerwerksproduktion an diesem Standort seitens der Politik infrage gestellt. Das Werk schließt auf Druck der Behörden und auch der Öffentlichkeit innerhalb eines halben Jahres.

Ein Notfallereignis eskaliert zur Katastrophe und entwickelt sich zur Unternehmenskrise. Mit einem gut funktionierenden Krisenmanagement hätte das Unternehmen vermutlich eine positivere Entwicklung ermöglichen und eine Schließung des Werks abwenden können.

Bei Ihrer Notfallorganisation sollten Sie deshalb immer mitberücksichtigen, dass diese für extrem seltene Ereignisse, wie einen Krisenfall, in der Regel nicht gerüstet ist. Hierzu bedarf es einer speziellen Organisationsstruktur, die in größeren Betrieben als Krisenmanagement bezeichnet wird.

Die Krisenorganisation ist eine spezielle Organisationsstruktur neben der Notfallorganisation.

Bei der Vorbereitung und Bewältigung von Krisen sollten deshalb zusätzlich speziell zur Notfallorganisation unter anderem folgende Aspekte berücksichtigt werden:

- Verantwortliche Personen für die Bewältigung der Krisensituation bestimmen und vorbereiten. Die grundlegende Verantwortung liegt bei der Unternehmensleitung.
- Einen Krisenstab einrichten und festlegen, welche taktischen Aufgaben dieser übernehmen soll. Die Mitglieder des Krisenstabs benennen und qualifizieren.
- Festlegen, welche Expertinnen und Experten im Krisenfall hinzugezogen werden müssen: Feuerwehr, Werkschutz (in größeren Betrieben), Spezialistinnen und Spezialisten zum Beispiel für Gefahrstoffe oder IT-Fachleute, Behördenvertreterinnen und -vertreter.
- Festlegen, wie die Informations- und Kommunikationsflüsse im Krisenfall verlaufen sollen (Krisenkommunikation).
- Einen Krisenstabsraum einrichten, der unabhängig vom Katastrophengeschehen zu nutzen ist.

7

7.2 Kontinuitätsmanagement – Business Continuity Management (BCM)

Neben der Notfallorganisation und dem Krisenmanagement ist es wichtig, wie der Betrieb nach eingetretenen Ereignissen mit hoher Schadensschwere möglichst schnell verlorene kritische Betriebsfunktionen wiederherstellen und somit zum Normalbetrieb zurückkehren kann.

Hiermit befasst sich das Kontinuitätsmanagement oder auch Business Continuity Management (BCM).

Die Business Impact Analyse (BIA) ist dabei ein zentraler Baustein des Kontinuitätsmanagements. Diese Methode zielt darauf ab, kritische Geschäftsprozesse, die für die Aufrechterhaltung des Geschäftsbetriebes notwendig sind, zu identifizieren und festzustellen, welche Folgen ein Ausfall haben kann. Diese kritischen Prozesse werden anschließend durch ein Maßnahmenpaket besonders abgesichert.

Die Business Impact Analyse kann in vereinfachter Form in nachfolgende Schritte unterteilt werden:

- **Auswahl der kritischen Geschäftsprozesse**

  Üblicherweise können diese in Kernprozesse (strategische und operative) sowie unterstützende Prozesse (Informationstechnologie, Stabsstellen, Öffentlichkeitsarbeit) untergliedert werden. Wie stark die Untergliederung der Prozesse in Teilprozesse stattfinden soll, hängt von der Art, Größe und Struktur des Betriebes ab.

- **Schadensanalyse**

  Hierbei wird der Schaden, der aus dem Ausfall eines Prozesses resultiert, näher untersucht, insbesondere vor dem Hintergrund des zeitlichen Ablaufs. Dazu werden Schadenskategorien definiert. Bewährt haben sich solche Kategorien, die sich nicht nur am monetären Schaden orientieren, sondern auch andere direkte und indirekte Schäden mit einbeziehen (wie etwa Imageverluste, Verstöße gegen Vorschriften oder Verträge).

- **Festlegung der Wiederanlaufparameter**

  Hierbei gilt es, die maximal tolerierbare Ausfallzeit (MTA) und Wiederanlaufzeit (WAZ) zu bestimmen. Die MTA bezeichnet den Zeitrahmen, in dem der Wiederanlauf eines Prozesses spätestens beginnen muss, damit das Unternehmen nicht in eine existenzbedrohende Lage kommt. Dagegen ist die WAZ die Zeitspanne, die erforderlich ist, um einen Prozess nach einem Ausfall wieder in einen Notbetrieb beziehungsweise in einen voll funktionsfähigen Betrieb zu überführen.

