Stiftung
Familienunternehmen

Business Continuity Management

Resilienz durch nachhaltiges Krisen- und Notfallmanagement

Vorwort

Familienunternehmen bleiben auch in Krisenzeiten tragende Säulen der deutschen Wirtschaft. Angesichts zunehmender Herausforderungen durch multiple Krisen sollte jedem endgültig bewusst sein, dass nachhaltiger Unternehmenserfolg eine vorausschauende Planung und die Berücksichtigung potenzieller Krisenszenarien erfordert.

Die Zahl potenziell schädlicher Ereignisse für unternehmerische Tätigkeiten, die sich nicht unmittelbar vorhersehen lassen, hat sich zuletzt noch einmal vergrößert: Neben Unwetterlagen, Pandemien und Cyberattacken müssen nun auch Anschläge extremistischer Organisationen oder Gefährdungen durch politisch motivierten Aktivismus sowie spezifische Anforderungen im Bereich der zivil-militärischen Zusammenarbeit verstärkt in den Blick genommen werden.

Diesem breiten Spektrum unternehmerischer Risiken widmet sich das vorliegende Kompendium in seiner 2. Auflage. Darin werden Maßnahmen zu Prävention und Krisenreaktion skizziert; etwa, wie sich Unternehmen auf Engpässe in der Energie- oder Wasserversorgung, Cyberattacken oder auf einen militärischen Krisenfall vorbereiten können.

Anhand eines strukturierten Business Continuity Managements können Sie sich für eine Vielzahl möglicher Szenarien wappnen. Ziel bleibt es, Schaden vom Unternehmen abzuwenden oder zumindest zu minimieren. In diesem Sinne dient das Kompendium als Baustein des nachhaltigen Unternehmenserfolgs, für den Familienunternehmen in Deutschland und Europa seit Generationen stehen.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre!

Ihre Stiftung Familienunternehmen

München, 2026

Inhalt

Hinweis: Zur besseren Lesbarkeit und Unterstützung des Leseflusses wurde innerhalb des Kompendiums auf die Verwendung des generischen Maskulinums zurückgegriffen. Selbstverständlich schließen alle Formulierungen und Personenbezeichnungen alle Geschlechter gleichermaßen ein.

Einleitung

Wie sind Unternehmen und ihre strategisch und administrativ-organisatorisch agierenden Krisen- und Verwaltungsstäbe, hier bezeichnet als Notfallstäbe, sowohl auf komplexe Bedrohungsszenarien von außen als auch auf neue Gesetzesvorgaben zur Gewährleistung der Sicherheit Deutschlands und seiner Unternehmen ausgerichtet? Wie kann ein effektives Krisenmanagement den Bedrohungen und neuen gesetzlichen Vorgaben zeitnah begegnen? Welche Maßnahmen müssen umgehend angegangen werden, um im Krisenfall „vor die Lage" zu kommen und wieder handlungsaktiv Entscheidungen treffen zu können? Diese und weitere umfassende Fragestellungen zu Resilienz und Nachhaltigkeit unternehmerischen Handelns in Krisen- und Notlagen, die Einführung und Umsetzung einer Strategie für „Business Continuity Management" (BCM), die Optimierung der Krisenprävention, die Erstellung betrieblicher Notfallpläne und nicht zuletzt die Konzeption und eine optimierte Ausbildungsstrategie von Notfallstäben sind Gegenstand des vorliegenden Kompendiums. Es liefert erste Lösungsansätze in Form von Handlungsempfehlungen zur Optimierung der Sicherheitsstrukturen von Unternehmen. Diesbezüglich werden auch die Rolle der Mitarbeiter innerhalb des BCM und der Krisenreaktion sowie die rechtlichen und regulatorischen Anforderungen an BCM behandelt. Damit verbunden werden die so wichtigen Fragestellungen „Resilienz und ihre Bedeutung für Unternehmen" diskutiert. Anhand eines Praxisbeispiels werden praktikable Ratschläge zur Umsetzung des BCM vorgestellt. Es gilt der Grundsatz, dass die Resilienz, die Durchhaltefähigkeit und die Nachhaltigkeit in Sachen Sicherheitsvorsorge eines Unternehmens stetig zu optimieren und zu steigern sind. Die Krisenresilienz von morgen steht und fällt damit, wie umfangreich und gezielt wir heute in präventive Maßnahmen investieren. Krisenprävention ist in erheblichem Maße kosteneffizienter als eine zu kurz greifende lückenhafte Krisenreaktion. Daher gilt es, die Krisenprävention jetzt anzugehen, um so die eigene Krisenreaktion an alle denkbaren Schadenslagen besser anpassen zu können.

Grundlagen des Krisenmanagements

1. Optimiertes Krisenmanagement

Unternehmen, Kommunen und Bürger sehen sich mit neuen Krisen und Gefahrenlagen konfrontiert. Die Komplexität von Schadensereignissen nimmt in den letzten Jahren drastisch zu. Die Ereignisse schaukeln sich gegenseitig auf. Somit entstehen multiple, kaskadierende Katastrophenlagen mit einer oftmals unbekannten Eigendynamik. Schnell können diese Schadensfälle die Dimension einer „Großschadenslage", einer „Katastrophe" oder gar „Krise" annehmen und sich über mehrere Tage erstrecken.

Im Fokus unserer Betrachtung stehen weniger betriebliche Unfälle, Störungen in Folge von Produktionsprozessen oder fehlerhafte Abläufe im Unternehmen selbst, sondern vielmehr Schadenslagen, die von außen auf Unternehmen einwirken.

Weil in den letzten Jahrzehnten eine Steigerungsrate von Naturereignissen als Grundlage für eine Katastrophe von über 30 Prozent pro Dekade ermittelt werden konnte, sind an erster Stelle Unwetterlagen und vor allem die Auswirkungen von Extremwetterlagen, wie z. B. Sturz- und Starkregen und auch ein Dauer-Starkregen-Ereignis (Flut-Katastrophe an der Ahr und Volme im Juli 2021), zu nennen. Sie führen häufig zu weiteren begleitenden Schadenslagen, wie plötzlich auftretenden Stromausfällen in Folge von Unwetterschäden. Daneben können im Zuge von baulichen Maßnahmen technisches und menschliches Versagen als Fehlerquelle genannt werden, wenn z. B. ein Bagger bei Arbeiten nicht nur die Hauptkabelleitung zerstört, sondern auch die Ersatzleitung beschädigt.

Hinzu kommen die Auswirkungen langanhaltender Epidemien und Pandemien, die die Bevölkerung und damit zugleich die Belegschaften in Unternehmen nachhaltig beeinträchtigen und prägen.

Eine völlig neue Dimension der Gefahrenlage für Unternehmen kann sich aus der gestiegenen Sicherheitsbedrohung Deutschlands als Unterstützerland für die völkerrechtswidrig von Russland angegriffene Ukraine ergeben, indem wichtige Importgüter, wie z. B. Gas, in Folge eines Lieferstopps oder Zerstörungen an Pipelines ausfallen. Zugleich wird die wichtige Rolle Deutschlands als Drehscheibe für

NATO-Truppentransporte zu Bündnispartnern sowie die Relevanz von Rüstungsunternehmen und deren Zulieferfirmen im neuen Operationsplan Deutschland (OPLAN DEU) hervorgehoben.

Seit Ende des Kalten Krieges in völlige Vergessenheit geraten sind Aktionen einer asymmetrischen Kriegsführung mit verdeckt operierenden Kräften im Sinne einer hybriden Angriffsbedrohung. Diese können gezielt wichtige Infrastruktureinrichtungen wie Kritische Infrastrukturen (KRITIS) mit Versorgungsleitungen, Transport- und Kommunikationswegen in Deutschland angreifen, beschädigen und letztendlich zu Betriebsausfällen führen.

> „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."
>
> Definition gemäß des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), siehe https://www.bbk.bund.de

Die Bedeutung „Kritischer Infrastrukturen" wird seit 2023 (https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/nationale-sicherheitsstrategie-2197780) durch die Veröffentlichung der Bundesregierung („Nationale Sicherheitsstrategie") unterstrichen.

Wesentlich ist die Umsetzung Europäischer Vorgaben zur Stärkung der Sicherheitsvorkehrungen. Die NIS-2-Richtlinie (EU) 2022/2555 zur Erhöhung der Cybersicherheit in kritischen und wichtigen Einrichtungen wurde in Deutschland mit dem „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" umgesetzt und gilt seit dem 6. Dezember 2025. Die „CER-Richtlinie (EU 2022/2557)" zum Schutz vor physischen Angriffen auf Unternehmen steht Anfang 2026 mit dem „Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen" (und dort ganz überwiegend über das KRITIS-Dachgesetz) zur Umsetzung an.

Übersicht KRITIS-Sektoren

[1] gemäß BSIG, [2] gemäß Bund-Länder-AG
Quelle: Eigene Darstellung.

Interessant dürfte die Veröffentlichung der „DIN SPEC 14027 Corporate Security – Anforderungen zur Stärkung physischer Resilienz von Organisationen" werden, die den Anspruch für einen fachlichen Standard von Unternehmen einnimmt und dabei erste Vorgaben zur Erstellung des DIN-Standards für eine Corporate Security liefert.

In dem Gesamtdokument mit detaillierten Anforderungen an ein komplexes Bedrohungs- und Schutzmanagement samt eines Anforderungskatalogs werden aktuelle Gefahrenlagen und Schutzmöglichkeiten für Unternehmen sehr detailliert behandelt und können auch als eine Mustergliederung für die Umsetzung des Krisen-/BCM-Managements dienen.

Damit werden sich für die Sicherheit von Unternehmen mit erweiterten Branchen und von Zulieferfirmen neue Mindestgrößen für die Notwendigkeit zur Prävention und an das Krisenmanagement ergeben.

Daher lautet der Tenor des Kompendiums, dass Unternehmen eine umfassende Strategie für BCM, Krisenprävention, Notfallpläne und Notfallstäbe benötigen, die die altbekannten und neu definierten Gefahrenlagen abdecken. Der Grundsatz gilt, dass ein effektives BCM-Programm zugleich einen integralen Bestandteil jeder erfolgreichen Organisation darstellt. Damit wird zudem sichergestellt, dass die Geschäftsprozesse auch bei unvorhergesehenen Ereignissen weiterlaufen und die Kontinuität des Unternehmens gewährleistet wird.

Um die Bedeutung des BCM zu verstehen, bedarf es vorab einiger Grundlageninformationen zu den Gefahrenlagen, die in einem Unternehmen auftreten können. Hierzu werden einige Begrifflichkeiten definiert, zu denen die unterschiedlichen Qualitätsstufen eines unvorhergesehenen Ereignisses gehören. Sowohl in ISO-Normen als auch in nationalen Standards wurden Begriffe definiert, die es dem Nutzer ermöglichen, eine einheitliche Einstufung vorzunehmen. Angewandt wird hier die ISO 22300:2021(E) zur Begriffsbestimmung mit den Eskalationsstufen „Ereignis", „Störung", „Notfall" und „Krise".

Das „Ereignis" beschreibt das Eintreten oder die Änderung eines bestimmten Sachverhalts. Als „Störung" wird ein größeres Ereignis bezeichnet, das zu einem Verlust, einem Notfall oder einer Krise führen kann oder könnte. Unter dem Begriff „Notfall" wird ein plötzliches, dringendes, meist unerwartetes Ereignis verstanden, das sofortiges Handeln erfordert. Die letzte Stufe, die „Krise", steht für einen instabilen Zustand, der eine bevorstehende abrupte oder erhebliche Veränderung beinhaltet, die dringende Aufmerksamkeit und Maßnahmen zum Schutz von Leben, Vermögenswerten, Eigentum oder der Umwelt erfordert. Beim Eintritt einer Krise befindet sich ein Unternehmen in einer Phase, in der die Funktionsfähigkeit beeinträchtigt ist, die Gefahr eines Zusammenbruchs des Unternehmens droht und/oder das Umfeld einer akuten Gefährdung ausgesetzt ist bzw. diese bereits eingetreten ist. Dabei kann eine Krise oder auch der Notfall durch viele verschiedene Ursachen hervorgerufen werden. Eines haben die potenziellen Ursachen jedoch gemein: Eskalieren sie zu einer Krise, so lassen sich diese nicht mehr allein durch die Alltagsorganisation beherrschen und abarbeiten.

Das Krisenmanagement umfasst verschiedene Aspekte: Es beinhaltet die Identifizierung potenzieller Bedrohungen, die Bewertung ihrer Auswirkungen und Wahrscheinlichkeiten, die Entwicklung von Notfallplänen, die Schulung von Mitarbeitern und die Einrichtung von Kommunikationssystemen, um effektiv auf Krisensituationen reagieren zu können. Das Ziel des Krisenmanagements besteht darin, die Sicherheit von Menschenleben, Vermögenswerten und der Umwelt zu gewährleisten und gleichzeitig den Geschäftsbetrieb so reibungslos wie möglich aufrechtzuerhalten.

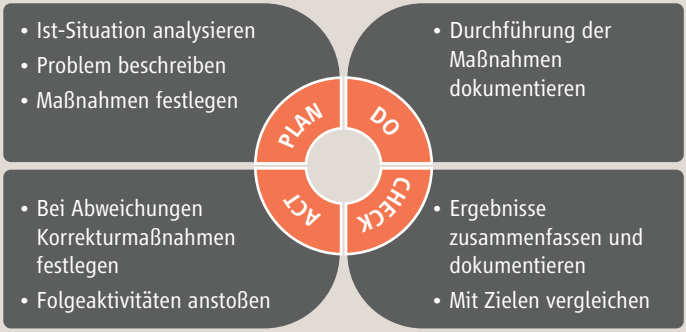
Ein erfolgreiches Krisenmanagement erfordert eine enge Zusammenarbeit zwischen verschiedenen Akteuren. Es erfordert klare Rollen und Verantwortlichkeiten, klare Kommunikationswege und einen koordinierten Ansatz, um die Reaktion auf eine Krise effektiv zu steuern. Zudem ist es wichtig, aus vergangenen Krisen zu lernen und kontinuierlich die eigenen Fähigkeiten und Maßnahmen zu verbessern, um zukünftige Krisen besser bewältigen zu können.

Das Krisenmanagement schafft die konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen, um die schnellstmögliche Rückführung einer eingetretenen außergewöhnlichen Situation in den Normalzustand zu unterstützen bzw. die negativen Konsequenzen so gering wie möglich zu halten. Die in einer Krise umgesetzten Maßnahmen des Krisenmanagements, die auf die Lagebewältigung abzielen, sind häufig operativ ausgerichtet und dienen der Krisenbewältigung. Es hängt sicherlich mit der Größe eines Unternehmens bzw. der Geschäftsbereiche und zu guter Letzt mit dem „Risikoappetit" des Inhabers oder seiner beauftragten Vertreter zusammen, in welcher Ausprägung und Ernsthaftigkeit ein Krisenmanagement in den Unternehmen vorhanden ist. Gänzlich außer Acht gelassen wird es sicherlich nicht, da jedes Unternehmen gezwungen ist zu handeln, um das schädigende Ereignis abzuwenden und dadurch den Fortbestand des Unternehmens zu sichern.

Zur Vorbereitung und Optimierung des Krisenmanagements empfiehlt sich die Anwendung des aus dem Qualitätsmanagement bekannten „Plan-Do-Check-Act" (PDCA)-Verfahrens. Es besteht aus vier aufeinanderfolgenden Schritten, die in einer Schleife wiederholt werden, um kontinuierliche Verbesserungen zu erzielen.

Der PDCA-Zyklus ist darauf ausgerichtet, kontinuierliche Verbesserungen in einem Prozess oder einer Organisation zu erzielen, so auch in ihrem Krisenmanagement.

Muster eines „PDCA"-Zyklus



Quelle: Eigene Darstellung.

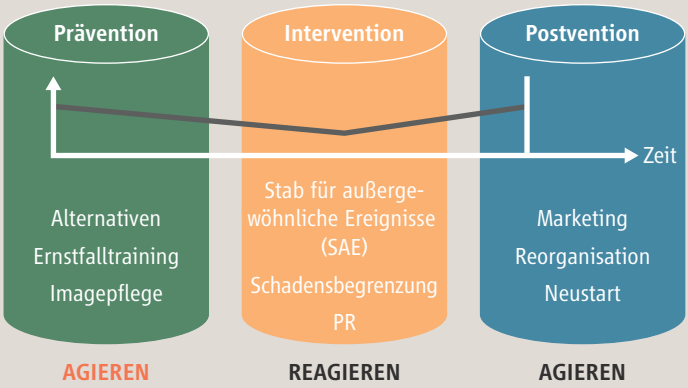
2. Präventionsplanung zentral für das Resilienzmanagement

Große Schäden entstehen nie durch einen einzigen Fehler, sondern immer durch das Zusammenwirken mindestens zweier Ereignisse, wobei jedes für sich harmlos sein kann, diese unter Umständen schon immer vorhanden waren, ihre Verknüpfung nicht vorhersehbar erschien, sie eigentlich nichts miteinander zu tun haben. Meist wird die Lage durch den menschlichen Faktor verschärft, sei es bei Prävention, Intervention oder Postvention.

Da sich solche Szenarien selbst bei bester Planung von Vorsorgemaßnahmen nicht gänzlich ausschließen lassen, muss im Rahmen eines sorgfältigen Krisenmanagements eine möglichst optimale Vorbeugung im Sinne einer Krisenprävention gefordert werden. Zugleich muss man sich dabei mit strategischem Handeln neben der Vorsorge bzgl. einer Schadenslage auch mit der Bewältigung einer solchen eingetreten Lage beschäftigen. Letztendlich geht es um sinnhaftes, um ein „gutes" Krisenmanagement, das möglichst optimal alle denkbaren Schadensereignisse und deren Eintrittswahrscheinlichkeit auflistet, beschreibt und bewertet, um daraus Folgerungen für die anstehende Prävention, die Intervention und auch für die Postvention zu gewinnen. „Schlechtes" Krisenmanagement gilt es dabei zu vermeiden, bedeutet es doch, dass keine oder eine nur unzureichend vorausschauende Vorbereitung für den Krisenfall

stattfindet, bevor dieser systemrelevant eintritt. Ein „schlechtes" Krisenmanagement selbst ist i. d. R. zu langsam, zu stark vom „Topmanagement" der Unternehmensleitung geprägt; Rückschlüsse sind zu sehr taktisch und operativ ausgerichtet und die „Gesamtfolgen" werden nicht umfassend erkannt; der strategische Lösungsansatz in der Planung wird zu wenig berücksichtigt.

Krisenmanagement von der Prävention bis hin zur Postvention



Quelle: Eigene Darstellung.

Im Schwerpunkt eines anzustrebenden „guten" Krisenmanagements steht immer das innovative Forschen nach neuen Präventionsstrategien, die das bestehende Krisenmanagement und vorhandene Präventionsstrategien jederzeit neu optimieren. Es gilt der eherne Grundsatz, die bestehenden Konzepte zukunftsorientiert und wertneutral zu analysieren und den aktuellen Gefahrenlagen anzupassen, um so die Krisenreaktion deutlich zu verbessern.