- **Festlegung der Ressourcen für den Normalbetrieb und den Schadensfall (Notbetrieb)**

  Prozesse sind eng mit dem Vorhandensein von Ressourcen verknüpft. Deshalb müssen für die als kritisch definierten Prozesse die notwendigen Ressourcen ermittelt werden.

  Dazu gehören insbesondere:

  – Personal (eigene Beschäftigte, Fremdpersonal, Beschäftigte mit Spezialwissen etc.),
  – Infrastruktur (Gebäude, Lagerflächen, Büroräume etc.),
  – Anlagen und Geräte (Stromversorgung, Wasserversorgung, Energieversorgung, Informations- und Kommunikationstechnik etc.),
  – Betriebsmittel (Rohstoffe etc.).

8

8 Alles selber machen?

Wann ist es sinnvoll, sich unterstützen zu lassen und wer kann helfen?

Als Unternehmerin beziehungsweise Unternehmer können Sie nicht alle Fakten zu sämtlichen Bedrohungen selbst zusammentragen. Deshalb sind nachfolgend exemplarisch einige Institutionen und Einrichtungen aufgeführt, bei denen Sie weiterführende Informationen und Praxishilfen abrufen können. Weiterhin bietet Ihnen die VBG zu diesem Themenkomplex ein Seminar mit dem Kürzel „RINOA“ an, in dem Sie oder eine Person aus dem Kreis Ihrer Führungskräfte weitere Kenntnisse für Ihr Unternehmen erwerben können.

Weitere Institutionen, bei denen Sie bei Bedarf Informationen und Praxishilfen abrufen können, sind unter anderem:

… für Fragen zur aktuellen Sicherheitslage und des Katastrophenschutzes:

- Bundesministerium des Innern (BMI) ⋯› www.bmi.bund.de
- Auswärtiges Amt (AA) ⋯› www.auswaertiges-amt.de
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ⋯› www.bbk.bund.de
- Center for Disaster Management and Risk Reduction Technology (CEDIM) ⋯› www.cedim.de

… für Fragen zur Gefährdung durch Krankheitserreger:

- Bundesministerium für Gesundheit (BMG) ⋯› www.bundesgesundheitsministerium.de
- Robert Koch-Institut (RKI) ⋯› www.rki.de
- Friedrich-Loeffler-Institut (FLI) ⋯› www.fli.bund.de

… für Fragen zum Brandschutz:

- Deutscher Feuerwehrverband e. V. (DFV) ⋯› www.dfv.org
- Vereinigung zur Förderung des Deutschen Brandschutzes e. V. (vfdb) ⋯› www.vfdb.de

… für Fragen zur Gebäudesicherung:

- VdS Schadenverhütung GmbH ⋯› www.vds.de
- Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen e. V. (BHE) ⋯› www.bhe.de
- Bundesverband Sicherungstechnik Deutschland e. V. (BSD) ⋯› www.bsd-ev.de
- Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI) ⋯› www.zvei.org
- Portal Sichere Schule (bei der DGUV; Hrsg.) ⋯› www.sichere-schule.de
- Deutsche Gesellschaft für wirtschaftliche Zusammenarbeit (DGWZ) ⋯› www.dgwz.de

8

... für Fragen zur IT-Sicherheit und zur Computer-Kriminalität:

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  ⋯⁘ www.bsi.bund.de
- Zentrale Ansprechstellen Cybercrime (ZAC) der Polizeien für Wirtschaftsunternehmen ⋯⁘ www.polizei.de, Telefon länderspezifisch
- IT-Förderprogramme – Förderdatenbank des Bundeswirtschaftsministeriums
  ⋯⁘ www.foerderdatenbank.de

... für Fragen zu Notfallhandbüchern und -plänen:

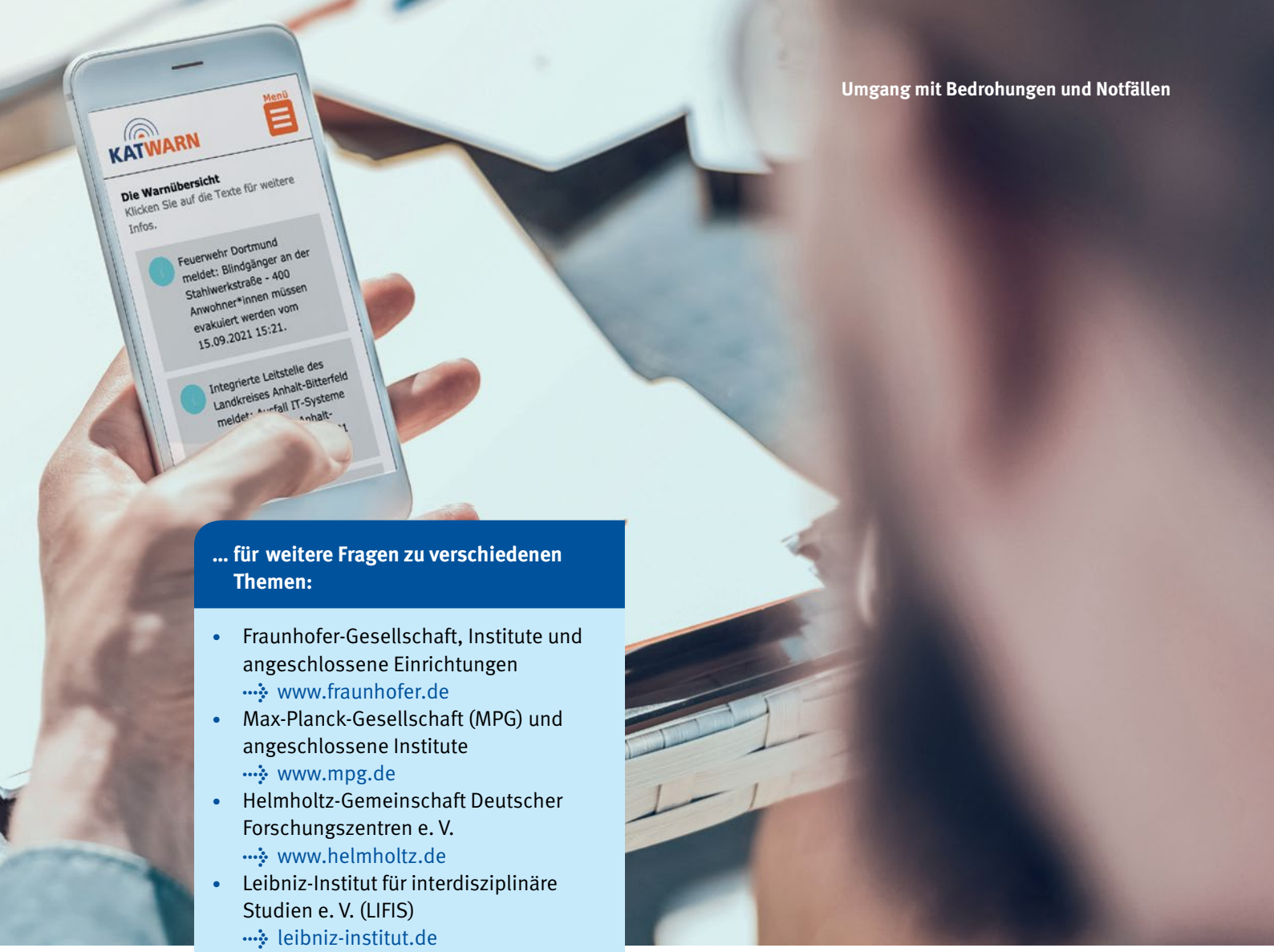
- Berufsgenossenschaft Rohstoffe und chemische Industrie (BG RCI); hier Ordner: Praxishilfe – Gerüstet für den Notfall
  ⋯⁘ www.bgrci.de
- Deutsche Industrie- und Handelskammern (IHK)
  ⋯⁘ www.ihk-notfallhandbuch.de
- beispielhaft für Schulen; in Berlin: Senatsverwaltung für Bildung, Jugend und Familie
  ⋯⁘ www.berlin.de

... für Fragen zur Sicherheit im Wirtschaftsleben:

- BMWi „Geheim- und Sabotageschutz in der Wirtschaft“
  ⋯⁘ www.bmwi.de
- Initiative Wirtschaftsschutz beim Bundesamt für Verfassungsschutz (hier finden Sie auch ein Muster für ein Notfallhandbuch)
  ⋯⁘ www.wirtschaftsschutz.info
- Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V. (ASW)
  ⋯⁘ www.asw-bundesverband.de