Gefahrenlagen wie die Corona-Pandemie haben in Unternehmen nachhaltig zu einem Überdenken vorhandener Krisen- und Notfallpläne und des reaktiven Krisenmanagements geführt. Zentral stellt sich die Frage für verantwortungsvolle Krisen- und Notfallmanager, ob man in der Vergangenheit ausreichend für die „neuen" Gefahren aufgestellt war, ob das Handeln in der Krise strategisch weitsichtig ausgerichtet war und nicht nur taktisch-operativ das Ereignis an sich für die nächsten Tage und Wochen gesehen wurde. Überaus wichtig wird, wie das vorhandene Krisenmanagement und

die Business-Continuity-Pläne (BCP) so ausgeplant werden können, dass sie den neuen Voraussetzungen und Anforderungen jederzeit gerecht werden. Aus Krisen- und Schadenslagen gilt es, zusammen mit dem bestehenden Krisen- oder Notfallmanagement die richtigen Schlüsse für die zukünftige Krisenbewältigung zu ziehen.

Modernes Krisenmanagement

Quelle: Eigene Darstellung.

Das Krisenmanagement kann wesentlich dazu beitragen, das Ansehen eines Unternehmens nachhaltig zu schützen und das Vertrauen von Kunden, Investoren und der Öffentlichkeit aufrechtzuerhalten.

Letztendlich zeigt sich in der inneren Stärke eines Unternehmens dessen Qualität bezüglich seiner Handlungsfähigkeit in Krisensituationen.

So sollte im „Worst-Case-Fall" bei einer langanhaltenden und flächendeckenden KRITIS-Lage über mehrere Tage (z. B. Stromausfall für große Teile einer Region) ein Unternehmen in der Lage sein, die vom Gesetzgeber geforderten Anforderungen zu erfüllen und darüber hinaus Kunden und Nutzer unterstützen.

Die Präventionsplanung ist daher immer der erste und zugleich wichtigste Bestandteil des Resilienzmanagements. Sie trägt dazu bei, potenzielle Risiken und Bedrohungen zu identifizieren und zu minimieren, bevor diese zu Krisen oder Katastrophen führen können.

Der Begriff „Resilienz“ nimmt einen immer größeren Stellenwert im Sprachgebrauch der Unternehmen ein. Im Folgenden soll die Bedeutung des Resilienzmanagements mit Fokus auf den Ablauf näher beschrieben werden:

- Anpassungsfähigkeit:
  Resiliente Unternehmen sind flexibel und können sich schnell an neue Gegebenheiten anpassen. Sie erkennen Veränderungen frühzeitig, reagieren darauf und passen ihre Strategien und Geschäftsmodelle an, um wettbewerbsfähig zu bleiben.
- Krisenbewältigung:
  Resiliente Unternehmen haben Krisenmanagementpläne und -strukturen etabliert, um schnell und effektiv auf solche Situationen zu reagieren. Sie können operative Unterbrechungen minimieren, die Auswirkungen auf ihre Kunden, Lieferanten und Mitarbeiter reduzieren und sich schneller erholen.
- Innovationskraft:
  Resiliente Unternehmen fördern eine Kultur der Innovation und des unternehmerischen Denkens. Sie ermutigen ihre Mitarbeiter, neue Ideen einzubringen, zu experimentieren und aus Fehlern zu lernen. Dies ermöglicht es ihnen, sich kontinuierlich weiterzuentwickeln, neue Produkte und Dienstleistungen zu entwickeln und sich den veränderten Kundenbedürfnissen zeitnah anzupassen.
- Mitarbeiterbindung und -entwicklung:
  Resiliente Unternehmen erkennen die Bedeutung ihrer Mitarbeiter für ihren Erfolg an. Sie investieren in die Entwicklung ihrer Fähigkeiten und ihres Wohlbefindens, bieten ihnen klare Kommunikation und Unterstützung während schwieriger Zeiten. Dies führt zu engagierten und motivierten Mitarbeitern, die bereit sind, sich den Herausforderungen jederzeit zu stellen und somit zum Erfolg des Unternehmens beizutragen.
- Risikomanagement:
  Resiliente Unternehmen verfügen über ein umfassendes Risikomanagement in ihren Geschäftsprozessen und haben dies vollständig integriert. Sie identifizieren potenzielle Risiken, bewerten sie und ergreifen proaktive Maßnahmen, um sie zu minimieren oder zu bewältigen. Dadurch sind sie besser gerüstet, um mögliche Störungen zu verhindern oder abzumildern.

Um ein Unternehmen entsprechend der aufgeführten Aspekte resilient aufzustellen, müssen Eigentümer und verantwortliche Geschäftsführer vorausschauend handeln. Bereits in „guten Zeiten" sollte der eigene Erfolg kritisch hinterfragt werden. Dies erfordert nicht nur Mut, sondern auch die Bereitschaft, „Schmerzen" im Verantwortungs- und Entscheidungsprozess auf sich zu nehmen, und zwar, bevor ein ernsthafter Leidensdruck entsteht. Damit wird deutlich, wie komplex und vielschichtig eine gute Präventionsplanung als ein wichtiger Bestandteil des Resilienzmanagements in der Umsetzung wird.

I. Gefahren für unternehmensrelevante Infrastrukturen

Nachfolgend werden Gefahrenlagen im Detail beschrieben, die von außen auf Unternehmen, ihre Belegschaften und deren privates Umfeld wirken und die zugleich Auswirkungen auf Zulieferfirmen und Abnehmer bzw. Kunden haben. Die aufgeführten Schadenslagen können durch Ad-hoc-Ereignisse in Form von Punkt- und Flächenlagen auf die jeweilige Liegenschaft einwirken, sie können aber auch als Flächenlagen mehrere Betriebsflächen zeitgleich beeinträchtigen und so das Schadens- bzw. Katastrophenausmaß erhöhen.

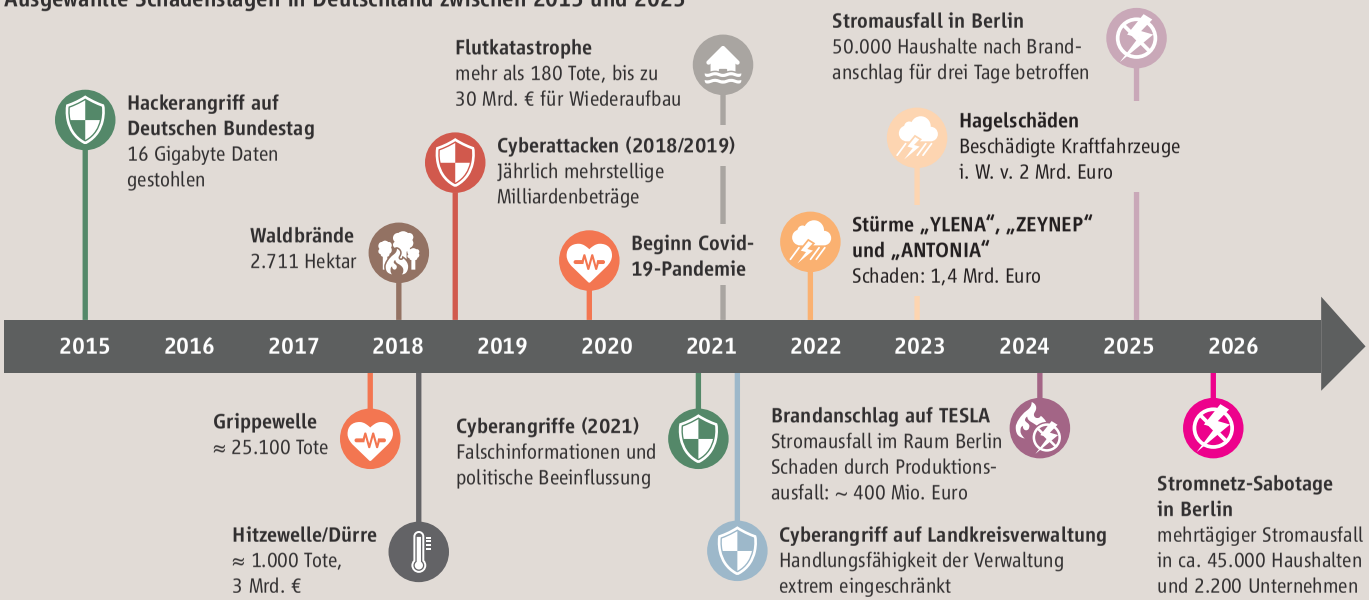
1. Naturkatastrophen und Umweltgefahrenlagen

Im Zuge des Klimawandels nehmen Naturkatastrophen als Gefahrenlagen für Unternehmen den höchsten Stellenwert ein. Gemäß der Rotkreuz- und Rothalbmondgesellschaft (2020) lösen diese immer mehr Katastrophen aus. So sind in den vergangenen Jahren vier von fünf Naturkatastrophen weltweit auf den Klimawandel zurückzuführen. Unter Naturkatastrophen subsumiert werden Unwetter, Überschwemmungen und Hitzewellen. Seit den 1990er Jahren ist die Zahl der klima- und wetterbedingten Katastrophen in jedem Jahrzehnt um fast 35 Prozent gestiegen.

Belastungen aus Wetterextremen (z. B. Starkregen) haben laut dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV, Stand 31. Mai 2025) im Jahr 2024 Schäden in Höhe von 5,7 Milliarden Euro verursacht. Hochwasserereignisse trafen weite Teile Deutschlands, vor allem das Saarland, Rheinland-Pfalz, Bayern und Baden-Württemberg. Insgesamt beliefen sich die Schäden in der Sachversicherung auf 4,5 Milliarden Euro, hierbei 2 Milliarden Euro allein auf Sturm- und Hagelschäden. Rund 2,5 Milliarden Euro gingen auf das Konto sogenannter sonstiger Naturgefahren wie Überschwemmungen und Erdrutsche, die oftmals in Folge von Starkregenereignissen auftreten.

Für Unternehmen, die in Mittelgebirgs- und Hochgebirgsregionen angesiedelt sind, ist dies risikoreich. Bei Starkregen und Dauerstarkregen können solche Unternehmen neben Blitzeinschlägen besonders von Überflutungen betroffen sein. Ereignisse wie Windhosen (Tornados) nehmen seit Jahren zu.

Ausgewählte Schadenslagen in Deutschland zwischen 2015 und 2025



Quelle: Eigene Darstellung.

Bei auftretenden Schadenslagen nehmen die Kosten für die Beseitigung der Schäden bzw. für die Wiederherstellung und Inbetriebnahme der ehemaligen Strukturen sehr schnell hohe Schadenssummen an.

Lösungsansätze für Unternehmen:

Im Rahmen einer Präventionsstrategie sollten Notstromaggregate und Rechenanlagen, Treibstofflager und Materiallager aller Art sowie firmenwichtige Archive mit Unterlagen, erst recht aber die Räumlichkeiten von Krisen-/Notfallstäben nicht in den Tiefgeschossen untergebracht werden. Als wichtige Präventionsaufgabe sollten Überflutungs- und Überschwemmungskarten mit Prognosemodellen für das jeweilige Betriebsareal unter Beachtung der Topografie und von Einleitern und Nebenflüssen erstellt werden. Zudem sollte die Räumung bzw. die Evakuierung historisch gewachsener Bereiche (Gebäudeteile und -flächen) geübt werden.

Dürreperioden und absinkende Grundwasserpegel können mit der Anlage von Rückhaltebecken, Wassertanks oder Tiefbrunnen begegnet werden. Die Bevorratung von ausreichend Trink- und Brauchwasser für wichtige Produktionsanlagen einschließlich der Räumlichkeiten der Verwaltung und im besonderen Maße die des Gebäudes vom Notfallstab sollte für mindestens 14 Tage ausgelegt werden. Zusätzlich kann über eigene Haus- und Notbrunnen auf dem Firmengelände die Wasserversorgung sichergestellt werden. Nicht zu unterschätzen sind schon aus hygienischen Gründen die Konzeption von Abwasserbehältern und ausreichende Toilettenkapazitäten, die ggf. den Zugriff auf Notersatz-Dixi-Toiletten gewährleisten.

2.
Gefahr von Stromausfällen

Deutschland verfügt in Europa über eines der besten und sichersten Stromnetze. Im Jahr 2023 musste jeder Verbraucher in Deutschland eine durchschnittliche Unterbrechung der Stromversorgung von etwa 12,8 Minuten hinnehmen. Dies ist

ein sehr guter Wert an sich, der jedoch zuvor niedriger lag: im Jahr 2020 bei nur 10,73 und 2019 bei 12,2 (sog. SAIDI-Wert in Minuten Stromausfall). Interessant und leider nicht im SAIDI-Wert aufgeführt sind Stromausfälle im Bereich von unter drei Minuten bis hin zu wenigen Millisekunden, die in den letzten Jahren zugenommen haben und Betriebe ohne ausreichende Notstrompufferung und leistungsstarke Notstromaggregate (bis hin zu eigenen Kraftwerksanlagen) nachhaltig treffen können.

Eine neue Gefahrenlage hat sich im Zuge des russischen Angriffskrieges auf die Ukraine und die folgende Gasembargolage durch Russland seit Sommer 2022 ergeben. Durch den Ausfall der Gaslieferungen aus Russland, die mit 55 Prozent den Hauptanteil der Gasimporte Deutschlands ausmachten, stellte sich vermehrt die Frage, woher die Gasmengen für die Stromerzeugung kommen, speziell die zum schnellen Hochfahren benötigen Gaskraftwerke (die zugleich als Überbrückungstechnologie beim Ausstieg der konventionellen Energieträger dienen sollten). Zum Verständnis: Der Anteil der Gaskraftwerke an der Stromerzeugung lag im Jahreswert 2024 (Statistisches Bundesamt, 2025) bei immerhin 14,9 Prozent. In der Betrachtung von Tages- und Stundenverläufen kann der Anteil der Gaskraftwerke an der Verstromung – speziell im Winterhalbjahr in den dunklen Abend-/Nacht- und Morgenstunden und bei Flaute im Offshore-Bereich – leicht 16 bis 20 Prozent ausmachen. Zusammen mit dem im April 2023 ausgeführten Ausstieg aus der AKW-Verstromung besteht die Gefahr, dass bei einem Gasmangel und zugleich stetiger und steigender Nachfrage von Gas als Heiz- und Brennstoff für private Haushalte und Unternehmen im gegebenenfalls kalten und langanhaltenden Winter befristet eine Deckungslücke in der Stromerzeugung in Deutschland auftreten kann, weil die Leistung bzw. die Lieferung von Stromerzeugern der Nachfrage nicht mehr gerecht würden.

Die Bundesnetzagentur (BNetzA) verweist am 3. September 2025 auf Risiken zur Sicherstellung der Stromversorgung in Deutschland bis 2035. Die Stromversorgung in Deutschland ist danach nur gewährleistet, wenn bis 2035 zusätzliche steuerbare Kapazitäten von bis zu 22,4 GW bzw. bis zu 35,5 GW – bei einem Szenario „Verzögerte Energiewende" – errichtet werden. Diesbezüglich ist zu beachten, dass es sich um Bruttowerte handelt, die den Zubau ohne Stilllegungen beziffern.

Von Seiten der vier großen Betreiber der Höchstspannungsnetze – Amprion GmbH, TransnetBW GmbH, TenneT TSO GmbH und 50Hertz Transmission GmbH – würden dann im Zuge des vertraglich vereinbarten Zurückfahrens stromintensiver Unter-

nehmen regionale Lastabwürfe (geplante befristete Stromabschaltung – bis zu 4 bzw. 6 Stunden – kleiner Regionen durch Netzbetreiber zur Stabilisierung der Netzsicherheit) von Minuten bis hin zu wenigen Stunden (sog. „Brownout") bzw. bis hin zum flächendeckenden und langanhaltenden „Blackout" nicht auszuschließen sein.

Speziell im Winter besteht die Gefahr, dass ein Stromverbraucher aufgrund auftretender Engpässe im Stromnetz durch Lastabwürfe ungeplant abgeschaltet wird. Für den betroffenen Verbraucher bedeutet dies einen Stromausfall mit geringer oder ohne Vorwarnzeit. Es besteht die Hoffnung, hierdurch die Energieversorgungssituation einmalig und kurzfristig für lokal begrenzte Bereiche (Versorgungswaben der Energieversorger) zu stabilisieren. In der Folge sollen die Stromnetze entlastet und für ein Wiederhochfahren vorbereitet werden. Dabei kann es zu stundenweisen Trennungen der Kunden von der Versorgung kommen, die aber nicht mit einem Blackout gleichzusetzen sind.

Bei einem Blackout bricht das gesamte Stromnetz vom Höchstspannungsnetz ausgehend in die nachgeordneten Spannungsebenen innerhalb weniger Minuten unkontrolliert zusammen. Dadurch fließt in weiten Teilen des westlichen Europas und damit auch in weiten Teilen Deutschlands kein Strom mehr. Die Eintrittswahrscheinlichkeit eines solchen Szenarios ist nach den Erkenntnissen eines bundesweiten Stresstests jedoch sehr gering. Hervorzuheben ist, dass die vier Übertragungsnetzbetreiber solche Szenarien nicht ganz ausschließen. Der erste europäische Blackout vom 28. April 2025, der ca. 60 Mio. Einwohner in großen Teilen Spaniens, Portugals und von Südfrankreich betraf, dauerte bis zu 24 Stunden.

Sollte sich eine solche Situation abzeichnen und andere Möglichkeiten zur Stabilisierung des Stromnetzes nicht mehr möglich sein, würde zuerst eine kontrollierte Lastabschaltung erfolgen, wobei die Netzbetreiber dann gezielt bestimmte Großverbraucher – Firmen sowie Privatkunden – in einem bestimmten Rhythmus vom Stromnetz nehmen. Dies kann beispielsweise stundenweise geschehen. Dabei werden in einer Versorgungswabe keine Unterschiede zwischen Unternehmen und Verbrauchern gemacht. Im Unterschied zum Blackout ist der sogenannte kontrollierte Lastabwurf regional und zeitlich begrenzt sowie gut von den Netzbetreibern zu steuern.

Im Falle eines Blackouts hätten Unternehmen so gut wie keine Vorwarnzeit. Alle Unternehmen, die über keine ausreichenden Notstromaggregate und Notstrom-

pufferung verfügen, wären nachhaltig betroffen. Ihre Produktion würde erheblich beeinträchtigt, wenn nicht – je nach Branche – sogar gegen Null fahren.

Dieser Schadensfall würde die Unternehmen insbesondere in einem langanhaltenden und sehr kalten Winter, aber auch die Belegschaft sehr stark treffen. Es ist davon auszugehen, dass ein hoher Anteil der Mitarbeiter dann nicht mehr zur Arbeit kommen wird, da private Belange – z. B. pflegebedürftige Angehörige, private Probleme im Lebensumfeld – die Resilienz der Belegschaft und auch der Mitglieder der Krisen- bzw. Notfallstäbe negativ beeinflussen dürften.

Lösungsansätze für Unternehmen:

Unternehmen sollten im Rahmen ihrer Präventionsstrategie Sorge dafür tragen, dass für wichtige Produktionsanlagen und speziell für die Räumlichkeiten des Notfallstabs neben Pufferungen zugleich ausreichende und leistungsstarke Notstromaggregate angeschafft werden. Dies können sowohl mobile als auch festinstallierte Aggregate sein.