... für Fragen zu Naturgefahren und zum Klimawandel:

- Umweltbundesamt
  ⋯⁘ www.umweltbundesamt.de
- Bundesanstalt für Geowissenschaften und Rohstoffe (BGR)
  ⋯⁘ www.bgr.bund.de
- Deutsches GeoForschungsZentrum, Helmholtz-Zentrum Potsdam (GFZ)
  ⋯⁘ www.gfz-potsdam.de
- Deutscher Wetterdienst (DWD)
  ⋯⁘ www.dwd.de
- Potsdam-Institut für Klimafolgenforschung (PIK)
  ⋯⁘ www.pik-potsdam.de



... für weitere Fragen zu verschiedenen Themen:

- Fraunhofer-Gesellschaft, Institute und angeschlossene Einrichtungen
  www.fraunhofer.de
- Max-Planck-Gesellschaft (MPG) und angeschlossene Institute
  www.mpg.de
- Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
  www.helmholtz.de
- Leibniz-Institut für interdisziplinäre Studien e. V. (LIFIS)
  leibniz-institut.de
- Warn-App NINA (für das Mobiltelefon) des BBK unter
  www.bbk.bund.de
- Reise-App „Sicher Reisen“ des Auswärtigen Amtes für eine sichere und möglichst reibungslose Auslandsreise unter
  www.auswaertiges-amt.de

Hinweise zu den vorgenannten Aufzählungen:

Die oben aufgeführten Institutionen und Einrichtungen sind eine beispielhafte Aufzählung und erheben keinen Anspruch auf Vollständigkeit. Bitte beachten Sie, dass die Bezeichnungen von Homepages Änderungen unterliegen können. Aufgrund der föderalen Struktur der Bundesrepublik Deutschland unterliegen viele Zuständigkeiten und Kompetenzen im thematischen Zusammenhang mit dieser Schrift den jeweiligen Bundesländern. Dies ist zum Beispiel beim Hochwasserschutz (und Schutz gegen andere Naturgefahren) und im Bildungsbereich der Fall. Die damit verbundene hohe Zahl von Links zu diesen länderspezifischen Informationen kann daher in der vorgenannten Aufzählung nicht berücksichtigt werden.

8 Glossar

Erläuterung zentraler Begriffe dieser Schrift

Bedrohung: Potenzielle Quelle eines Risikos, die zu einer ungünstigen Entwicklung führen kann. Das Gegenteil der Bedrohung ist die Chance.

Gefahr: Potenzielle Quelle eines Risikos, die zu einem plötzlich eintretenden Schadensereignis führen kann.

Gefährdung: Gefahr, die sich negativ auf Personen (auch Sachen oder Ziele) auswirken kann.

Katastrophe: Ereignis mit extremem Schadensausmaß, das stark über die Ausmaße von Schadensereignissen, wie zum Beispiel Notfälle, hinausgeht und dabei Leben, Gesundheit, Sachgüter oder wichtige Infrastrukturen erheblich gefährdet oder zerstört. Aus einer Katastrophe kann sich unternehmensintern eine Krise entwickeln. Katastrophen kommen äußerst selten vor.

Krise: Komplexe Situation, die für eine Organisation existenzgefährdend ist. Die Krisenbewältigung erfordert organisationsweit außerordentliche Maßnahmen, weil bestehende Organisationsstrukturen und Prozesse (zum Beispiel eine Notfallorganisation) nicht ausreichen. Die Krise kann durch einen eskalierten Notfall oder direkt durch eine Katastrophe ausgelöst werden.

Krisenmanagement: Prozesse, Verhaltensweisen und koordinierte Tätigkeiten, die eine Organisation ausführen muss, um eine Krise zu bewältigen.

Notfall: Ereignis mit hohem Schadensausmaß. Notfälle können sich zu einer Katastrophe ausweiten. Notfälle treten nur selten auf.

Notfallmanagement: Prozesse, Verhaltensweisen und koordinierte Tätigkeiten, die eine Organisationseinheit ausführen muss, um drohende oder bereits eingetretene Notfälle zu bewältigen.

Notfallorganisation: Betriebliche Maßnahmen, die nötig sind, um nach Zwischen- oder Notfällen negative Auswirkungen auf Menschen, den Betrieb oder die Umwelt so gering wie möglich zu halten.

Risiko: Kombination aus der Wahrscheinlichkeit und der Häufigkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Risiko ist eine spezielle Form der Unsicherheit beziehungsweise Unwägbarkeit. Die Auswirkungen können positiv oder negativ sein.

Risikoanalyse: Systematisches Vorgehen, um ein Risiko zu verstehen. Dabei werden die Wahrscheinlichkeit und Auswirkung des Risikos auf eine Organisation eingeschätzt.

Risikobeurteilung: Gesamtheit des Verfahrens, das Risikoidentifikation, Risikoanalyse und Risikobewertung umfasst.

Risikobewertung: Prozess, der anhand der Ergebnisse der Risikoanalyse bestimmt, ob die Risikohöhe akzeptierbar beziehungsweise tolerierbar ist.

Risikoidentifikation: Prozess, um Risiken zu finden, und mit ihren Ursachen und Auswirkungen zu beschreiben.

Risikomanagement: Prozesse, Verhaltensweisen und koordinierte Tätigkeiten, die darauf ausgerichtet sind, eine Organisation bezüglich Risiken zu steuern. Das bedeutet eine systematische Anwendung von Grundsätzen, Verfahren und Tätigkeiten, um Risiken zu identifizieren, zu analysieren, zu bewerten, zu bewältigen, zu überwachen sowie die Risiko-Themen zu kommunizieren. Notfall-, Krisen und Kontinuitätsmanagement sollten in das Risikomanagement integriert sein.

Sicherheit und Gesundheit bei der Arbeit: Bewahrung von Leben und Gesundheit in Verbindung mit der Berufsarbeit. Der Begriff beschreibt eine menschengerechte Gestaltung und eine ständige Verbesserung der Arbeit, damit diese insgesamt den körperlichen und geistigen Leistungsvoraussetzungen der Beschäftigten entspricht. Der Begriff umfasst die Abwehr von Unfallgefahren und arbeitsbedingten Gesundheitsgefahren. Die Bezeichnung wird synonym zum Begriff „Arbeitsschutz“ verwendet.

Szenario: Bildhafte Darstellung/Beschreibung eines Risikos mit Annahmen über Abläufe und Auswirkungen von Ereignissen. Es zeigt auf, wie sich eine Bedrohung in einem Unternehmen auswirken kann.

Zwischenfall (Störung): Ereignis mit einem geringen Schadensausmaß. Zwischenfälle können in der Regel im allgemeinen Tagesgeschäft behoben werden. Sie können sich zu einem Notfall ausweiten. Zwischenfälle kommen relativ häufig vor.

Weitere Informationen

8 Quellen für die Wissensboxen „Gewusst?“

1. Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt, Bitkom (2020), zugegriffen am 08.11.2021 www.bitkom.org

2. Die Entwicklung von Starkniederschlägen in Deutschland – Plädoyer für eine differenzierte Betrachtung, Deutscher Wetterdienst (2016), zugegriffen am 02.11.2021 www.dwd.de

3. Informationen zur Laienreanimation in Deutschland, Bundeszentrale für gesundheitliche Aufklärung (2021), zugegriffen am 08.11.2021 www.bundesgesundheitsministerium.de

4. Die Bilanz der Naturkatastrophen 2020, Münchener Rückversicherung (2021), zugegriffen am 28.10.2021 www.munichre.com/de

5. Spionage, Sabotage und Datendiebstahl (siehe Quelle 1)

6. So groß ist die Gefahr durch die Schneelast, Spiegel Online (2019), zugegriffen am 02.11.2021 www.spiegel.de

7. Gefährdungsdossier „Meteoriteneinschlag“ des Schweizer Bundesamts für Bevölkerungsschutz (2020), zugegriffen am 01.11.2021 www.babs.admin.ch

8. Deutsches Komitee Katastrophenvorsorge e. V. (2020), DKKV-Newsletter April 2020

9. Spionage, Sabotage und Datendiebstahl (siehe Quelle 1)

10. Juli-Flut: Rekordzahl an Großschäden, Gesamtverband der Deutschen Versicherungswirtschaft e.V (2021), zugegriffen am 02.11.2021 www.gdv.de

11. Golfstrom: So schwach wie seit 1.000 Jahren nicht, Scinexx.de (2021), zugegriffen am 02.11.2021 www.scinexx.de

12. Mit Sicherheit für Köln – Ein Meilenstein für den Hochwasserschutz, Stadtentwässerungsbetriebe Köln, (2008), zugegriffen am 02.11.2021 www.steb-koeln.de