Das BBK hat in seinem Dokument „Autarke Notstromversorgung der Bevölkerung“ aus dem Jahre 2015 als Ersatz- und Kompensationsmaßnahmen PV-Systeme, Brennstoffzellen, Kleinwindkraftanlagen, Batterieanlagen, Kurbelgeneratoren und Dieselgeneratoren bis hin zu umfangreichen Blockheizkraftwerken vorgestellt. Unternehmen müssen vor der Wahl dieser Ersatzmaßnahmen prüfen, ob Aspekte wie Leistung, Preis, Handhabung, Umwelteinflüsse und Akzeptanz dabei ausreichend berücksichtigt werden. Vom Grundsatz her lässt sich die Notstromversorgung in zwei Arten differenzieren. Zum einen die „unterbrechungsfreie Stromversorgung“ (USV) und zum anderen sogenannte Netzersatzanlagen. Im ersten Fall wird die Energie über Akkumulatoren bereitgestellt. Diese Anlagen springen relativ zeitnah an, sie sind aber meist nur für eine kurze Überbrückungszeit ausgelegt. Daran schließen sich technische Systeme wie Netzersatzanlagen an. Diese Anlagen werden in der Regel von Dieselmotoren angetrieben. Deren Übernahme erfordert einen gewissen zeitlichen Vorlauf.

Allen Netzersatzanlagen ist gemein, dass diese über einen Treibstoffvorrat

von mindestens 72 Stunden (und mehr) verfügen sollten. Daher sollten ausreichende Treibstofflager errichtet und die vertragliche Verfügbarkeit von Lieferfirmen geprüft und abgestimmt werden. Diese Tanklager bedürfen einer umfangreichen Sicherung sowie eines Logistikkonzeptes, um verderbliche Treibstoffe (z. B. Dieselkraftstoff) durch rechtzeitigen Verbrauch bzw. durch Zugabe von Zusatzstoffen vor einem Umschlagen zu schützen. Firmenfahrzeuge sollten abends möglichst vollgetankt abgestellt werden, um eine ausreichende Eigenbevorratung zu sichern.

Die Unternehmensleitungen sollten im Rahmen der Stärkung der Resilienz der Belegschaft prüfen, ob Mitglieder solcher Stäbe sowie deren Angehörige täglich mit Notversorgungsmitteln auszustatten sind. Dies setzt jedoch ein umfangreiches Logistik-Konzept voraus.

3.
Gefahr einer Gasmangellage

Vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine stellt sich die wichtige Frage, wie die Bundesrepublik Deutschland nachhaltig eine hohe Versorgungssicherheit von Energieträgern wie Erdgas und Erdöl sowie Steinkohle gewährleisten kann, da Russland als direkter Lieferant ausfällt.

Die russischen Gaslieferungen haben in der Vergangenheit bis zu 55 Prozent der Gasimporte Deutschlands ausgemacht. Die Lageeinschätzung der Bundesnetzagentur sah in den prognostizierten Szenarien deutliche Gefahrenlagen für die deutsche Gasversorgung. Gemäß einer Studie des bdew e. V. vom 17. März 2022 lässt sich der Ausfall der Lieferungen aus Russland nur zu einem Drittel durch Einsparungsmaßnahmen kompensieren. Im Bereich der Industrie lagen die Einsparpotenziale lediglich bei maximal 8 Prozent. Speicherstand 1. Januar 2026: 56,2 Prozent (1. Januar 2025: 79,8 Prozent).

Zugleich wird von der Bundesnetzagentur und dem Bundesministerium für Wirtschaft und Energie (BMWE) in stärkerem Maße hinterfragt, wie sicher die Gasversorgung

von Deutschland in einem Winter ist und was passiert, wenn ein langanhaltender und sehr kalter Winter droht und die Gasversorgung für das Heizen und als Kochmöglichkeit nicht mehr ausreichend für alle privaten Haushalte, für Unternehmen und deren KRITIS-relevante Anlagen und Einrichtungen zur Verfügung steht. Diese zentrale Frage beschäftigt seit der Frühwarnstufe des Notfallplans Gas, ausgerufen am 30. März 2022, mit der weiteren am 23. Juni 2022 eingeführten „zweiten Eskalationsstufe" des Notfallplans Gas und deren Rückstufung zur Frühwarnstufe am 1. Juli 2025 weiterhin alle Unternehmen. Die Belegschaft ist nachhaltig betroffen, sobald die ehemals sichere grundlegende Daseinsvorsorge nicht mehr verfügbar ist und sich Schäden an Leib und Leben sowie an Material nicht mehr ausreichend abwenden lassen.

Das Kernproblem für ein angepasstes Krisen-Resilienzmanagement liegt darin, dass es bislang keine Praxiserfahrung und keine Vorstellung der dauerhaften Gefahrenlage Gasmangel gibt. Die Worte „Krieg" und „absoluter Lieferstopp aus Russland" kamen im 37-seitigen deutschen „Notfallplan Gas" aus 2019 kein einziges Mal vor, werden aber im Notfallplan vor allem auf das Szenario ausgelegt, dass der Gasverbrauch in Deutschland für einen kurzen Zeitraum zu hoch wird, um komplett bedient werden zu können. Mit dem „Notfallplan Erdgas" aus 2023 werden die Warnstufen, die Rolle der Bundesnetzagentur und die Form der Zusammenarbeit näher festgelegt. Für die Einstufung des Schweregrades einer Versorgungskrise werden drei Stufen genannt:

Krisenstufen des Notfallplans Gas

Warnstufe	Voraussetzungen für das Ausrufen	Folgen
Frühwarnstufe	Wenn es konkrete, ernstzunehmende und zuverlässige Hinweise gibt, dass der Eintritt eines möglichen Ereignisses die Gasversorgungslage erheblich verschlechtern könnte.	Der Staat greift nicht ein, aber ein Krisenstab aus Behörden und Energieversorgern wird gebildet. Versorger und Betreiber müssen die Gasversorgungslage regelmäßig für die Bundesregierung einschätzen.

Warnstufe	Voraussetzungen für das Ausrufen	Folgen
Alarmstufe	Die Störung der Gasversorgung oder eine außergewöhnlich hohe Nachfrage nach Gas, die zu einer erheblichen Verschlechterung der Gasversorgungslage führt.	Der Staat greift nicht ein, der Markt ist noch in der Lage, die Störung oder Nachfrage allein zu bewältigen. Die Preisanpassungsklausel kann von der Bundesnetzagentur aktiviert werden, um höhere Preise für Betreiber an Verbraucher weiterzugeben.
Nofallstufe	Die Bundesregierung ruft diese Stufe per Verordnung aus, wenn eine außergewöhnlich hohe Nachfrage an Gas, eine erhebliche Störung der Gasversorgung oder eine andere erhebliche Verschlechterung der Versorgungslage vorliegt.	Der Staat greift in den Markt ein, um vor allem die Gasversorgung der geschützten Kunden sicherzustellen. Dazu gehören u. a. private Haushalte, Krankenhäuser, die Feuerwehr, Polizei und Gaskraftwerke. Die Bundesnetzagentur wird zum Bundeslastverteiler und regelt die Verteilung von Gas.

Quelle: Notfallplan Gas für die Bundesrepublik Deutschland.

In diesem Zusammenhang ist es wichtig, den Notfallplan Gas für die Bundesrepublik Deutschland vom September 2019 zu kennen. Er beschreibt u. a. die Sicherheit der Gasversorgungslage und verweist auf die Wichtigkeit der hohen Befüllung der deutschen Gasspeicher. Bezogen auf Versorgungssicherheit mit Gas in extrem kalten Winterlagen reichen die Gasfüllstände für maximal sieben Tage. In einer optimistischeren Lageeinschätzung reicht die Versorgungssicherheit auf Basis des Gasverbrauchs mit einem sehr kalten Winter für 30 Tage.

Parallel dazu wurde die Frage diskutiert, was mit der Gasversorgung passiert, wenn der Strom großflächig und langanhaltend ausfällt. Sollte der Strom ausfallen, dann wären alle Gas-Regelanlagen, alle Heizanlagen sowie die wichtigen Übernahmestationen

bis hin zu den Zählern und den Anschlussbetreibern besonders betroffen. Zu einem gravierenden Problem würde bei einer sogenannten Flächenlage die geringe Zahl fachlich versierter Handwerker, die jeweils zur Inbetriebnahme der Gasanschlüsse die Gebäude aufsuchen und von Hand wieder freischalten müssten. Diese sind aber in der benötigten Größenordnung nicht verfügbar.

Lösungsansätze für Unternehmen:

Seit Herbst 2022 haben neben kreisfreien Städten und Landkreisen auch Unternehmen in verantwortlicher Weise die Aufgabe vom klassischen Bevölkerungsschutz und der Katastrophenhilfe bzw. der Notfallvorsorge für ein Unternehmen angenommen und ihre bisherigen Gefahrenabwehr- bzw. Notfallpläne neu hinterfragt. Die Unternehmen und ihre Notfallstäbe haben begonnen, ihre Liegenschaften aufgrund der Versorgungsmangellage, hier der „24/7"-sicheren Gasversorgung mit besonderem Fokus auf ihre eigenen Produktions- und Verwaltungsbereiche, zu prüfen. Zugleich wird deren Durchhaltefähigkeit über drei Tage und mehr hinterfragt. Dabei wurden Ersatz- bzw. Kompensationsmaßnahmen, z. B. über Flüssiggastanks, für das Beheizen von Verwaltungsgebäuden und deren externe Stromversorgung in enger Abstimmung mit Fachberatern von Stadtwerken sowie externen Gutachtern geprüft. Schnell zeigte sich der Nachholbedarf an festen und mobilen Notstromaggregaten und Anschlussmöglichkeiten sowie der Bedarf eines umfangreichen Logistikkonzepts, welches über den Fuhrpark der klassischen Einsatzfahrzeuge, z. B. von Werksfeuerwehren, hinausgeht.

Krisenmanager und Sicherheitsbeauftragte von Unternehmen sollten sich von der guten und günstigen Witterungslage aus den letzten drei milden Wintern nicht täuschen lassen und die Zeit bis zum nächsten Winter dahingehend nutzen, das zum Teil noch sehr rudimentär vorhandene und veraltete Krisenmanagement zu überdenken und dementsprechend die verbleibende Zeit für eine Optimierung vorhandener Planungen zu nutzen. Noch liegt das strategische Element der Führung und der Ausplanung von Maßnahmen bei den Verantwortlichen.

4.
Ausfall der Versorgung mit Treibstoffen

Deutschland verfügt über ein dichtes und gut ausgebautes Netz an Tankstellen und Depots. Der Treibstoff gelangt in Masse von den Raffinerien über Kanal- und Flussschiffe zu den Verteilstandorten und Depots. Von dort aus wird der Treibstoff per LKW zu Tankstellen transportiert. Ähnlich verhält es sich mit Tankmöglichkeiten von Unternehmen. Viele verfügen über eigene Werks-Tankstellen. Für die Fahrzeugflotte verlässt man sich zudem auf öffentliche Tankstellen. Nur 100 der rund 14.200 Tankstellen in Deutschland verfügen über eine Notstrompufferung, die es ermöglicht, Treibstoff auch bei Stromausfall zu fördern. Somit dürfte bei einem flächendeckenden und langanhalten Stromausfall die vorhandene Menge an Treibstoff (Dieselkraftstoff, Superbenzin, vereinzelt Gemisch für z. B. Kettensägen und an Ad-Blue-Zusatz für Dieselfahrzeuge) eine knappe und wertvolle Ware werden.

Lösungsansätze für Unternehmen:

Unternehmen sollten im Rahmen der Präventionsmaßnahmen ausreichend Treibstoff in gut gesicherten Tanklagern bevorraten und diesen zugleich in Lagern umfangreich sichern. Kraftstoffe wie Diesel können dabei nicht beliebig lang gelagert werden. Es kann auch bei einer fachkundigen Lagerung dazu kommen, dass der Kraftstoff verunreinigt wird. Aufgrund altersbedingter Veränderung oder mikrobiologischen Wachstums kann der Kraftstoff unbrauchbar werden oder zumindest an Qualität verlieren. Daher sollte der Dieselkraftstoff als Treibstoff von Notstromaggregaten regelmäßig umgeschlagen und mit Zusätzen versehen werden, damit nicht Verunreinigungen zu „Dieselpest" führen und somit die Notstromaggregate ausfallen lassen. Bei bestehenden Lieferverträgen mit Händlern sollte die „KRITIS-Resilienz" abgefragt und deren Durchhaltefähigkeit in den oben beschriebenen Mangellagen geprüft werden. Generell sollten Unternehmen prüfen, ob sie eigene Tankstellen mit ausreichend Tankkapazitäten in ihrem Werkgelände vorhalten können, um so in der Krise autark zu bleiben.

5.
Ausfall der Wasser- und Abwasserversorgung

Wasser gehört zu den wichtigsten Gütern. Es ist notwendig zur täglichen Deckung menschlicher Grundbedürfnisse. Es dient speziell Unternehmen als Rohstoff, als Prozess- und Kühlmittel und wird zugleich als Löschmittel u. a. für Werksfeuerwehren benötigt. Wasser ist somit für die Sparten der Wasserversorgung (mit Trink- und Brauchwasser und dem Abwasser) ein hochkomplexes technisches System. Es weist aufgrund seiner historisch gewachsenen Infrastruktur enge Verknüpfungen zu anderen KRITIS-Sektoren auf. In Deutschland gibt es ca. 6.200 Wasserversorger und ca. 7.000 Abwasserentsorger, zudem ca. 10.000 Kläranlagen mit ca. 10 Milliarden m³ Jahresabwassermenge (meist biologische Verfahren). Während der Durchschnittsverbrauch an Trinkwasser je Einwohner pro Tag bei ca. 129 Litern liegt (davon nur max. drei Liter zum Trinken und zum Kochen benötigt), werden ca. 44 Liter für Toilette und ca. 41 Liter für Baden und Duschen verwendet. Der virtuelle Wasserverbrauch (z. B. für die industrielle Produktion) liegt bei 4.000 bis 5.000 Litern pro Kopf pro Tag. Unabdingbar für eine Wasserversorgung ist dabei die Sicherstellung einer dauerhaften und stets störungsfreien Stromversorgung.

Sollte die Wasserversorgung durch Störung z. B. in der Stromversorgung ausfallen oder in einem Hitzesommer nicht ausreichend Wasser über Uferfiltrate, Flüsse und Seen zur Verfügung stehen, gibt es in Deutschland rund 5.200 Trinkwassernotbrunnen, die – zumindest eingeschränkt – eine Trinkwassernotversorgung sicherstellen sollen.

Die größte Gefahr für die Wasserversorgung der Unternehmen und deren großflächige Liegenschaften geht von einem Stromausfall aus. Dieser führt kurzfristig zu einem Wegfall der Pumpleistung. Infolgedessen herrscht nur noch ein sehr geringer Wasserdruck vor und es kommt zeitnah zu einem Zusammenbruch der Wasserversorgungsnetze.

Für einen zweiten Bereich, den Ausfall der Abwasserentsorgung, sind bislang nur wenige Untersuchungen bekannt. Die resiliente Abwasserentsorgung sollte Gegenstand einer Präventionsplanung sein. Fällt die Wasserversorgung aus, wird nur noch

wenig Flüssigkeit in den Rohrleitungen vorhanden sein. Die vorhandene Kanalisation ist aber auf einen Trinkwasserverbrauch von 130 Liter pro Person am Tag ausgelegt. Dagegen entfallen auf Notbrunnen nur noch 10 bis 15 Liter pro Kopf. Zudem steigt die Gefahr eines Ausfalls der eventuell vorhandenen biologischen Reinigung von Kläranlagen, so dass Kläranlagen ohne Strom nach sechs bis acht Stunden kippen. Ferner ist aufgrund der geringen Wassermengen mit Schäden an Abwasserrohrleitungen zu rechnen.

Lösungsansätze für Unternehmen:

Als notwendige Maßnahmen zur Kompensation im Bereich Wassermangel sollten Unternehmen ausreichend Wassermengen in Tanks vorhalten und hinlängliche Mengen an Trink- und Brauchwasser auch für die Räumlichkeiten eines Notfallstabs und der Mitarbeiter einrichten. Pro Mitarbeiter sollen pro Tag drei Liter Frischwasser für mindestens 14 Tage vorgehalten werden. An Brauchwasser, u. a. für die Toilettenspülung, sollten Tanks mit mehreren tausend Litern möglichst in höheren Etagen (vom Stabsraum ausgesehen, um ein Gefälle zu haben) veranschlagt werden.

Daneben sollten in größeren Werksgeländen eigene Trinkwassernotbrunnen eingerichtet werden und deren Betrieb regelmäßig geübt werden. Trinkwassernotbrunnen bedürfen einer hygienischen Überprüfung, ggf. müssen ausreichend Chlortabletten bereitgehalten werden.

Verfügen Unternehmen aufgrund ihrer Produktionsprozesse über eigene Kläranlagen, so sind diese mit leistungsstarken Notstromaggregaten auszustatten und bedürfen ausreichender Treibstoffmengen für die Aggregate. Bei größeren Werksgeländen ist zu prüfen, ob über eigene Wassertürme für längere Zeit der Wasserdruck im Netz aufrechterhalten werden kann.

Erste Arbeitslösungen für Unternehmen und deren Notfallstäbe sind:

- Natürliches Gefälle für Trinkwasserversorgung beachten
- Bereitstellung von Notbrunnen sichern

- Notstromersatzanlagen und deren Leistungen nachfragen
- Kommunikation klären
- Ausplanung von Latrinenkonzepten für die Belegschaft
- Mobile Wasseraufbereitungsanlagen bereitstellen: Kapazitäten erfragen

6.
Ausfall der Informationstechnik und Telekommunikation

Ein Ausfall der Informationstechnik und Kommunikation hat gravierende Auswirkungen auf alle KRITIS-Sektoren und die Arbeit der Einsatzkräfte (Bereitschaftsdienste vor Ort), der Krisen- und Verwaltungsstäbe von Behörden, der Notfallstäbe von Unternehmen sowie der sogenannten Blaulichtorganisationen (BOS).

Ohne Kommunikation ist Krisenmanagement nicht möglich bzw. alle Entscheidungen und deren Umsetzung werden extrem lange dauern. Damit eine organisierte Krisenbewältigung möglich wird, ist auch der Informationsaustausch zwischen den unterschiedlichen Akteuren der Krisenbewältigung erforderlich. Bei einem Blackout werden nur limitierte Übertragungswege zur Verfügung stehen. Parallel dazu wird sich der Koordinierungsbedarf deutlich erhöhen.

Während der Zeit des Krisen- bzw. Katastrophenfalles bis zur Wiederherstellung eines sicheren Zustandes ist es wichtig, dass eine zuverlässige und reibungslose Kommunikation in regelmäßigen Zeitabständen wichtige Informationen im Zusammenhang mit der Lage liefert, um mit allen in der Schadenslage beteiligten Firmenangehörigen, Vertretern der Gebietskörperschaften (Stadt/Kreis/Landkreis) sowie mit den BOS in Kontakt zu bleiben.

Am Beispiel des bislang größten Kommunikations-Gaus in Deutschland, dem Ausfall des Telekom-Netzes in Siegen-Wittgenstein am 21. Januar 2013, bei dem 500.000 Haushalte und zahlreiche Unternehmen in den benachbarten Kreisen bis zu fünf Tage

betroffen waren, hat sich gezeigt, dass nicht nur Telefon und Internet, nein sogar der Funk, aber auch Datenleitungen und der elektronische Belegfluss im Führungsstab der Einsatzkräfte nachhaltig betroffen und ausgefallen waren. Lediglich Richtfunk und die Arbeit in einem D2-Netz sowie der Einsatz von Meldern und Boten konnten noch genutzt werden.

Im Falle eines großflächigen Stromausfalles im Sinne eines Blackouts würde binnen weniger Minuten nach Schadenseintritt das gesamte Telefonfestnetz und das Mobilfunknetz sowie das Internet ausfallen. Nach Aussagen der Netzbetreiber Deutsche Telekom und Vodafone sind zwar die Antennenstandorte zur kurzzeitigen Überbrückung von Stromausfällen mit Batterien ausgestattet. Jedoch bereits nach zwei bis vier Stunden ohne Strom sei deren vorgehaltene Batteriekapazität aufgebraucht. Lediglich mit einem schnurgebundenen analogen Telefon wäre Kommunikation untereinander von einem zum anderen analogen Geräten noch möglich. Telefone mittels ISDN, VOIP, Basisstationen von schnurlosen DECT-Mobilteilen, wie auch Telefonanlagen funktionieren dagegen ohne Lichtstrom nicht mehr.

Lösungsansätze für Unternehmen:

Betroffene Kommunen nutzen bislang den Einsatz von Lautsprecherwagen. Diese informieren die Bevölkerung in regelmäßigen Zeitabständen und geben Hinweise aus Rundfunksendern, die noch zeitlich begrenzt Lagemeldungen senden können – beispielsweise die Empfehlung zur Nutzung von batteriegestützten Radios. Unternehmen und deren Notfallstäbe sollten sich bereits in der Phase der Prävention mit der Erstellung eines Notkommunikationsplans befassen, um im Krisenfall eines Blackouts die Kommunikation untereinander zu gewährleisten.

Die Kommunikation im Krisenfall kann neben dem Einsatz von Meldern und Boten noch über Analogfunk, CB-Funk oder Feldtelefon gehalten werden. Der Einsatz kostenintensiver Satelliten-Telefone scheint auf den ersten Blick eine vielversprechende Rückfallebene der Kommunikation zu sein. Allein Satellitentelefone mit entsprechenden Freischaltungen und Verträgen stellen ein verlässliches Kommunikationsmittel dar, vorausgesetzt, sie werden außerhalb von Gebäuden und Kellern mit Empfang zum Satelliten genutzt.

Um möglichen Überlastungen vorzubeugen, sind hierzu aber im Vorfeld sämtliche Kommunikationsbeziehungen und -prozesse festzulegen und die Funktionsfähigkeit der geplanten Maßnahmen in Übungen zu überprüfen.

Allerdings werden in einem flächendeckenden Blackout ganzer Landesteile die Satelliten-Kapazitäten (im Vorwärts- und Rückwärtskanal) aufgrund eingeschränkter Datenmengenkapazitäten überlastet sein und dementsprechend auch ausfallen. In einer bislang wenig bekannten Studie des Fraunhofer-Instituts für Integrierte Schaltungen IIS wurden die Defizite hinreichend belegt und geben Anlass zur berechtigten Sorge, dass auch dieses Medium, auf das die Kommunen derzeit ihre Hoffnungen setzen, nur eingeschränkt nutzbar sein wird.

7.
Ausfall von Arbeits- und Fachkräften durch Infektionsausbrüche

Im Zuge der Corona-Pandemie, wie auch bei Grippe-Wellen, gab es Sorge und Warnungen, dass Kritische Infrastrukturen zusammenbrechen könnten, weil die Belegschaft in weiten Teilen erkranken würde.

Im Januar 2022 meldeten bis zu 40 Prozent aller Betriebe hohe Erkrankungsraten und hatten Probleme im Betriebsablauf. Zugleich mehrten sich Hinweise, dass durch Folgeerscheinungen, wie z. B. Kindererkrankungen, die häusliche private Betreuung nicht mehr ausreichend gewährleistet wäre und Arbeitnehmer daher ausfallen könnten.

Betriebe fingen seit Beginn der Corona-Pandemie im Frühjahr 2020 an, Schritt für Schritt die betrieblichen Pandemieplanung anzupassen. Da die genauen Auswirkungen (Verlauf und Schwere) einer Pandemie nicht vorhergesagt, allenfalls mit Prognosemodellen geschätzt werden konnten, waren vereinzelt Modellrechnungen von Erkrankungsraten, nicht selten von 50 bis 60 Prozent, Gegenstand von Pandemieplänen. Besondere Bedeutung bekamen Mitarbeiter, deren Familienangehörige

erkrankten und versorgt werden mussten, so dass viele betriebliche Prozesse nicht mehr aufrechterhalten werden konnten und Produktionsbetriebe über einen längeren Zeitraum geschlossen werden mussten.

Dadurch können Unternehmen durch Nichteinhaltung vertraglicher Verpflichtungen finanzielle Schäden entstehen.

Lösungsansätze für Unternehmen:

Unternehmen sollten ihre Notfallpläne und Hygieneschutzverordnungen stets aktuellen Bedrohungslagen anpassen. Dabei können betriebliche organisatorische Maßnahmen einen erheblichen Beitrag zur Reduzierung der Ansteckungsgefahr leisten.

Die Pandemiepläne erforderten ein sogenanntes Change-Management mit aufgeschlossenen Veränderungen in einer Pandemielage und seiner Auswirkungen auf das Personalmanagement vom Notfallstab. Hinsichtlich des Schutzes und der Sicherung der Mitarbeiter in allen Phasen/Lagen sollten die Vorgaben des BBK von Mitte März 2020, hier im Detail die Analyse der Handlungsempfehlungen für Unternehmen insbesondere für Betreiber Kritischer Infrastrukturen mit der bekannten 9-Punkte-Checkliste für ein Krisenmanagement in einer Pandemie, beachtet werden.

Im Detail bedeutet dies das Aufzeigen der wichtigen Vorgaben für ein betriebliches Krisenmanagement, hier die bestmögliche Aufrechterhaltung der Funktionsfähigkeit Kritischer Infrastrukturen bzw. der schnellstmögliche Wiederanlauf der kritischen Prozesse nach einer Störung.

Schutz der Beschäftigten

- Maßnahmen zur frühzeitigen und ausreichenden Information des Personals
- Bereitstellung von Schutzausstattung
- Allgemeine Verhaltens- und Hygieneregeln
- Gegebenenfalls Zutrittsbeurteilungen

Personalausfall aufgrund von Quarantänemaßnahmen

Zu prüfen sind:

- Das Vorhalten des betrieblichen Personals im Rahmen von Quarantänemaßnahmen während und nach dem Dienstbetrieb für mindestens 14 Tage, insbesondere bei betroffenem Schlüsselpersonal
- Empfehlungen für die Besetzung von Schlüsselfunktionen entsprechend der Personalplanung, u. a. durch Stellvertretungsregelungen sicherzustellen
- Personalausfall aufgrund der Schließung von Schulen, Kitas und anderen öffentlichen Einrichtungen
- Ausgangsbeschränkungen bzw. Kontaktverbote

Alle oben genannten Maßnahmen sollten immer unter Beachtung der Auswirkungen auf die Cybersicherheitslage bei Nutzung von Homeoffice gesehen werden.

8.
Gefahr gestörter Lieferketten und Handelshemmnisse

Dem Supply-Chain-Management kommt in einer globalisierten Gesellschaft und darin agierenden Unternehmen eine erhebliche und weiter steigende Bedeutung zu. Die Bestandteile der Kette als ein wichtiger Bestandteil der wertschöpfenden Tätigkeiten dürfen nicht unterbrochen werden oder gar ausfallen. In der Vergangenheit unterlagen diese einer starken Effizienzbetrachtung mit dem Ziel einer Gewinnoptimierung über alle Ebenen hinweg.

Veränderte Sicherheitslagen im Ausland, geopolitische Spannungen, mögliche Sperrungen der Seewege von Schifffahrtslinien durch Rebellenaktivitäten, neue Zollhindernisse langjähriger Partnerländer (hier: von den USA) sowie Seuchen bzw.

Pandemien stellen Unternehmen vor nachhaltige Herausforderungen und somit vor wirtschaftliche Probleme, um bestehende Vereinbarungen und Verträge fristgerecht zu erfüllen. Erstrecken sich Lieferketten über mehrere Kontinente, können schnell sogenannte Bullwhip-Effekte zu Nachfrageveränderungen und somit zu Streitereien in der Prozesskette – von der Rohstoffgewinnung über die einzelnen Stationen der Zwischenprodukt-Aufbereitung bis hin zum Endprodukt und seinem Absatz am Zielort – führen.

Ein bekannter Fall war die Automobilindustrie und deren Auslagerung der Produktion und Teileerstellung in Niedriglohnländern. Auch der medizinische Sektor mit der Ausrichtung auf Billigproduktion von Pharma-Produkten nach China hat gezeigt, was im Falle von Lieferengpässen schnell am deutschen Verbrauchermarkt passieren kann. Nicht-Verfügbarkeit von Produkten oder deren lange Lieferzeiten können selbst bei gleicher Nachfrage zu deutlich steigenden Preisen bei Verbrauchern führen.

Natürlich geben erste Störungen in der Lieferkette nicht immer Anlass für Rechtsstreitigkeiten. Mit der Ausweitung an Lieferketten über mehrere Länder und Kontinente kann die Anzahl der Probleme schnell ansteigen. Die Auswirkungen von Rechtsstreitigkeiten können sich neben den bekannten Vertragspartnern auch auf Untervertragspartner in weiteren Ländern ausweiten. Effekte dieser negativen Art können sich im Rahmen des sogenannten Spill Over-Effekts auch auf weitere Marktteilnehmer auswirken, so dass sich Verluste in der Wertschöpfungskette potenzieren können. Einher gehen mit diesen Effekten stets Zeitverzögerungen und steigende Kosten, die im Extremfall sogar einen vollkommenen Produktionsstopp bedingen. In den letzten Jahren sind die Gesamtverlustrisiken deutlich angestiegen. Unter Umständen sind dadurch gesamte Lieferkettenabschnitte bedroht.

Lösungsansätze für Unternehmen:

Unternehmen sollten prüfen, ob der Einsatz von mehr Geld für teurere Produkte alternativer Lieferanten mit kürzeren Lieferwegen und wenigen Akteuren nicht der bessere Weg ist. Dies ist abhängig von den Gewinnmargen der jeweiligen Branchen. Zum anderen könnten mit einer Aufklärungskampagne im Vorfeld eines Geschäftes die jeweiligen potenziellen Akteure entlang der Lieferkette dahingehend informiert werden, wie komplex und verletzbar das

Beziehungsgeflecht bei veränderten Rahmenbedingungen ist. Es ist also höchste Zeit, dass alle Akteure entlang der Lieferkette ein Verständnis dafür entwickeln, wie komplex das Beziehungsgeflecht inzwischen geworden ist. Darüber hinaus können mögliche Redundanzen gesucht, abgestellt und die Flexibilität der Lieferketten somit gestärkt werden.

Zusammenfassend sollte das gesamte Lieferkettenmanagement auf agile Beschaffung, Nachhaltigkeit und Resilienz überprüft werden. Im Einzelfall können unabhängige Sachverständige als neutrale Fachberater Lösungswege aufzeigen.

9. Bedrohungen durch Kriminalität und Terrorismus

Mit der wachsenden Globalisierung und den zunehmenden internationalen Verflechtungen von Unternehmen entstehen nicht nur neue wirtschaftliche Perspektiven, sondern auch neue Möglichkeiten für kriminelle Aktivitäten. Deutsche Unternehmen, bekannt für technologischen Fortschritt und hohe Qualität, sehen sich verstärkt Angriffen ausgesetzt, wobei sowohl große Konzerne als auch kleine und mittelständische Betriebe betroffen sind.

Wichtige Phänomene der aktuellen Kriminalitätslage sind:

- **Cyberkriminalität:** Eine der größten Bedrohungen, bei der Straftaten über das Internet und andere digitale Netzwerke begangen werden, einschließlich Malware, Phishing und Ransomware.
- **Terrorismus:** Ein ernstzunehmendes Problem, das durch Gewalt und Einschüchterung politische Ziele verfolgt. Extremistische Gruppen haben ihre Aktivitäten in den letzten Jahren ausgeweitet.
- **Organisierte Kriminalität:** Kriminelle Gruppen, die sich auf illegale Aktivitäten spezialisiert haben und schwer zu bekämpfen sind.

- **Korruption:** Der Missbrauch von Macht zur Erlangung persönlicher Vorteile, der das Vertrauen in Institutionen und Regierungen untergräbt.
- **Gewaltkriminalität:** Umfasst Straftaten wie Mord, Körperverletzung und Raub, die sowohl von Einzeltätern als auch von organisierten Gruppen begangen werden.
- **Sabotage:** Infolge des russischen Angriffs auf die Ukraine sehen sich deutsche Unternehmen, unabhängig von Größe und Umsatz, verstärkt Bedrohungen durch Ausspähungen und Sabotageaktionen ausgesetzt. Sabotageschutz wird zunehmend wichtig, um Unternehmen vor gezielten Eingriffen, Zerstörungen oder Störungen durch interne oder externe Personen zu schützen. Typische Risikobereiche sind Produktionsanlagen, IT-Infrastruktur und Forschungs- und Entwicklungsabteilungen.
- **Ziele des Sabotageschutzes:**
  - Schutz von Betriebsabläufen vor gezielten Störungen.
  - Sicherung sensibler Informationen.
  - Verhinderung wirtschaftlicher Schäden.
  - Vermeidung von Reputationsverlust.
- **Arten der Sabotage:**
  - **Physische Sabotage:** Zerstörung oder Manipulation von Maschinen und IT-Hardware, Brandstiftung, Sabotage von Versorgungsleitungen.
  - **Digitale Sabotage (Cyber-Sabotage):** Einschleusen von Schadsoftware, Lahmlegung von IT-Systemen, Manipulation von Produktionssteuerungen.
  - **Innere Sabotage:** Datenklau und absichtliches Fehlverhalten durch frustrierte oder radikalisierte Mitarbeiter.
- **Maßnahmen zum Sabotageschutz:**

  Organisatorische Maßnahmen
  - **Zutrittskontrollen:** Implementierung von Ausweissystemen und Besuchermanagement zur Einschränkung des Zugangs zu sensiblen Bereichen.
  - **Sicherheitsrichtlinien:** Entwicklung und Durchsetzung klarer Sicherheitsrichtlinien und Verhaltensvorgaben.

- **Mitarbeiterschulungen:** Regelmäßige Sensibilisierung und Schulung der Mitarbeiter zu den Risiken von Sabotage.
- **Sicherheitsüberprüfungen:** Durchführung von Sicherheitsüberprüfungen bei Bewerbern für kritische Positionen.

Technische Maßnahmen

- **Videoüberwachung:** Einsatz von Kameras und Alarmanlagen zur Überwachung sensibler Bereiche.
- **Netzwerküberwachung:** Implementierung von Firewalls, Antivirensoftware und Netzwerküberwachung zur Erkennung von Bedrohungen.
- **Backup-Systeme:** Einrichtung von Backup- und Wiederherstellungssystemen zum Schutz vor Datenverlust.
- **Segmentierung und Verschlüsselung:** Schutz sensibler Systeme durch Segmentierung und Verschlüsselung von Daten.

Personelle Maßnahmen

- **Sicherheitsdienst:** Bereitstellung von Sicherheitsdiensten und Werkschutz zur Überwachung und Reaktion auf Sicherheitsvorfälle.
- **Umgang mit Insiderbedrohungen:** Implementierung von Whistleblower-Systemen und anderen Maßnahmen zur Erkennung und Meldung von Insiderbedrohungen.

- **Spionage:** Spionage ist ein ernstzunehmendes Thema für deutsche Unternehmen, sowohl durch staatliche Akteure als auch durch organisierte Kriminalität oder Wettbewerber.
- **Formen der Wirtschaftsspionage/Konkurrenzausspähung:**
  - **Staatlich gelenkte Spionage:** Ziel auf Schlüsseltechnologien in Branchen wie Maschinenbau, Chemie und IT.
  - **Konkurrenzausspähung:** Private Konkurrenten versuchen, Informationen über Produkte, Patente und Strategien zu erlangen.
  - **Cyberangriffe:** Phishing, Malware und Ransomware, wobei besonders KMUs gefährdet sind.
  - **Innere Risiken (Insider):** Mitarbeiter geben Informationen weiter.

- **Social Engineering:** Manipulation von Personen, um an sensible Daten zu gelangen.

- **Besonders gefährdete Branchen:**
  - Rüstungsindustrie
  - Automobil- und Maschinenbau
  - Chemie und Pharma
  - IT und Software
  - Energie und Infrastruktur

In Zeiten zunehmender geopolitischer Spannungen und Cyberbedrohungen gewinnen sowohl Sabotage- als auch Spionageschutzmaßnahmen stark an Bedeutung. Unternehmen müssen proaktive Strategien entwickeln, um sich gegen diese Bedrohungen zu wappnen und ihre sensiblen Informationen zu schützen.

Um die Auswirkungen von Kriminalität, insbesondere Spionage und Sabotage, auf Unternehmen zu minimieren, sollten verschiedene Maßnahmen ergriffen werden. Zunächst ist es entscheidend, kontinuierlich angemessene Sicherheitsmaßnahmen zu implementieren, einschließlich des Einsatzes von Sicherheitspersonal und moderner Technologien.

Der Einsatz von Perimeterschutz-Systemen, wie Alarmanlagen und Überwachungskameras, schützt vor unbefugtem Eindringen. Zudem sollten Mitarbeiter über Sicherheitsmaßnahmen informiert und geschult werden, um angemessen auf kriminelle Aktivitäten reagieren zu können.

Eine enge Zusammenarbeit mit Strafverfolgungsbehörden ist wichtig, um Kriminalität zu verhindern und zu bekämpfen. Darüber hinaus fördert die Netzwerkbildung mit anderen Unternehmen den Austausch von Best Practices zur Vermeidung von Kriminalität.

Durch die Umsetzung dieser Ansätze können Unternehmen ihre Sicherheitslage stärken und das Risiko krimineller Aktivitäten erheblich reduzieren.

10.
Cyberrisiken/
Gefährdung der Datensicherheit

In den letzten Jahren haben Cyberangriffe auf deutsche Unternehmen erheblich zugenommen. Laut Branchenverband Bitkom verursachten Cyberkriminelle allein in den letzten beiden Jahren einen Gesamtschaden von 202 Milliarden Euro für die deutsche Wirtschaft. Im Jahr 2025 waren 87 Prozent der Unternehmen von Datendiebstahl betroffen, wobei Ransomware und Phishing die häufigsten Angriffsmethoden darstellen. Auch analoge Angriffe, wie der Diebstahl physischer Dokumente und das Abhören von Gesprächen, nehmen zu.

Deutschland ist in Europa das am häufigsten von Hackerangriffen betroffene Land. Die zunehmende Vernetzung und Digitalisierung von Prozessen erhöhen die digitale Verwundbarkeit. Cyberangriffe, Cyberspionage und Cybersabotage bedrohen nicht nur Unternehmen, sondern auch die demokratische Gesellschaft. Daher sollten der wirksame Schutz gegen Cyberangriffe und die Stärkung der Cyberresilienz oberste Priorität für Unternehmen haben.

Besonders kleine und mittlere Unternehmen benötigen fachliche Unterstützung, da das Bewusstsein für die Gefahrenlage oft nicht ausreichend ausgeprägt ist. Ein effektives Präventionsmanagement ist entscheidend, um die Existenz eines Unternehmens zu schützen und das Schadenspotenzial zu minimieren.

Die Hauptbedrohung bleibt Ransomware, ergänzt durch Distributed-Denial-of-Service (DDoS)-Angriffe von sogenannten Hacktivisten.