13. Spionage, Sabotage und Datendiebstahl (siehe Quelle 1)

14. Spionage, Sabotage und Datendiebstahl (siehe Quelle 1)

15. Blackout – Wie sicher ist die deutsche Stromversorgung?, Deutschlandfunk (2018), zugegriffen am 01.11.2021 www.deutschlandfunk.de

16. Sicherheitsbericht 2020, Eisenbahn-Bundesamt, Stand 15.09.2021, zugegriffen am 08.11.2021 www.eba.bund.de

17. Schwere psychische Beeinträchtigungen als Arbeitsunfall, VBG, zugegriffen am 01.11.2021 www.vbg.de

Herausgeber:

VBG
Ihre gesetzliche
Unfallversicherung

www.vbg.de

Massaquoipassage 1
22305 Hamburg
Postanschrift: 22281 Hamburg

Artikelnummer: 30-05-6426-1

Konzeption:
VBG in Zusammenarbeit mit der Stiftung
„Mittelstand – Gesellschaft – Verantwortung“
www.stiftung-m-g-v.de

Text:
Oleg Cernavin (Stiftung M-G-V),
Matthias Bludau (VBG),
Christof Radusch (VBG),
Hauke Burmann (VBG)

Redaktion: Hauke Burmann

Gestaltung:
Jedermann-Verlag GmbH
www.jedermann.de

Version 1.0
Stand Januar 2022

Der Bezug dieser Informationsschrift
ist für Mitgliedsunternehmen der VBG
im Mitgliedsbeitrag enthalten.

Fotos:
Titel und S. 3 Hummingbird Art – stock.adobe.com
S. 8 Menyhert – stock.adobe.com, Andreas Prott – stock.adobe.com, Gina Sanders – stock.adobe.com
S. 9 dieter76 – stock.adobe.com
S. 11 m.mphoto – stock.adobe.com
S. 12 Halfpoint – stock.adobe.com
S. 15 iStock.com/A stockphoto
S. 16 .shock – stock.adobe.com
S. 20 Sanja – stock.adobe.com
S. 22 Kadmy – stock.adobe.com
S. 24 photo 5000 – stock.adobe.com
S. 26 oporkka – stock.adobe.com
S. 28 daniilvolkov – stock.adobe.com
S. 31 Mihail – stock.adobe.com
S. 34 iStock.com/Willowpix
S. 36 Martin Bílek – stock.adobe.com
S. 38 Pixel-Shot – stock.adobe.com, Brian – stock.adobe.com, Kostiantyn – stock.adobe.com
S. 39 Daco – stock.adobe.com,
alhim – stock.adobe.com
S. 40 iStock.com/baranozdemir
S. 43 Andrey Popov – stock.adobe.com
S. 44 VBG
S. 46 iStock.com/Perboge
S. 48 Nightman1965 – stock.adobe.com
S. 50 Gorodenkoff – stock.adobe.com
S. 53 Andreas Prott – stock.adobe.com
S. 54 Chalabala – stock.adobe.com
S. 56 Chalabala – stock.adobe.com
S. 58 insta_photos – stock.adobe.com
S. 69 iStock.com/DK Media
S. 60 AA+W – stock.adobe.com
S. 62 Song_about_summer – stock.adobe.com
S. 64 kerkezz – stock.adobe.com
S. 66 Yakobchuk Olena – stock.adobe.com

Wir sind für Sie da!

www.vbg.de

Kundendialog der VBG: 040 5146-2940
Notfall-Hotline für Beschäftigte im Auslandseinsatz:
+49 40 5146-7171
Sichere Nachrichtenverbindung:
www.vbg.de/kontakt

Für Sie vor Ort – die VBG-Bezirksverwaltungen:

Bergisch Gladbach
Kölner Straße 20
51429 Bergisch Gladbach
Tel.: 02204 407-0 · Fax: 02204 1639
E-Mail: BV.BergischGladbach@vbg.de
Seminarbuchung unter
Tel.: 02204 407-165

Berlin
Markgrafenstraße 18 · 10969 Berlin
Tel.: 030 77003-0 · Fax: 030 7741319
E-Mail: BV.Berlin@vbg.de
Seminarbuchung unter
Tel.: 030 77003-128

Bielefeld
Nikolaus-Dürkopp-Straße 8
33602 Bielefeld
Tel.: 0521 5801-0 · Fax: 0521 61284
E-Mail: BV.Bielefeld@vbg.de
Seminarbuchung unter
Tel.: 0521 5801-165

Dresden
Wiener Platz 6 · 01069 Dresden
Tel.: 0351 8145-0 · Fax: 0351 8145-109
E-Mail: BV.Dresden@vbg.de
Seminarbuchung unter
Tel.: 0351 8145-167

Duisburg
Wintgensstraße 27 · 47058 Duisburg
Tel.: 0203 3487-0 · Fax: 0203 2809005
E-Mail: BV.Duisburg@vbg.de
Seminarbuchung unter
Tel.: 0203 3487-106

Erfurt
Koenbergkstraße 1 · 99084 Erfurt
Tel.: 0361 2236-0 · Fax: 0361 2253466
E-Mail: BV.Erfurt@vbg.de
Seminarbuchung unter
Tel.: 0361 2236-439

Hamburg
Sachsenstraße 18 · 20097 Hamburg
Tel.: 040 23656-0 · Fax: 040 2369439
E-Mail: BV.Hamburg@vbg.de
Seminarbuchung unter
Tel.: 040 23656-165

Ludwigsburg
Martin-Luther-Straße 79
71636 Ludwigsburg
Tel.: 07141 919-0 · Fax: 07141 902319
E-Mail: BV.Ludwigsburg@vbg.de
Seminarbuchung unter
Tel.: 07141 919-354

Mainz
Isaac-Fulda-Allee 3 · 55124 Mainz
Tel.: 06131 389-0 · Fax: 06131 389-410
E-Mail: BV.Mainz@vbg.de
Seminarbuchung unter
Tel.: 06131 389-180

München
Barthstraße 20 · 80339 München
Tel.: 089 50095-0 · Fax: 089 50095-111
E-Mail: BV.Muenchen@vbg.de
Seminarbuchung unter
Tel.: 089 50095-165

Würzburg
Riemenschneiderstraße 2
97072 Würzburg
Tel.: 0931 7943-0 · Fax: 0931 7842-200
E-Mail: BV.Wuerzburg@vbg.de
Seminarbuchung unter
Tel.: 0931 7943-407

VBG-Akademien für Arbeitssicherheit und Gesundheitsschutz:

Akademie Dresden
Königsbrücker Landstraße 2
01109 Dresden
Tel.: 0351 88923-0 · Fax: 0351 88349-34
E-Mail: Akademie.Dresden@vbg.de
Hotel-Tel.: 030 13001-29500

Akademie Gevelinghausen
Schlossstraße 1 · 59939 Olsberg
Tel.: 02904 9716-0 · Fax: 02904 9716-30
E-Mail: Akademie.Olsberg@vbg.de
Hotel-Tel.: 02904 803-0

Akademie Lautrach
Schlossstraße 1 · 87763 Lautrach
Tel.: 08394 92613 · Fax: 08394 1689
E-Mail: Akademie.Lautrach@vbg.de
Hotel-Tel.: 08394 910-0

Akademie Ludwigsburg
Martin-Luther-Straße 79
71636 Ludwigsburg
Tel.: 07141 919-181 · Fax: 07141 919-182
E-Mail: Akademie.Ludwigsburg@vbg.de

Akademie Mainz
Isaac-Fulda-Allee 3 · 55124 Mainz
Tel.: 06131 389-380 · Fax: 06131 389-389
E-Mail: Akademie.Mainz@vbg.de

Akademie Storkau
Im Park 1 · 39590 Tangermünde
Tel.: 039321 531-0 · Fax: 039321 531-23
E-Mail: Akademie.Storkau@vbg.de
Hotel-Tel.: 039321 521-0

Akademie Untermerzbach
ca. 32 km nördlich von Bamberg
Schlossweg 2 · 96190 Untermerzbach
Tel.: 09533 7194-0 · Fax: 09533 7194-499
E-Mail: Akademie.Untermerzbach@vbg.de
Hotel-Tel.: 09533 7194-100

Seminarbuchungen:
online: www.vbg.de/seminare
telefonisch in Ihrer VBG-Bezirksverwaltung

Bei Beitragsfragen:
Telefon: 040 5146-2940
www.vbg.de/kontakt

VBG – Ihre gesetzliche Unfallversicherung
Massaquoipassage 1 · 22305 Hamburg
Tel.: 040 5146-0 · Fax: 040 5146-2146