Lösungsansätze für Unternehmen:

Zur Vertiefung dieser wichtigen Thematik eignen sich sowohl das Kompendium Cyber-Security der Stiftung Familienunternehmen als auch die aktuellen Studien und Empfehlungen des BSI. Sie zeigen neben den aktuellen Gefahren aus dem Cyber-Raum auch Lösungsbeispiele und Präventionsstrategien auf

und führen umfangreiche Listen von Anlaufstellen auf Bundes- und Landesebene für den Fall eingetretener Cyberangriffe auf. Hier kommt es auf ein zeitnahes und entschlossenes Handeln an.

Darüber hinaus sollten die Warnungen des BSI ernst genommen werden. Das BSI rät in einem Lockbit-Papier, die Server eines Unternehmens kontinuierlich mit aktueller Anti-Viren-Software zu bespielen, ggf. sogenannte Sandboxed Browsers zu installieren, mit denen Mitarbeiter im Internet surfen können, ohne direkt einen Anschluss zum Firmennetzwerk zu legen. Die Rechte von Administratoren, die Zugriff auf kritische IT-Prozesse haben, sollten möglichst eng begrenzt werden. Mitarbeiter sind zu belehren, dass Drucker und Faxgeräte ein gängiges Einfallstor für Hackerangriffe darstellen, insbesondere wenn Mitarbeiter im Homeoffice deren häusliche Anlagen für betriebliche Zwecke nutzen und diese wenig geschützt sind.

11. Militärischer Konflikt/Krisenfall

Spätestens seit Beginn des russischen Angriffskriegs gegen die Ukraine am 24. Februar 2022 sind die europäischen Staaten und NATO-Partner alarmiert, dass Russland seine expansive Außenpolitik mit militärischen Mitteln zum Leidwesen weiterer Staaten fortsetzt. Damit stellt sich für Unternehmen, Bevölkerung und Verwaltungen die Frage, wie im Vorfeld eines militärisch nicht mehr gänzlich auszuschließenden Konfliktes mit Russland die deutschen Unternehmen – insbesondere Betreiber kritischer Infrastrukturen, aber auch „Nicht-KRITIS-Unternehmen" – aufgrund von Lieferkettenabhängigkeiten in die staatliche Sicherheitsvorsorge einbezogen werden.

Zu unterscheiden sind folgende Phasen der Konfliktverschärfung:

- **Zustimmungsfall**
  Noch bevor es zu einem Spannungs- oder Verteidigungsfall kommt, kann der Deutsche Bundestag der Anwendung einzelner oder aller Notstandsvorschriften nach Artikel 80 a Grundgesetz (GG) zustimmen. Dadurch soll es dem Parlament

ermöglicht werden, gezielt Verteidigungsmaßnahmen vorzubereiten.

Unternehmen sollten in dieser Phase ihre Vorbereitungen auf die folgenden Fälle und bestehende Konzepte prüfen.

- **Spannungsfall**
  Der Spannungsfall nach Artikel 80 a GG ist die Vorstufe zum Verteidigungsfall. Er erweitert die Befugnisse der Bundesregierung, bestimmte Notstandsgesetze bereits vorzeitig anzuwenden, wenn der Deutsche Bundestag den Spannungsfall feststellt.

- **Verteidigungsfall**
  In Art. 115 a ff. Grundgesetz (GG) wird im Deutschen Bundestag mit Zustimmung des Bundesrates (mit einfacher Mehrheit) der Verteidigungsfall festgestellt, wenn das Bundesgebiet mit Waffengewalt angegriffen wird oder ein solcher Angriff unmittelbar bevorsteht. Auch für den Fall, dass der Deutsche Bundestag handlungsunfähig ist, wird diese Entscheidung durch den Gemeinsamen Ausschuss (Art. 115a Abs. 2 GG) getroffen.

Die politischen und staatlichen Folgen eines Inkrafttretens der Notstandsverfassung bedingen besondere Regelungen zur Gesetzgebung, zur Verwaltung und zu Einsatz und Umfang der Bundeswehr. Die Exekutive erhält erweiterte Befugnisse, d. h. die Bundesregierung kann schnellere Entscheidungen treffen. Verkürzte Gesetzgebungsverfahren ermöglichen es, notwendige Gesetze in einem Schritt zu erlassen. Zugleich kann es zu einer Verlängerung der Wahlperiode kommen, so dass der Deutsche Bundestag länger im Amt bleibt und anstehende Wahlen verschoben werden.

Mit den o. g. Fällen treten folgende Gesetze in Kraft, die auch Unternehmen im besonderen Maße treffen:

Sicherstellungs- und Vorsorgegesetze

Sicherstellungs- und Vorsorgegesetze treten im Falle einer Feststellung des äußeren Notstandes, also für den Verteidigungsfall Deutschlands als anwendbare Gesetze in Kraft. Diese Eingriffsrechte betreffen alle Wirtschaftsbereiche und können Unternehmen verpflichten, Leistungen und ihre Infrastruktur zur Verfügung zu stellen.

Vorsorgegesetze hingegen können auch im Fall besonderer Gefahrenlagen, etwa

Naturkatastrophen, angewendet werden.

Das Wirtschaftssicherstellungsgesetz (WiSiG) dient bereits im Spannungsfall dazu, planwirtschaftliche Maßnahmen durch Verordnungen der Bundesregierung, z. B. zur Steuerung von Produktion, Rohstoffverteilung und Vorratswirtschaft bis hin zu Lieferketten, zu treffen. Darüber hinaus kann auch der Finanzsektor etwa mit der Schließung der Börsen betroffen sein.

Über das Bundesleistungsgesetz (BLG) kann durch den Staat auf Sachen, Grundstücke sowie Werk- und Verkehrsleistungen zugegriffen werden.

Für den Fall, dass bestimme Liegenschaften für die Verteidigung benötigt werden, kann durch das Landesbeschaffungsgesetz (LBG) auf diese Flächen zugegriffen (z. T. Enteignung) werden. Weitergehende Nutzungseinschränkungen von Grundstücken können durch das Schutzbereichsgesetz (SchBerG) erlassen werden.

Für einzelne Wirtschaftssektoren können weitergehende Regelungsfälle Geltung finden:

Das Energiesicherungsgesetz (EnSiG) erlaubt unabhängig vom Verteidigungsfall Eingriffe in die Produktion, die Verteilung und Lagerung sowie die Preisbindung von Energieträgern. KRITIS-Betreiber können dabei gemäß KRITIS-Verordnung vom BSI unter Treuhandverwaltung bis hin zu einer Enteignung gestellt werden.

Im Rahmen des Ernährungssicherstellungs- und -vorsorgegesetzes (ESVG) kann die Bundesregierung zur Abwendung einer Versorgungskrise Maßnahmen zur Steigerung der Lebensmittelproduktion und zur zentralen Verteilung anordnen. Dies betrifft auch die Sicherstellung der Wasserversorgung, hier über das Wassersicherstellungsgesetz (WasSiG), welches Unternehmen zum Bau von Notbrunnen verpflichten kann.

Weitere Vorgaben liegen mit dem Postsicherstellungsgesetz (PSG) vor, welches die Postunternehmen zur Priorisierung von Postbevorrechtigungen (hier: Bundeswehr, Behörden, Gesundheitswesen) bei Störungen der Zustellungen verpflichtet und den Betrieb einer Feldpost regelt. Vergleichbare Vorgaben mit Einschnitten treffen auch mit dem Telekommunikationsgesetz (TKG) zu, die den Telekommunikationsanbietern Vorgaben machen.

Mit dem Verkehrssicherstellungsgesetz (VerkSiG) wird der Zugriff und die Steuerung

auf die Bereiche Verkehrsinfrastruktur geregelt, um diese aufrecht zu erhalten.

Die Mehrzahl der o. g. Gesetzesvorgaben zeigt damit auf, in welcher Vielfalt der Staat im Krisen- oder im Spannungs- bis hin zum Verteidigungsfall auf privatwirtschaftliche Ressourcen zugreifen kann.

Konkret müssen sich Unternehmen auf folgende mögliche Aufgaben einstellen, die in Friedenszeiten so nicht ausgeführt werden. Speziell die KRITIS-Betreiber (Energie, Wasser, IT, Gesundheit, Transport, Ernährung) und bestimmte „Nicht-KRITIS-Zulieferfirmen" müssen Pläne für die Umsetzung bereithalten, wenn erste Einschränkungen bei Lieferketten, Personalbereitstellung bzw. schon vermehrten Cyberangriffen auf die Minderung der Produktionsfähigkeit des Unternehmens hinwirken. Zugleich bietet es dem Staat die Möglichkeit, Unternehmen zu verpflichten, deren Kapazitäten für die öffentliche Versorgung bereitzustellen bzw. hochzufahren. Produzierende Unternehmen können zur Priorisierung bestimmter Produkte oder Rohstoffe angewiesen werden (z. B.: ein Maschinenbauunternehmen produziert nur noch Ersatzteile für Energie- oder Rüstungsindustrie).

Weitere Regelungen und Eingriffe wirken auf den Sektor Logistik/Transport. Hier können frühzeitig Fahrzeuge, Lagerflächen und Personal für staatliche Zwecke eingeplant werden. Unternehmen aus dem Bereich der IT- und Kommunikation müssen für die Aufrechterhaltung sicherer Kommunikationskanäle sorgen. Zugleich unterliegen sie einer erhöhten Cybersicherheits- und Geheimhaltungspflicht.

Erwartungen an Unternehmen im Spannungsfall:

- **Business Continuity Management:** Pläne müssen spätestens jetzt aktiv werden.
- **Kooperation mit Behörden:** Unternehmen treten in Austausch mit Krisenstäben (z. B. Landratsamt, Bundesnetzagentur).
- **Kommunikation:** Transparenz gegenüber Mitarbeitern, enge Abstimmung mit Verwaltung und Verbänden.
- **Resilienz:** Vorratshaltung, Notstrom, redundante IT-Systeme, Schutz vor Cyberangriffen.

Es lässt sich festhalten, dass bereits im Spannungsfall (erst recht im Verteidigungsfall)

Unternehmen nicht nur Betroffene sind, sondern aktive Bausteine der staatlichen Sicherheitsarchitektur. Sie müssen ihre Leistungen stabil halten, können staatlich zur Mitwirkung verpflichtet werden und sollten ihre Krisen- und BCM-Pläne dazu aufgestellt haben, um diese frühzeitig aktivieren zu können.

Gravierende Auswirkungen hat dies unmittelbar auf die Bundeswehr. Der Einsatz der Bundeswehr zur Landesverteidigung im In- und Ausland erhält höchste Priorität. Eine ausgesetzte Wehrpflicht kann wieder aktiviert werden. Reservisten können zeitnah einberufen werden. Spezielles Personal von Unternehmen, vorrangig solche als Reservisten, können zur Bundeswehr eingezogen werden; gleichzeitig können Fachkräfte für kriegswichtige Betriebe freigestellt werden.

Zusammenfassend lässt sich festhalten, dass im Verteidigungsfall Unternehmen einen großen Teil ihrer wirtschaftlichen Eigenständigkeit verlieren und selbst faktisch zu verlängerten Armen der staatlichen Gesamtverteidigung werden. Im Unterschied zum Spannungsfall, während dort noch „Vorbereitung und Kooperation" im Vordergrund stehen, gilt im Verteidigungsfall ein staatlicher Durchgriff mit verbindlichen Verpflichtungen.

Vorsorgemaßnahmen für Unternehmen:

Die hohe Anzahl an Sicherstellungs- und Vorsorgegesetzen verdeutlicht, wie umfangreich und zugleich in die Tiefe gehend der Staat im Krisen- oder Verteidigungsfall eingreifen kann. Unternehmen werden dadurch veranlasst, die vom Staat geforderten Maßnahmen zeitnah und umfassend auszuführen. Damit werden Unternehmen ein wichtiger Teil einer strategischen Resilienz des Staates.

Unternehmen sollten daher ihre Krisen-, BCM- und Notfallpläne auf diese spezielle Form der Bewirtschaftung (d. h. die staatliche Bevormundung einer Inanspruchnahme) ausrichten und kritisch prüfen.

Bereits in Friedenszeiten sollte ein guter Kontakt zu den Behörden (Landratsämter/Kreisverwaltung und Verwaltungen der kreisfreien Städte, ggf. zu Verwaltungen größerer kreisangehöriger Städte und deren Krisen-/Verwaltungsstäben) gesucht und durch gemeinsame koordinierte Ausbildungen und Übungen vertieft werden.

II. Business Continuity Management und Notfallpläne

Die Resilienz- und Durchhaltefähigkeit eines Unternehmens gegenüber existenzbedrohenden Risiken von innen und außen, vor bekannten als auch vor neuen Gefahrenlagen (u. a. in KRITIS-Bereichen) und die Erfüllung der branchenspezifischen rechtlichen und vertraglichen Anforderungen sind die Kernaufgaben eines nachhaltigen Krisenmanagements.

In einer zunehmend volatilen, unsicheren, komplexen und ambivalenten Welt stehen Unternehmen und deren Führungskräfte einschließlich der zuständigen, mit Sicherheitsaufgaben betrauten Personen vor einer Vielzahl von Herausforderungen. Die globale Wirtschaft, disruptive Technologien, sich ändernde Kundenbedürfnisse und unvorhersehbare politische und geopolitische Ereignisse sind nur einige Beispiele für die Unsicherheiten, mit denen Unternehmen täglich konfrontiert sind.

Inmitten dieses turbulenten Umfelds ist das BCM wichtiger Bestandteil einer unverzichtbaren Strategie, um die Widerstandsfähigkeit und den Bestand des Unternehmens nachhaltig zu sichern. Die Bedeutung des BCM geht dabei über die reine Sicherstellung der Geschäftskontinuität hinaus.

Im Folgenden sind explizit die wichtigsten Gründe für die Einführung und Umsetzung eines BCM im Unternehmen aufgeführt:

- Schutz der Geschäftskontinuität:
  Die Sicherstellung der Geschäftskontinuität ist der zentrale Aspekt des BCM. Allein Unternehmen, die jederzeit und dauerhaft ihre Geschäftskontinuität sicherstellen können, sind in der Lage, Störungen zu bewältigen und Ausfallzeiten zu minimieren. Dies hilft, den Geschäftsbetrieb aufrechtzuerhalten, Kundenerwartungen zu erfüllen und die gesteckten Geschäftsziele zeitrealistisch zu erreichen.

- Risikomanagement:
  Ein optimiertes BCM-Konzept hilft Unternehmen, ihre Risiken besser zu verstehen und zu bewerten. Erst auf Basis der Identifizierung kritischer Geschäftsprozesse im Unternehmen, von Geschäftssystemen sowie äußerer auf das Unternehmen einwirkender Gefahren kann eine nachvollziehbare Bewertung aller Risiken für das jeweilige Unternehmen vorgenommen werden. Unternehmen werden so in die Lage versetzt, frühzeitig die richtigen Maßnahmen zu ergreifen, um ihre Widerstandsfähigkeit zu erhöhen

- Compliance:
  BCM hilft Unternehmen, ihre Compliance-Anforderungen konsequent zu erfüllen. Viele Branchen weisen spezifische Vorschriften und Standards auf, die Unternehmen einhalten müssen, um ihre Geschäftskontinuität dauerhaft sicherzustellen. BCM kann hierbei wesentlich helfen, diese Anforderungen zu erfüllen und in Form rechtlich prüfbarer Nachweise beweissichernd zu dokumentieren.

- Verbesserung der Reaktionsfähigkeit:
  BCM hilft Unternehmen, ihre Reaktionsfähigkeit für alle denkbaren als auch realistisch erwartbaren Krisensituationen zu verbessern. Durch die Implementierung von BCM-Strategien und -Plänen können Unternehmen schnell und effektiv auf plötzliche Ereignisse reagieren und somit ihre Geschäftskontinuität sicherstellen bzw. zeitnah wieder die Ausgangssituation vor der Krise/dem Schadensfall einnehmen.

- Schutz der Reputation des Unternehmens:
  Ein schnelles und effektives Krisen-/Resilienzmanagement kann dazu beitragen, das Image eines Unternehmens zu schützen. Unternehmen, die im Rahmen erstellter Notfallpläne gut auf Krisen vorbereitet sind und schnell reagieren können, werden so besser in die Lage versetzt, das Vertrauen ihrer Kunden und Stakeholder aufrechtzuerhalten.

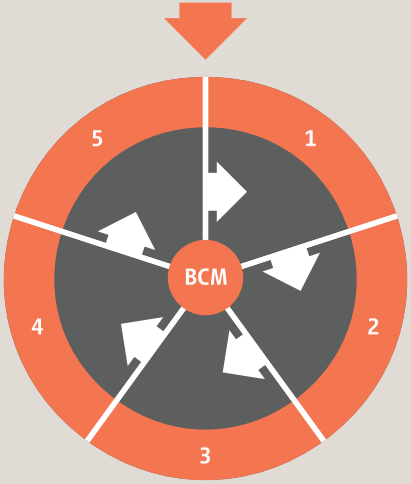
Hauptaufgaben Business Continuity Management

Initiierung des Notfallmanagements
Verantwortung, organisatorische Strukturen, Festlegung Methodik
Leitlinien zum Notfallmanagement, Einbindung Mitarbeiter

5. **Überprüfung und Verbesserung**
   Self-Assessment
   Revision
   Verbesserungsprozess

4. **Test und Übungen**
   Übungsarten
   Dokumente
   Durchführung

3. **Notfallbewältigung**
   Aufbau-/Ablauforganisation im Notfall
   Notfallkommunikation
   Notfallhandbuch



1. **BCM-Konzeption**
   Business Impact-Analyse
   Risikoanalyse Ist-Zustand
   Notfallstrategien

2. **Umsetzung des Notfallkonzeptes**
   Notfallkonzept erstellen
   Umsetzungsreihenfolge
   Aufgaben und Verantwortung
   Umsetzungsbegleitende Maßnahmen
   Kosten- und Aufwandsschätzung

Quelle: Eigene Darstellung.

1.
BCM-Impact Analyse

Bei der Einführung eines BCM oder dessen Evaluation sollte im ersten Schritt eine Zustandsanalyse potenzieller Gefahren von innen und von außen für ein Unternehmen und dessen Liegenschaften erfolgen. Zuerst steht die Identifizierung von Risiken und Schwachstellen in Form einer Business Impact Analyse (BIA) an.

BIA ist ein Prozess, bei dem die Auswirkungen eines potenziellen Vorfalls oder einer Störung auf das Geschäft eines Unternehmens bewertet werden. Ziel einer BIA ist es, kritische Geschäftsprozesse, Ressourcen und Systeme zu identifizieren, die für den kontinuierlichen Betrieb eines Unternehmens unerlässlich sind sowie potenzielle Risiken und deren Auswirkungen auf das Unternehmen zu bewerten. Dabei sollten auch Gefahren, die von der Umgebung auf den Standort einwirken können, verstärkt in den Fokus genommen werden.

Der BIA-Prozess besteht typischerweise aus den folgenden Schritten:

- Identifizierung von Geschäftsprozessen:
  Eine BIA beginnt mit der Identifizierung und Dokumentation der verschiedenen Geschäftsprozesse eines Unternehmens. Dies umfasst typischerweise die Identifizierung der wichtigsten Funktionen, Abteilungen, Systeme und Ressourcen.

- Bewertung von Auswirkungen:
  In diesem aufbauenden zweiten Schritt werden die Auswirkungen eines Vorfalls oder einer Störung auf die identifizierten Geschäftsprozesse bewertet. Dabei werden Faktoren wie finanzielle Verluste, Betriebsunterbrechungen, Kundenzufriedenheit, rechtliche Konsequenzen und Imageschäden berücksichtigt, die Unternehmen negativ beeinträchtigen können.

- Identifizierung von Abhängigkeiten:
  Es ist wichtig, die Abhängigkeiten zwischen verschiedenen Geschäftsprozessen, Systemen und Ressourcen zu verstehen. Eine BIA identifiziert diese Abhängigkeiten, um potenzielle Engpässe oder kritische Punkte zu erkennen, die sich negativ auf den Geschäftsbetrieb auswirken könnten.

- Festlegung von Wiederherstellungszielen:
  Basierend auf den Bewertungen der Auswirkungen werden Wiederherstellungsziele festgelegt, die angeben, wie schnell und in welchem Umfang die kritischen Geschäftsprozesse nach einem Vorfall oder einer Störung gänzlich (ggf. nur über Teilschritte) wiederhergestellt werden müssen.

- Entwicklung von Notfallplänen:
  Basierend auf den Ergebnissen der BIA werden Notfallpläne entwickelt, um auf potenzielle Störungen vorbereitet zu sein. Diese Pläne umfassen Maßnahmen zur Schadensbegrenzung, zur Wiederherstellung von Geschäftsprozessen und zur Kommunikation mit internen und externen Stakeholdern.

2.
Gefahren-Matrizes

Wie wahrscheinlich ist der Eintritt eines Schadensfalls? Welches sind seine Auswirkungen? Wie lässt sich die Schadenshöhe anschaulich und leicht verständlich beschreiben?

Ein weiteres Werkzeug, welches Bestandteil der BIA sein kann, ist die Visualisierung der Risiken auf das Geschäftsumfeld durch das Erstellen von Gefahren-Matrizes. Diese zeigen anschaulich und in leicht verständlicher graphischer Form die Betrachtung eines Risikos unter den Gesichtspunkten „Eintrittswahrscheinlichkeit" und „Schadenshöhe" bzw. „erwartbares Schadensausmaß". Diese Gefahren-Matrizes werden auch als Risiko-Matrizes oder Risikobewertungs-Matrizes bezeichnet und ermöglichen es, potenzielle Gefahren zu identifizieren, ihre Auswirkungen zu bewerten und so als Grundlage für die Ausplanung und Durchführung geeigneter Maßnahmen zur Risikominderung ergriffen zu werden.

Die Gefahren-Matrix besteht normalerweise aus zwei Hauptachsen: Der Achse der Eintrittswahrscheinlichkeit und der Achse der Auswirkungen. Jede Achse ist in verschiedene Stufen unterteilbar, die je nach Güte der Untersuchung und der Komplexität der Schadensgefahr einer Organisation variieren können.

Die Eintrittswahrscheinlichkeit gibt an, wie wahrscheinlich es ist, dass eine bestimmte Gefahr – auch wenn sie in einigen Fällen nur sehr abstrakt gesehen wird – eintritt.

Dies kann auf historischen Daten, statistischen Analysen oder Fachwissen basieren. Die Auswirkungen hingegen beschreiben das Ausmaß der Schäden oder Verluste, die eintreten können, wenn sich eine Gefahr realisiert. Dies umfasst Kategorien wie finanzielle Verluste, Reputationsverluste, Verletzungen oder den Verlust des Lebens von Mitarbeitern oder Kunden, Betriebsunterbrechungen und andere negative Konsequenzen.

Typische Kategorien können sein:

- Niedriges Risiko: Niedrige Eintrittswahrscheinlichkeit und geringe Auswirkungen.
- Mittleres Risiko: Moderate Eintrittswahrscheinlichkeit und moderate Auswirkungen.
- Hohes Risiko: Hohe Eintrittswahrscheinlichkeit und hohe Auswirkungen.
- Kritisches Risiko: Sehr hohe Eintrittswahrscheinlichkeit und katastrophale Auswirkungen.

Gefahren-Matrix

Risiko-Matrix		Schadensausmaß				
		niedrig	mittel	hoch	sehr hoch	kritisch
Eintrittswahrscheinlichkeit	kritisch	mittel	hoch	sehr hoch	sehr hoch	sehr hoch
	sehr häufig	mittel	hoch	hoch	sehr hoch	sehr hoch
	häufig	niedrig	mittel	hoch	hoch	sehr hoch
	mittel	niedrig	niedrig	mittel	mittel	hoch
	selten	niedrig	niedrig	niedrig	niedrig	mittel

Quelle: Eigene Darstellung.

Durch die Verwendung einer Gefahren-Matrix können Organisationen ihre Risiken priorisieren und gezielt grundlegende Maßnahmen zur Risikominderung planen. Gefahren mit hohen oder kritischen Risiken erfordern in der Regel umfangreichere Maßnahmen zur Verhütung, Vorbereitung oder Reaktion, während Gefahren mit niedrigen Risiken möglicherweise weniger dringend behandelt werden können.

Wichtig anzumerken ist, dass die Gefahren-Matrix nur ein Werkzeug, wenn auch ein wichtiges, zur Bewertung von Risiken ist und nicht alle Aspekte oder Feinheiten einer Gefahr berücksichtigen kann. Eine umfassende Risikobewertung erfordert oft weitere Analysemethoden und eine kontinuierliche Überwachung der Risikolandschaft.

3.
Varianten eines angepassten BCM

Obwohl für jedes Unternehmen ein gewisser individueller Ansatz der Untersuchung gewählt werden sollte und somit zu einem individuellen BCM führt, sind doch gewisse Arbeitsschritte immer als Grundlage für eine Umsetzung des BCM zu sehen. Im Folgenden werden die Schritte erläutert, die ein Unternehmen umsetzen sollte, um eine BCM-Strategie zu entwickeln.

Risikoanalyse

Eine umfassende Risikoanalyse ist integraler Bestandteil der Unternehmensführung. Sie hilft Unternehmen, ihre Widerstandsfähigkeit nachhaltig zu erhöhen. Folgende Auflistung zeigt die Varianten der Umsetzung und Abfolge eines BCM:

- Konzeption bzw. Entwicklung einer **unternehmensspezifischen BCM-Strategie**: Hierbei müssen alle möglichen Störungen berücksichtigt werden, die die Geschäftstätigkeit beeinträchtigen können, einschließlich Naturkatastrophen, Stromausfällen, Cyberangriffen, KRITIS-Gefahrenlagen und natürlich auch den Faktor menschlichen Versagens. Die Risikoanalyse sollte auch identifizieren, welche Geschäftsprozesse und -systeme am stärksten gefährdet sind.

- Bei der **Geschäftsprozessanalyse** sollten die kritischen Geschäftsprozesse identifiziert werden, die bei einer Störung unbedingt aufrechterhalten werden müssen, um das Geschäft am Laufen zu halten. Diese kritischen Prozesse sollten priorisiert werden, damit sich das Unternehmen auf die wichtigsten Aspekte konzentrieren kann.
- Mit der **Wiederherstellungsstrategie** wird festgelegt, wie das Unternehmen auf Störungen reagieren wird. Dies beinhaltet die Schritte, die das Unternehmen einleiten wird, um die Geschäftstätigkeit wiederherzustellen und eine Einschätzung, wie lang der Zeitraum zu definieren ist, bis dies umfassend geschieht. Die Wiederherstellungsstrategie sollte auch sicherstellen, dass alle notwendigen Ressourcen verfügbar sind, um die Wiederherstellung zu unterstützen.
- **Einführung und Umsetzung einer Notfallplanung**: Der Notfallplan sollte spezifische Schritte enthalten, die das Unternehmen umsetzen wird, um schnell und effektiv auf eine Störung zu reagieren. Dies beinhaltet die Kommunikation mit Mitarbeitern, Kunden und anderen wichtigen Stakeholdern.
- **Testen und Üben**: Eine BCM-Strategie ist nur so gut, wie ihre Umsetzung. Unternehmen sollten ihre Strategie regelmäßig testen und üben, um sicherzustellen, dass sie in der Lage sind, schnell und effektiv auf Störungen zu reagieren. Durch das Testen und Üben kann auch sichergestellt werden, dass alle notwendigen Ressourcen verfügbar und alle Mitarbeiter mit der Strategie vertraut sind.
- **Überprüfung und Aktualisierung**: Eine BCM-Strategie sollte regelmäßig überprüft und aktualisiert werden. So kann sichergestellt werden, dass sie den aktuellen Bedürfnissen des Unternehmens entspricht. Dies beinhaltet die Überprüfung der Risikoanalyse, der Wiederherstellungsstrategie und der Notfallplanung.

Spezifische Ausprägungen des BCM

Ein BCM kann je nach spezifischen Anforderungen und Gegebenheiten eines Unternehmens unterschiedlich ausgeprägt sein. Nachfolgend sind einige Aspekte aufgeführt, die zu Unterschieden in der Ausprägung eines BCM führen können:

- Der **Umfang des BCM** kann je nach Unternehmen variieren. Einige Unternehmen konzentrieren sich möglicherweise auf die Geschäftskontinuität für ihre wichtigsten kritischen Prozesse, während andere einen umfassenderen Ansatz verfolgen und auch unkritische Prozesse und Abteilungen einbeziehen.

- **Bewertung und Priorisierung** von Risiken können in verschiedenen Unternehmen unterschiedlich sein. Einige Unternehmen führen eine detaillierte Risikoanalyse durch, um die Auswirkungen potenzieller Störungen zu bewerten und ihre Ressourcen entsprechend auszurichten. Andere Unternehmen können eine weniger umfangreiche Risikobewertung durchführen und sich auf allgemeine Bedrohungen konzentrieren, da sie keine isolierten kritischen Geschäftsprozesse haben, die ein Alleinstellungsmerkmal am Markt bilden und durch deren Gefährdung der Fortbestand des Unternehmens gefährdet ist.

- Die Art der **Maßnahmen und Strategien**, die im Rahmen des BCM implementiert werden, kann je nach Unternehmen variieren. Dies kann die Implementierung von Redundanzlösungen, die Nutzung von Cloud-Diensten für die Datensicherung, die Entwicklung von alternativen Arbeitsplätzen oder die Umsetzung von Krisenkommunikationsplänen umfassen. Die spezifischen Maßnahmen hängen von den individuellen Bedürfnissen und Möglichkeiten des Unternehmens ab.

- Der Ansatz für die **Kommunikation und Schulung** in Bezug auf das BCM kann variieren. Einige Unternehmen legen Wert auf regelmäßige Schulungen und Bewusstseinsbildung für Mitarbeiter, um das Verständnis für Geschäftskontinuität zu fördern und die richtigen Verhaltensweisen in Notfällen zu etablieren. Andere Unternehmen konzentrieren sich stärker auf die interne Kommunikation und die Weitergabe von Informationen in Krisensituationen.

- Die Häufigkeit und Intensität der **Überprüfung und Verbesserung des BCM** kann von Unternehmen zu Unternehmen unterschiedlich sein. Einige Unternehmen führen regelmäßige Tests und Übungen durch, um die Wirksamkeit ihrer Pläne und Maßnahmen zu überprüfen und Schwachstellen zu identifizieren. Andere Unternehmen können eine weniger regelmäßige Überprüfung durchführen oder sich auf reaktive Anpassungen konzentrieren.

4.
Aufgabe und Funktion von Notfallplänen

In der Literatur findet man vielerlei Begriffe zum Themenfeld Notfallpläne. Oftmals werden sie auch als „Krisenhandbuch", als „Crisis Communication Manual" bzw. als „Emergency Action Folder" oder als „Handbuch Krisenkommunikation" bezeichnet. Nachfolgend werden relevante Begrifflichkeiten erläutert:

Notfallhandbuch

Das Notfallhandbuch umfasst alle Dokumente, die eine angemessene Reaktion auf Krisen und Notfälle unterstützen sollen. Im Hinblick auf die Fortführung der Geschäftsprozesse sind insbesondere das Notfallhandbuch und der Plan für Sofortmaßnahmen wichtig:

- Das Notfallhandbuch kann Dokumente einschließen, die thematisch eher dem allgemeinen Krisenmanagement einer Institution zugeordnet werden können.
- Der Plan für die Sofortmaßnahmen beschreibt die ersten Schritte beim Eintreten einer Krise oder eines Notfalls. Er enthält insbesondere auch solche Maßnahmen, mit denen die Sicherheit und Unversehrtheit beteiligter Personen geschützt werden sollen.

Die Notfallplanung soll kurz und übersichtlich sein. Allzu detaillierte Pläne sind für die sinnvolle Beherrschung eines Notfalls meist hinderlich. Es ist in der Regel unmöglich, jedes spezifische Unfall- und Schadensszenario in allen Einzelheiten im Detail zu planen. Deshalb muss die Organisation im Notfall flexibel und jederzeit angepasst reagieren können.

Die Bewältigung einer Notfallsituation erfolgt durch eine Vielzahl von Organisationseinheiten, von denen einige eine besondere Führungsposition einnehmen. Die erfolgreiche Bewältigung eines Notfalles hängt wesentlich vom menschlichen Verhalten ab. Bei der Planung sollen Verhalten und Handeln von Menschen unter extremer physischer und psychischer Belastung Berücksichtigung finden.

Der Prozess der Notfallplanung ist ein kontinuierlicher Vorgang. Es ist unerlässlich, einen einmal gefertigten Plan regelmäßig zu überprüfen und zu bearbeiten. Einerseits sollte die Planung ständig verfeinert und verbessert werden, andererseits unterliegen die Bedingungen der potenziellen Gefahren (im Raum) einem ständigen Wechsel. Dabei sind die Erkenntnisse aus regelmäßigen Schulungen und Ausbildungen sowie aus abgehaltenen Übungen zu berücksichtigen.

Krisenhandbuch

Das Krisenhandbuch ist das „ultimative Instrument" für eine verlässliche Krisenprävention, Krisenintervention und Krisenpostvention potenzieller und eingetretener kritischer Situationen auf ein bzw. in einem Unternehmen.

Daher darf das Krisenhandbuch nicht eine „08/15-Kopie" eines Musterwerks sein. Es muss spezifisch an die individuellen Bedürfnisse eines jeden Unternehmens angepasst werden. Es muss umfassend und darf dennoch kein zu komplexes Werk sein. Allen Beteiligten im Unternehmen muss es (nachweislich) bekannt gemacht sein. Es muss stets fortgeführt und damit aktuell sein (Fortführung mindestens zweimal bis viermal im Jahr). Es darf ferner die mit dem Krisenmanagement betrauten Verantwortlichen nicht in deren Handeln einengen und Kompetenzen beschneiden.

Im Detail bedeute dies, dass ein Notfallplan bzw. die Dienstanweisung zum Notfallhandeln des Unternehmens alle wichtigen aufbau- und ablauforganisatorischen Regelungen, die in einem Notfall zum Schutz der Mitarbeiter des Unternehmens mit ihren Standorten und Anlagen sowie der Öffentlichkeit zu beachten sind, enthalten sollte. Es legt zugleich die organisatorischen Maßnahmen des Notfallmanagements des Unternehmens fest.

Folgende Grundsätze bilden den Rahmen für das Notfallmanagement des Unternehmens:

Oberstes Gebot aller Notfallmaßnahmen sind der Schutz und die Rettung von Menschen. Daneben soll die Ausbreitung von Schäden (u. a. Umweltschutz) und die Zerstörung von Sachwerten verhindert werden. Die Reihenfolge der Prioritäten lautet:

1. Menschenschutz (Rettung von Personal und Bevölkerung)
2. Umweltschutz (Schadensminimierung)
3. Sachgüterschutz (Schadensminimierung)

Betreuung der Notfallpläne

Die Betreuung der Notfallpläne im Sinne eines Standards für ein Notfallmanagement sollte im Unternehmen im Vorfeld klar geregelt werden.

Die für den Notfallplan verantwortliche Stelle im Unternehmen kann durch Fachberater, z. B. von Vertretern eines technischen Gebäudebereiches oder technischer Anlagen, unterstützt werden. Sie wird insoweit als handlungsverantwortliche Stelle geführt. Diese hat sicherzustellen, dass die Regelungen des Notfallplans formell den Anforderungen genügen. Ihr obliegt die Aktualisierung des oben genannten Standards bei Änderungen und Ergänzungen sowie die interne Verteilung. Die Verantwortung für die inhaltliche Richtigkeit der Regelungen des Standards Notfallplan liegt bei allen Vorgesetzten der jeweiligen Abteilungen bzw. Fachsparten des Unternehmens. Möglicher Änderungsbedarf ist der handlungsverantwortlichen Stelle zu melden und wird von dieser weiterbearbeitet.

Neue und geänderte Kapitel, Abschnitte oder Unterabschnitte des „Notfallplans" werden durch die jeweiligen Leitungsebenen, z. B. Fachabteilungen und Sparten, freigegeben und durch die handbuchverantwortliche Stelle zur Verfügung gestellt. Der Bearbeitungs- und Revisionsstand ergibt sich aus dem Datum und dem Revisionsindex. Die betroffenen Bereiche und Abteilungen werden hausintern per E-Mail über relevante Änderungen im Handbuch informiert.

Jeder Handbuchinhaber, der das Handbuch in Papierform führt, ist verpflichtet, sein Handbuch auf aktuellem Stand zu halten, indem er die Änderungen in das Handbuch einpflegt. Bei Änderungen ist die jeweilige Richtlinie, Liste bzw. der entsprechende Passus auszutauschen.

Alle Vorgesetzten sind verpflichtet, sich und ihre Mitarbeiter mit den Inhalten des Notfallplans des Unternehmens vertraut zu machen und dessen Einhaltung sicherzustellen. Grundsätzlich sind geänderte wie neue Richtlinien zu behandeln. Die Geschäftsführung leitet, soweit erforderlich, die notwendigen Korrekturmaßnahmen ein.

III. Stabsarbeit im Unternehmen

1.
Aufbau und Funktion von Notfallstäben in Unternehmen

Der Notfallstab eines Unternehmens ist ein Verwaltungsstab, der durch die Unternehmens- bzw. Konzernleitung mit besonderen Kompetenzen ausgestattet ist, um die Schadenslagen möglichst kurzfristig zu managen. Der Notfallstab plant, koordiniert und überwacht die Notfallbewältigung im Sinne eines befristeten Krisenstabes. Während eines Notfalls bzw. einer Krisenlage ersetzt der Notfallstab die Führung der normalen Organisation. Die operativen Ebenen bleiben jedoch wie in der normalen Betriebsorganisation bestehen oder werden vorgehalten.

Zusammensetzung des Notfallstabs

Der Notfallstab eines Unternehmens sollte in Anlehnung an die Feuerwehrdienstvorschrift bzw. an militärische Stäbe hierarchisch aufgebaut sein. Zu seinen Bestandteilen zählen:

- **Leitung des Notfallstabs**

  Die Leitung und die jeweiligen Leiter der Funktionen des Notfallstabs nehmen deren festgelegte Funktionen in den Aufgabenverteilungen wahr.

  Die Leitungsebene des Notfallstabs koordiniert, entscheidet und leitet die notwendigen und zweckdienlichen Schutz- und Hilfsmaßnahmen ein. In der Umsetzung von Entscheidungen und Aufträgen bedient sie sich dabei der weiteren Organisationseinheiten des Notfallstabs. Die Leitung des Notfallstabs prüft, ob dessen Einberufung notwendig ist. Sie veranlasst die Alarmierung aller zuständigen Stellen und ruft diejenigen Mitglieder des Notfallstabs zusammen, die er im konkreten Fall benötigt.

  Zu den originären Aufgaben zählen insbesondere:

  → Einberufung und Leitung des Notfallstabs

  → Entscheidung über die Zusammensetzung des Notfallstabs

- Koordination und Entscheidung von Maßnahmen zur Krisenbewältigung und zum Krisenmanagement
- Information benachbarter Unternehmen
- Information und fachlicher Austausch mit den zuständigen Katastrophenschutzbehörden des Landkreises bzw. der kreisfreien Stadt (und der kreisangehörigen Stadt/Gemeinde), mit der Einsatzleitung der Feuerwehr sowie den zuständigen BOS der Gebietskörperschaft
- Teilnahme und verantwortliche Leitung von Medien-/Pressekonferenzen
- Ggf. Entscheidung zur Räumung von Anlagen und Gebäuden
- Kontakt zu anderen Bereichen innerhalb des Unternehmens sowie zur Geschäftsführung bzw. Konzernleitung
- Kontakt zu den Ermittlungsbehörden in Abstimmung mit den weiteren Vertretern des Notfallstabs sowie Rechtsberatern eines Unternehmens
- Kontakt zu den Medien und Information der Öffentlichkeit in Abstimmung mit den für die Medienarbeit und Bevölkerungsinformation zuständigen Vertretern im Notfallstab

Um jederzeit alle Bereiche besetzen zu können, werden jeweils zwei Verhinderungsvertreter bzw. Vertreter in der Folgeschicht (bei längeren Schadenslagen) benannt und ausgebildet.

- **Koordinierungsgruppe**

Zur Unterstützung der Leitungsebene des Notfallstabs und zur Koordination der Arbeiten der anderen Mitglieder des Notfallstabs wird eine Funktion „Koordinierungsgruppe" (KGS), häufig auch Lage/Versorgung/Koordination (LVK) genannt, gebildet. Die Funktion KGS/LVK mit Schwerpunkt Dokumentation der Lage und Prognose der weiteren Lageentwicklung kann – je nach Fall – mit mehreren Personen bzw. unterschiedlichen Organisationseinheiten besetzt werden.

Die Funktion KGS bzw. LVK hat zum einen Unterstützungsfunktion für die Leitungsebene des Notfallstabs. Zum anderen koordiniert die Leitung vom KGS/LVK-Bereich die Zusammenarbeit der einzelnen externen und internen Stellen des Notfallstabs miteinander. Zum Aufgabengebiet der KGS/LVK gehört auch

die Führung der Gesamtdokumentation im Sinne eines Einsatztagebuches (ETB).

Zu den Aufgaben dieser Funktion KGS/LVK zählen insbesondere:

- Beratung der Leitung des Notfallstabs
- Sicherstellen des ETBs
- Beschaffung und Auswertung notwendiger Informationen bzw. Erkenntnisse, Meldungen und Unterlagen zur Lagebeurteilung, zur Einschätzung der weiteren Lageentwicklung sowie zur Einleitung lösungsorientierter Maßnahmen der Stabsarbeit, auch im Kontakt mit externen Fachberatern
- Abstimmung mit allen Mitgliedern des Notfallstabs zur Vorbereitung von „Lagevorträgen zur Unterrichtung" (LVU)
- Erstellung von Entscheidungshilfen mit Handlungsoptionen in Form eines „Lagevortrages zur Vorbereitung einer Entscheidung" (LVE)
- Lagedarstellung und -meldung
- Kontaktstelle für externe Meldungen
- Sicherstellung der Versorgung bzw. der Logistik innerhalb des Notfallstabs sowie der Einsatzkräfte von Feuerwehr und den BOS
- Kontaktstelle zum Einsatzleiter vor Ort
- Kommunikation mit externen Hilfskräften und zum Verwaltungsstab vom Landkreis/ Kreis bzw. der kreisfreien Stadt (und/oder der kreisangehörigen Stadt/Gemeinde) und den BOS, ggf. durch Abstellung von Verbindungspersonen und Boten

- **Notfallsteuerung**

  Das Aufgabengebiet Notfallsteuerung innerhalb des Notfallstabs dient der fachlichen Beratung und Unterstützung des Leiters Notfallstab bzw. der KGS/ LVK. Diese Unterstützung bezieht sich auf die Analyse und Erfassung definierter Probleme. Die Funktion Notfallsteuerung als fachliche Beratung besteht aus mehreren Führungskräften der Sparten bzw. der Abteilungen des Unternehmens. Die fachliche Beratung erstreckt sich u. a. auf Belange des Arbeits- und Umweltschutzes, der Sicherheit und der Anlagentechnik. Zu den Aufgaben der

Funktion Notfallsteuerung zählen – abhängig von der jeweiligen Fachfunktion – insbesondere folgende:

- Beratung der Leitung des Notfallstabs und Zuarbeit für die KGS/LVK sowie andere Stabsfunktionen in spezifischen Fachfragen der betroffenen Sparten bzw. Abteilungen
- Mitwirken bei der Lagebeurteilung und der Festlegung von Maßnahmen
- Fachberatung in Fragen des Arbeits- und Umweltschutzes
- Fachberatung in Fragen der Anlagentechnik und -sicherheit
- Beiträge zur Rechtsberatung aus dem jeweiligen fachlichen Aufgabenfeld

Der Bereich Notfallsteuerung erhält jederzeit Unterstützung von weiteren Mitarbeitern (Leitungskräften) der Notfallsteuerung. Die Zusammensetzung des Notfallstabs, insbesondere die Funktion „Notfallsteuerung" in den Sparten bzw. Abteilungen des Unternehmens hängt von der Art des Notfalles ab. Die Entscheidung hierüber liegt beim jeweiligen Leiter des Notfallstabs.

- **Fachgruppenleiter**

  Bei größeren Unternehmen, insbesondere bei Konzernen, kann es auch sogenannte Einsatzleiter vor Ort im Sinne eines Fachgruppenleiters (FGL) geben, die nach Art des Notfalles spezifisch zu benennen sind. Dieser Funktionsträger veranlasst die Umsetzung der technischen und organisatorischen Maßnahmen, die der Notfallstab zur Beherrschung der Situation angeordnet hat.

  Zu den Aufgaben gehören im Detail:

  - Beratung der Notfallsteuerung und des Bereichs KGS/LVK
  - Veranlassung der vom Notfallstab beschlossenen Schutzmaßnahmen
  - Personaleinsatzplanung vor Ort für die unterstellten Hilfskräfte und Fachleute
  - Anweisung an Schicht, Technik, werkseigene Hilfskräfte und Pförtner
  - Koordination des Einsatzes werkseigener und externer Hilfsdienste
  - Einweisung externer Hilfsdienste in Besonderheiten der Notfallsituation

- Zusammenarbeit und fachliche Unterstützung mit Einsatzkräften der BOS am Schadensort in Abstimmung mit den Vorgaben und Empfehlungen des Verwaltungsstabs des Landkreises/Kreises bzw. der kreisfreien Stadt (ggf. des „Stabes außergewöhnliche Ereignisse" der kreisangehörigen Stadt/Gemeinde) sowie der Feuerwehrkräfte

- **Bereitstellung der Notfallkommunikation**

  Einen wichtigen, meist vernachlässigten und oftmals unterschätzten Teil im Aufbau des Notfallstabs nimmt die Bereitstellung der Notfallkommunikation ein, quasi eine Einheit für die „Information und Kommunikation" (IUK). Sie ist verantwortlich für die sichere und umfassende Kommunikation innerhalb des Notfallstabs, zu den Außenstellen der Einsatzleitung vor Ort sowie zum Verwaltungsstab der agierenden Gebietskörperschaft einschließlich der BOS. Dieses Aufgabengebiet ist ferner verantwortlich für das Planen und Halten des Informations- und Kommunikationseinsatzes.

  Im Detail sind folgende Aufgaben zu erfüllen:

  - Herstellung der Arbeitsbereitschaft in den Stabsräumen des Notfallstabs und Ausrüstung sowie Überprüfung der Kommunikationseinrichtungen
  - Feststellen des Ist-Zustandes der Führungs- und Fernmeldeorganisation
  - Ermitteln des Kräftebedarfs für den Kommunikationsbetrieb
  - Ermitteln des Materialbedarfs für den Kommunikationsbetrieb
  - Absprache der Führungsorganisation mit dem Leiter Notfallstab und dem Bereich KGS/LKV
  - Bereithalten von Kommunikationsmitteln im Stab (Druckerpatronen, Toner, Papier, Karten etc.)
  - Erarbeiten eines Kommunikationskonzeptes einschließlich Fernmeldeskizze
  - Feststellen der Einsatzmöglichkeiten von Funk- und Satellitentelefonen, ggf. von Kommunikationsverbindungen über Feldkabel, und andere drahtgebundene Netze
  - Dokumentation des Kommunikationsbetriebes sowie des Ein- und Ausgangs aller Meldungen in einer sogenannten Nachweisung

- Aufrechterhaltung der sicheren Kommunikation in allen Schadenslagen mit den Außenstellen des Notfallstabs (Einsatzleitung vor Ort) sowie zu den Behörden und Einrichtungen der Verwaltung, der Gebietskörperschaft über Telefonverbindungen, Faxverbindungen, Satellitentelefone, EDV-Kommunikation (Internet/ Intranet) und ggf. Funk
- Ggf. Anfordern oder Abstimmen von Sonderkanälen
- Bereitstellung mobiler Boten und deren Einsatz bei Ausfall der Kommunikationsmöglichkeiten
- Vorhalten von Papierkommunikationszetteln und Kartenmaterial für Botengänge

- **Informationshotline**

Ein weiterer Bestandteil des Notfallstabs ist der Bereich Informationshotline. Diese ist die Anlaufstelle für Anfragen von Behörden, Bürgern und Medienvertretern an den Notfallstab bzw. des Unternehmens in Schadenslagen. In Abstimmung mit dem Leiter Notfallstab bzw. dem Bereich KGS/LVK werden Informationen für Dritte erstellt und zugleich aus den Anfragen von außen die wichtigsten Themen zur Beratung im Notfallstab aufbereitet. Die Informationshotline stimmt sich unmittelbar mit dem Bereich „Presse- und Medienarbeit" ab und liefert entsprechend Textvorgaben.

Zu beachten ist, dass die „Informationshotline" immer als eine Reaktionsebene arbeitet. Dabei geht es um Informationen sowohl über vergangenes Geschehen, wie über die Absichten und Planungen beim Fortschreiten der Krisenbewältigung.

Zur Informationshotline zählen folgende Aufgaben:

- Nutzung sämtlicher Info-Kanäle
- Verifizierung der Inhalte eingegangener Meldungen, ggf. durch Rückfragen auch direkt bei den jeweiligen Absendern
- Permanente Abstimmung mit Bereich KGS/LVK und Presse- und Medienarbeit
- Abstimmung der Vorlagen aller geplanten „Ausgänge" beim Leiter des Stabes bzw. mit dem Bereich KGS/LVK
- Erstellen von Kurztexten in thematischen Agenden als Sprechvorlage

- **Presse- und Medienarbeit**

  Die Presse- und Medienarbeit sammelt Informationen aus dem Einsatz bzw. den Schadenslagen, wählt aus diesen aus und bereitet sie auf. Eine enge Kooperation mit allen anderen Aufgabegebieten im Notfallstab ist unerlässlich. Über die eigene Informationsgewinnung hinaus erfasst der Notfallstab die Presse- und Medienlage, dokumentiert sie und wertet sie aus.

  Dieses Aufgabengebiet setzt zu regelmäßigen Zeiten mit dem Leiter des Notfallstabs abgestimmte Informationen und Presse-/Medienmeldungen ab und hält mit den Presse- und Medienvertretern dauerhaft Kontakt. Dabei kommt der Beachtung von Social Media eine wichtige Rolle zu. Deren Beobachtung und Analyse ist ein weiteres Aufgabenfeld. Zu prüfen ist auch, ob es zu Fake News im Netz kommt, die umgehend korrigiert und richtiggestellt werden sollten.

  Dieses Aufgabengebiet steuert außerdem die Presse- und Medienarbeit mit anderen betroffenen Organisationen und Behörden, u. a. in Absprache mit anderen Behördensprechern, Polizeisprechern oder Pressesprechern der anderen BOS.

  Bei vom Leiter Notfallstab angeordneten Presse-/Medienkonferenzen organisiert dieser Bereich diese Veranstaltungen mit entsprechenden Tischvorlagen und schriftlichen Berichten. Während der Presse- und Medienkonferenz übernimmt die Leitung des Bereichs „Presse- und Medienarbeit" die Moderation der Sitzung und hält den weiteren Kontakt zu den Presse- und Medienvertretern.

  Die Presse- und Medienarbeit sollte dabei stets die Ziele der Krisenkommunikation beachten:

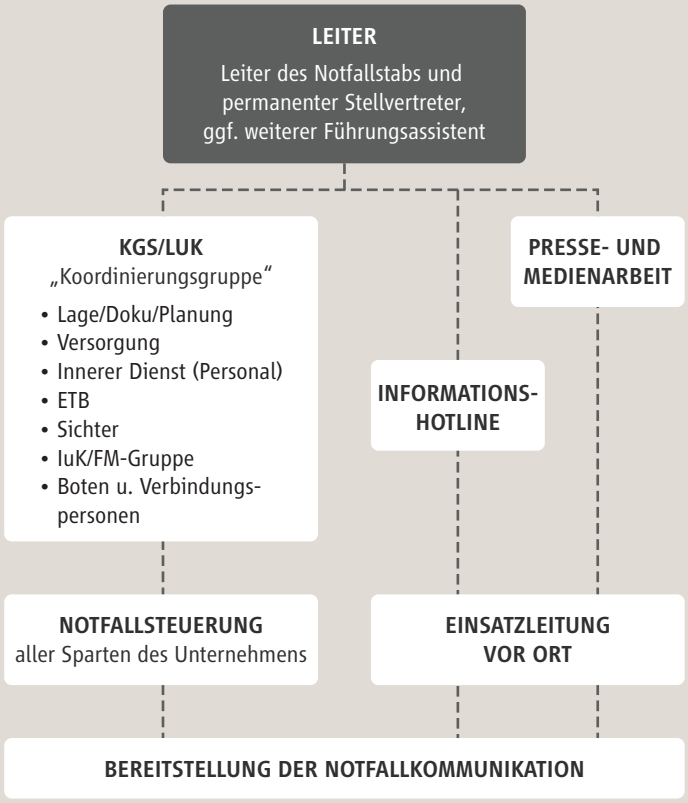
  - Faire Berichterstattung erzeugen
  - Berichterstattungszeiträume verkürzen
  - Spekulationsspielräume einschränken
  - Emotionen dämpfen
  - Nebenthemen ausklammern

  Bei Notfällen mit Toten und Schwerverletzten und bei behördlichen Ermittlungen im Zusammenhang mit einem Notfall sind stets die Geschäftsführer einzubeziehen sowie interner und gegebenenfalls externer Rechtsrat einzuholen.

Im Bedarfsfall kann der Notfallstab durch externe Stellen, z. B. Fachberater und Verbindungsperson zur Feuerwehr, der Stadt oder zum THW in „Funktion“ Beratung verstärkt werden.

Der Notfallstab setzt sich gemäß Schaubild wie aufgeführt zusammen:

Muster eines Notfallstabs



Quelle: Eigene Darstellung.

Weitere Unterstützung der Vertreter des Notfallstabs kann – je nach Ausmaß der Schadenslage – mit Verbindungspersonen und Boten erfolgen.

Arbeitsort und Arbeitsbeginn des Notfallstabs

Der Notfallstab kommt in speziell dafür ausgestatteten Räumen zusammen, in denen die angemessene Informationsversorgung gewährleistet ist. Die einzelnen Elemente des Notfallstabs ermöglichen eine ruhige und effiziente Arbeit der Stabsmitglieder. Hier laufen alle Informationen zusammen. Von hier aus werden alle erforderlichen Maßnahmen gesteuert. Sie sind in einem gesicherten Bereich des Betriebsgeländes eingerichtet. Die Stabsräume können während des Normalbetriebes zu anderweitigen Zwecken genutzt werden. Dabei ist sicherzustellen, dass die Einsatzbereitschaft der Stabsräume für den Notfall nicht beeinträchtigt wird.

Ausweich- und Ersatzräume

Unter Berücksichtigung der örtlichen Gegebenheiten und möglicher Notfallszenarien am Standort ist durch den zuständigen Notfallstab frühzeitig zu ermitteln, ob für den Ausfall des Notfallstabsraums ein oder mehrere Ausweichräume außerhalb des Betriebsgeländes einzurichten sind. Sollte das Gebäude des Notfallstabsraums aufgrund einer dringend erforderlichen Evakuierungsmaßnahme (z. B. Gefahrstoffwolke, Bombendrohung etc.) als Stabsraum nicht mehr nutzbar sein, verlegt der Notfallstab umgehend in die vorgeplanten Ausweich- und Ersatzräume. Die Ausstattung des Ausweichraumes muss nicht im vollen Umfang den Anforderungen des eigentlichen Notfallstabsraumes entsprechen. Es müssen jedoch zumindest ausreichende Kommunikationsmöglichkeiten bestehen und ein Zugriff auf betriebsinterne Daten möglich sein.

2.
Regeln der Stabsarbeit

Nach Ausruf des Notfalls obliegen dem Notfallstab folgende grundsätzliche Aufgaben. Einem Dreiklang in der klassischen Stabsarbeit folgend sind dies: die Lagefeststellung sowie die anschließende Lagebeurteilung mit dem daraus ableitbaren Entschluss bzw. den Folgeentscheidungen.

Im Detail beinhaltet dies:

- Vorbereitung auf außergewöhnliche Ereignisse mit entsprechender personeller und materieller Ausstattung, um stets und für längere Zeiten einsatzfähig zu sein
- Die erforderlichen Notfallunterlagen zu erstellen und aktuell zu halten
- Im Notfall die Lage zuverlässig zu beurteilen und entsprechende Sofortmaßnahmen zur Abwehr oder Bekämpfung zu stellen
- Bis zur Schadensbehebung ggf. Ausweichmöglichkeiten festzulegen sowie den die Anlagen so rasch wie möglich wieder dem Normalbetrieb zuzuführen
- Die Ergebnisse der eigenen Handlungen auszuwerten und daraus Optimierungspotential und weitere Handlungsoptionen abzuleiten

Im Folgenden werden die Schritte der Stabsarbeit im Notfallstab aufgeführt:

Lagefeststellung (Lagebildgewinnung einer Schadenslage)

Zunächst ist es erforderlich, sich ein möglichst genaues Lagebild vom Schadensumfang und -verlauf zu verschaffen. Die Lagefeststellung schafft die Voraussetzungen für ein sinnvolles Beurteilen, Planen, Umsetzen sowie die zielorientierte Überwachung der Realisierung. Bei der Lagefeststellung geht man von vorhandenen Informationen aus, z. B. von Meldungen, Informationen oder persönlichen Erkenntnissen.

Als wichtige Unterstützungsfunktion für den Leiter des Notfallstabs veranlasst der Bereich LVK die Erstellung und Zusammenfassung des Lagebildes der einzelnen Organisationseinheiten und koordiniert die Zusammenführung in ein aktuelles Lagebild. Der Bereich LVK ist dabei zuständig für die Datenermittlung, deren Gesamtdokumentation in einer Lagekarte (Papierversion, ggf. EDV-Geographisches-Informations-System) sowie in Abbildungen (Tabellen, Zeitstrahl und andere Graphiken) auf Basis vorhandener Gefahrenabwehrpläne und des Notfallprotokolls des Aufgabengebiets ETB erfolgt.

Lagebeurteilung

Die Beurteilung umfasst folgende Aspekte:

- Gefahren- und Schadenslage
- Lage der eigenen Kräfte (Unternehmen, Teilorganisationen)

- Abwägung der Möglichkeiten zur Bewältigung/Deeskalation
- Erfassen der Rahmenbedingungen für den Einsatz

Nachdem jedes Mitglied des Notfallstabs die Situation hinsichtlich seines Aufgabenbereichs eigenständig beurteilt hat, wird in Zusammenarbeit mit dem Bereich LVK ein Gesamtlagebild mit Handlungsoptionen für die Leitungsebene des Notfallstabs erstellt. Dieser Vortrag wird in Form eines LVU bzw. dem LVE gereicht. Der Bereich LVK trägt in einem knappen und klar strukturierten LVE des verantwortlichen Leiters des Notfallstabs im Rahmen der Notfallbesprechungen die speziellen Problemstellungen und mögliche Lösungsansätze vor. Dabei ist wichtig, dass auch Lösungsmöglichkeiten aufgezeigt werden, die über die normalen betrieblichen Entscheidungsspielräume hinausgehen. Hierbei sollten bereits im Rahmen des Risikomanagements geplante Maßnahmen einbezogen werden.

Entschlussfassung

Die Leitung des Notfallstabs entscheidet nach der Lagebeurteilung mit dem Bereich LVK, ggf. bei schwierigen Lagen ergänzt um einzelne Mitglieder des Notfallstabs, als alleinig Verantwortlicher über die weitere Vorgehensweise.

Dafür gelten folgende Regeln:

- Entscheidungen schnell und trotzdem fundiert treffen
- Agieren statt reagieren – die Initiative ergreifen und behalten
- Handlungsfreiheit schaffen durch Bildung von Reserven (z. B. zusätzlich Personalkapazitäten) oder Alternativen – ggf. Alternativen parallel verfolgen
- Begrenzte Ressourcen gezielt dort einsetzen, wo sie für die Aufgaben optimiert verwendet werden können
- Berücksichtigung und Sicherstellung der Arbeitsfähigkeit der in- und externen Einsatzkräfte und Ressourcen durch Einrichten von Sammel- und Informationsstellen. Dabei ist zu prüfen, ob Sammel- und Informationsstellen für in- und externe Einsatzkräfte und Ressourcen erforderlich sind, wo diese eingerichtet und mit welchem internen Mitarbeiter sie besetzt werden können

Alle Entscheidungen werden vom ETB stets schriftlich im Einsatzkalender Notfallstab festgehalten. Die Mitglieder des Notfallstabs liefern an das ETB hierzu in kurzer und prägnanter Form schriftlich ihre Fachbeiträge und Entscheidungsgrundlagen.

Umsetzung der Entscheidungen und Auftragserteilung

Die Leitung des Notfallstabs erteilt auf der Grundlage ihrer Entscheidungen und in Absprache mit dem Bereich LVK entsprechende Aufträge. Diese Arbeitsaufträge (Anweisungen) sind klar und widerspruchsfrei zu formulieren, übersichtlich zu gestalten und müssen erfüllbar sein. Sie sind bindend. Die Aufträge sind zu protokollieren und durch die Notfallsteuerer an die Einsatzkräfte vor Ort weiterzugeben.

Überwachung und Kontrolle

Zur Sicherstellung der Auftragsausführung ist diese zu kontrollieren und zu überwachen. Dabei ist jeder Mitarbeiter des Notfallstabs für bestimmte Teilaufgaben selbst und dauerhaft zuständig. Der Bereich KGS/LVK koordiniert die Dokumentation der einzelnen internen und externen Stellen während der Krisenlage und stellt eine Evaluierung der Stabsarbeit jederzeit sicher.

Beendigung der Arbeit des Notfallstabs

Die Leitung des Notfallstabs entscheidet je nach Notfall und bei größeren Katastrophenlagen in Abstimmung mit der Katastrophenschutzbehörde, wann das Notfallmanagement beendet werden kann und wie der Übergang zum Normalbetrieb im Einzelfall ausgestaltet wird. Auch wenn der Notfall als beendet erklärt worden ist, kann die Arbeit mit administrativ-organisatorischen Maßnahmen für Teile des Notfallstabs noch weitergehen, bis der Stabsleiter die Beendigung anordnet. Diese ist entsprechend zu dokumentieren.

Auswertung des Krisenablaufs und Weiterentwicklung des Notfallkonzepts

Spätestens bei Rückkehr zum Normalbetrieb ist eine Analyse der Eignung und Funktionsfähigkeit der betrieblichen Strukturen und Regelungen zu diesem Notfall-

konzept durchzuführen. Der Bereich KGS/LVK erstellt auf Basis seiner durchgeführten Evaluierungen eine Ergebniszusammenstellung und -auswertung. Die im Rahmen der Analyse gewonnenen Erkenntnisse sind in das Notfallkonzept einzuarbeiten.

3. Ausbildung und Übung

Die Mitarbeiter des Notfallstabs sollten in regelmäßigen Abständen über das Notfallmanagement des Unternehmens informiert werden. Dabei sollen den Mitarbeitern insbesondere folgende Kenntnisse vermittelt werden:

- Aufnahme und Meldung von Notfällen
- Handhabung des einschlägigen Betriebs- und Organisationshandbuchs
- Notfallrelevante Aufbau- und Ablauforganisation
- Einbindung des Unternehmens und ggf. weiterer Zweigstellen (Niederlassungen) mit ihren Standorten in die externe Notfall- und Katastrophenschutzplanung des Landkreises/Kreises bzw. der kreisfreien Stadt

Für die Durchführung entsprechender Informationsveranstaltungen, z. B. in Form von halb- oder ganztägigen Workshops, sind die Notfallverantwortlichen zuständig. Sie können abteilungs- und/oder bereichsbezogen in Form von Vorträgen, Lehrgesprächen, Diskussionen oder auch im Rahmen von E-Learning-Veranstaltungen durchgeführt werden. Grundlage für die Information der Mitarbeiter bildet der Notfallplan des Unternehmens.

Schulungen der Beteiligten in Seminaren

Auf allen Ebenen des Unternehmens sollte eine zweckorientierte Schulung der in das Notfallmanagement eingebundenen Mitarbeiter erfolgen. Die Schulung ist im Notfall an den jeweiligen Anforderungen an die Mitarbeiter auszurichten und hat die notfallspezifischen Aufgabenbereiche innerhalb der verschiedenen Ebenen zu berücksichtigen. Im Rahmen der Schulung sollen den eingebundenen Mitarbeitern grundlegende Kenntnisse vermittelt werden:

- Notfallmanagementsystem des Unternehmens
- Spezifische Notfälle/Schadenslagen im Bereich der Gebietskörperschaft (Landkreis/Kreis bzw. Stadt) und den angrenzenden Städten/Gemeinden und die einschlägigen Gefahrenabwehrpläne und Sonderschutzpläne
- Die Aufgabenverteilung innerhalb des Notfallstabs
- Grundlagen der Stabsarbeit und vertiefende Stabsarbeit
- Nachweissichere Dokumentation und Kommunikation innerhalb des Notfallstabs und mit externen Fachberatern
- Kooperation von Notfallstab zu externen Einsatzkräften und Vertretern des Verwaltungsstabes der zuständigen Gebietskörperschaft
- Kooperation mit den BOS und deren Einsatz- und Leistungsfähigkeiten bei spezifischen Schadenslagen/Notfällen
- Rettungsmaßnahmen im Brandschutz
- Grundlagen der Bergung von Personen
- Grundlagen der Ersten Hilfe
- Sicherheitsbestimmungen
- Verhalten bei Bombendrohungen
- Führungsverhalten in Notfallsituation
- Bevölkerungs-/Kundeninformation und die Medienarbeit in Notfällen bzw. im Katastrophenfall

Die Schulungen dienen auch der Überprüfung der Zweckmäßigkeit organisatorischer und führungstechnischer Maßnahmen des Notfallmanagements. Sie sind im Rahmen des Erfahrungsrückflusses für eine Optimierung des Notfallplanmanagements zu berücksichtigen.

Durchführung von Notfallübungen

Zur Vorbereitung auf eventuelle Notfälle sind vom Unternehmen aus in regelmäßigen Abständen Notfallübungen in abgestufter Form durchzuführen. Zweck der Notfallübung ist es,

- die Mitarbeiter in Notfallmaßnahmen zu unterweisen,
- Schwachstellen im Notfallmanagement zu erkennen und zu beseitigen und
- das Zusammenwirken mit sowie zwischen internen und externen Stellen zu überprüfen.

Dabei ist eine konkrete Notfallsituation vorzugeben, deren Bewältigung in einer angemessenen Zeit (Dauer der Übung z. B. fünf bis sieben Stunden) geübt wird.

Die während der Übung geführte Dokumentation bzw. das ETB ist vom zuständigen Leiter des Notfallstabs in Zusammenarbeit mit dem Bereich KGS/LKV sowie mit den Notfallverantwortlichen und ggf. weiteren Fachstellen auszuwerten. Soweit erforderlich, ist die Dienstanweisung Notfallplan des Unternehmens auf der Grundlage der in der Übung gewonnenen Erkenntnisse zu aktualisieren. Technische Korrektur- bzw. Optimierungsmaßnahmen sind von den zuständigen Fachteams durchzuführen. Das Ergebnis der Übung ist den Beteiligten mitzuteilen und mit ihnen durchzusprechen.

Stufenkonzept Notfallübungen

Übungen für den Notfallstab des Unternehmens sollten gemäß des Stufenkonzepts erfolgen und inhaltlich abgestimmt aufeinander aufbauen:

Stufe 1: Probealarm für alle Mitarbeiter eines Standortes

Der Probealarm dient der Überprüfung der Funktionstüchtigkeit der Alarmierungsanlagen. Alle Mitarbeiter des Standortes sammeln sich an den ausgewählten Sammelstellen, soweit dies den sicheren Betrieb des Unternehmens nicht beeinträchtigt. Verantwortlich für Planung und Durchführung des Probealarms ist der Standortverantwortliche. Eine solche Alarmierung sollte mindestens einmal im Jahr durchgeführt werden.

Stufe 2: Probealarm für alle Mitglieder des Notfallstabs

Diese Alarmierungsübung dient der Überprüfung der Funktionstüchtigkeit der Alarmierungsanlagen und zeigt auf, bis wann die Mitglieder des Notfallstabs in den Stabsräumen eintreffen und ihre Arbeit aufnehmen können.

Solche Alarmierungsübungen sollten auch außerhalb der Kernarbeitszeit, etwa in

den Abend-/Nachtstunden sowie an Wochenenden erfolgen, um die Bereitschaft zum rechtzeitigen Eintreffen an solchen Verhinderungszeiten aufzuzeigen. Verantwortlich für die Planung und Durchführung des Probealarms ist der Leiter des Notfallstabs bzw. der zeitlich anwesende Vertreter. Eine solche Alarmierung sollte mindestens einmal im Jahr durchgeführt werden.

Stufe 3: Plan-/Ausbildungsübung für alle Mitglieder des Notfallstabs

Diese Form der Übung kann mit echter Alarmierung oder mit einer rechtzeitigen Ankündigung des Übungstages durchgeführt werden. Die Plan-/Ausbildungsübung ist als eine angeleitete, in mehrere Übungsabschnitte gegliederte Übung ausgelegt, die insbesondere in der Funktion im Notfallstab noch jungen Mitgliedern die in den einzelnen Phasen erwartbaren und ausgeführten Maßnahmen im Handeln des Notfallstabs durch Vertreter der Übungsleitung erläutert. Im Detail werden folgende Übungsinhalte festgelegt:

- Einberufung des Notfallstabs
- Informationsweitergabe gemäß der jeweiligen Stabsfunktionen
- Information der benötigten externen Stellen
- Übung der technischen Funktionen in den Stabsräumen
- Festlegung und Koordination der Maßnahmen zur Notfallbewältigung
- Kontakt und Abstimmung mit der Einsatzleitung (verkörpert durch die Übungsleitung)
- Externe Unterstützung durch Fachkräfte
- Ggf. kann eine simulierte Medien-/Pressekonferenz zum Ende der Übung eingeplant werden, bei der Vertreter der Übungsleitung die Pressevertreter darstellen und ausgewählte Vertreter des Notfallstabs (Leiter des Notfallstabs und der Presse-/Medienbeauftragte sowie weiterer Fachleute) sich den kritischen Fragen der Medien-/Pressevertreter stellen.

Die Übung sollte nicht von Mitgliedern des Notfallstabs vorbereitet und ausgeplant werden. Falls möglich, sind unabhängige Fachgutachter und Experten in Funktion als Übungsausplaner mit der Anlegung und Durchführung der Übung zu betrauen. Es ist anzustreben, dass die Arbeit des Notfallstabs anhand nachvollziehbarer Kriterien überprüft und zertifiziert wird, um Vorgaben für weitere Übungen zur Weiterentwick-

lung und Optimierung der Stabsarbeit des Notfallstabs zu bekommen. Die Plan-/Ausbildungsübung kann an einem Werktag während der Kernarbeitszeit stattfinden, z. B. mit Alarmierung ab 6:00 Uhr und Beginn der Stabsarbeit ab ca. 7:00 Uhr. Die Dauer sollte ca. fünf bis sieben Stunden betragen. Verantwortlich für die Planung und Durchführung der Übung ist ein Unternehmensvertreter der Führungsetage. Eine solche Übung sollte mindestens einmal im Jahr durchgeführt werden.

Stufe 4: Stabsübung für die Mitglieder des Notfallstabs mit einem Schichtwechsel

Diese Form der Übung kann beim ersten Mal mit einer rechtzeitigen Ankündigung des Übungstags durchgeführt werden. In späteren Folgen kann sie auch aus einer Alarmierungsübung hervorgehen. Die Stabübung ist eine fortlaufende Übung, die aufbauend auf den Erkenntnissen vorangegangener Plan-/Ausbildungsübungen die Mitglieder des Notfallstabs mit einer komplexeren Notfalllage/Krisenlage konfrontiert.

Im Detail werden folgende Übungsinhalte festgelegt:

- Einberufung des Notfallstabs
- Informationsweitergabe gemäß der jeweiligen Stabsfunktionen
- Information der benötigten externen Stellen
- Übung der technischen Funktionen in den Stabsräumen
- Festlegung und Koordination der Maßnahmen zur Notfallbewältigung
- Kontakt und Abstimmung mit der Einsatzleitung (verkörpert durch die Übungsleitung)
- Externe Unterstützung durch Fachkräfte, ggf. Einbindung und Absprache mit Vertretern der zuständigen Katastrophenschutzbehörde der Gebietskörperschaft und weiterer BOS
- Simulierte Medien-/Pressekonferenz im Verlauf der Übung, bei der Vertreter der Übungsleitung die Pressevertreter darstellen und sich ausgewählte Vertreter des Notfallstabs den kritischen Fragen der Medien-/Pressevertreter stellen
- Durchführung eines Schichtwechsels mit Übergabe der Aufgaben-/Funktionstätigkeiten aller Vertreter vom Notfallstab an deren weitere Vertreter in der Funktion

Es ist anzustreben, dass die Arbeit des Notfallstabs anhand nachvollziehbarer Kriterien überprüft und zertifiziert wird, um Vorgaben für weitere Übungen zur

Weiterentwicklung und Optimierung der Arbeit des Notfallstabs zu erlangen.

Die Stabsübung kann an einem Werktag während der Kernarbeitszeit stattfinden, z. B. mit Alarmierung ab 6:00 Uhr und Beginn der Stabsarbeit ab ca. 7:00 Uhr. Die Dauer sollte ca. sieben bis zehn Stunden betragen und einen Schichtwechsel umfassen. Verantwortlich für die Planung und Durchführung der Übung ist ein Vertreter der Unternehmensführung. Eine solche Übung sollte mindestens aller zwei Jahre im Folgejahr zu einer Plan-/Ausbildungsübung stattfinden. Eine frühzeitige Abstimmung mit externen Kräften der zuständigen Katastrophenschutzbehörde von der Gebietskörperschaft, der Feuerwehr sowie den BOS ist zu gewährleisten.

Stufe 5: Stabsübung (Vollübung) für die Mitglieder des Notfallstabs mit Schichtwechsel außerhalb der Kernarbeitszeit

Aufbauend auf den Ergebnissen der zuvor durchgeführten Plan-/Ausbildungsübung und der Stabsübung kann für einen erfahrenen Notfallstab eine Stabsübung als Vollübung außerhalb der Kernarbeitszeit geplant werden. Diese Übung kann entweder am späten Nachmittag oder in den frühen Morgenstunden beginnen, um so dem Stab zu verdeutlichen, dass sich bestimme Notlagen/Krisen nicht immer an einer tariflich festgelegten Arbeitszeit ausrichten und auch in den Abend- und Nachtstunden bzw. am Wochenende oder gar an Feiertagen eintreten können. Der Ablauf bzw. die Inhalte dieser Form der Stabsübung sind ähnlich der Stufe 4, können aber in Abstimmung mit der zuständigen Katastrophenschutzbehörde der Gebietskörperschaft auf eine komplexere und langanhaltende Krisenlage ausgelegt werden, die besonders das Zusammenspiel mit dem Verwaltungsstab der Gebietskörperschaft und den beteiligten BOS trainiert.

Auch hier ist es anzustreben, dass die Arbeit des Notfallstabs anhand nachvollziehbarer Kriterien überprüft und zertifiziert wird, um Vorgaben für weitere Übungen zur Weiterentwicklung und Optimierung der Stabsarbeit des Notfallstabs zu erhalten. Die Dauer sollte ca. acht bis zwölf Stunden betragen und mindestens einen Schichtwechsel beinhalten. Verantwortlich für die Planung und Durchführung der Übung ist ein Vertreter der Unternehmensleitung. Eine solche Übung sollte mindestens aller vier Jahre im Folgejahr einer Stabsrahmenübung stattfinden. Eine frühzeitige Abstimmung mit externen Kräften der zuständigen Katastrophenschutzbehörde der Gebietskörperschaft sowie den BOS ist zu gewährleisten.

IV. Zivil-Militärische Zusammenarbeit

Unternehmen und ihre Rolle im Operationsplan Deutschland

Seit 2024 stellt sich vermehrt die Frage, wie mit einem vernünftigen Einsatz von Finanzmitteln der Zivilschutz Deutschlands neu belebt und wieder hergestellt werden kann, um die Bevölkerung im Falle eines Krieges weitgehend vor Angriffen zu schützen.

Dazu hat das Bundesverteidigungsministerium (BMVg) seit 2024 einen sogenannten Operationsplan Deutschland (OPLAN DEU) in Planung.

Der OPLAN DEU regelt die Verteidigung Deutschlands, liefert Grundlagen zu Einsätzen der Bundeswehr (BW) im Inland und verweist gleichzeitig auf den Unterstützungsbedarf der privaten Wirtschaft.

Sein Ziel ist der Schutz Deutschlands, der Bevölkerung, von Unternehmen sowie KRITIS-Einrichtungen bei Bedrohungen im Rahmen von Artikel 87a GG (Verteidigungsfall). Zugleich bildet er die Schnittstelle zur Zivil-Militärischen Zusammenarbeit (ZMZ), da zivile Infrastruktur und Behörden massiv einbezogen werden müssen.

Der OPLAN DEU integriert Unternehmen indirekt über ihre Rolle in der gesamten zivil-militärischen Verteidigungsarchitektur. Dabei sind KRITIS-Betreiber und rüstungsrelevante Unternehmen (einschließlich deren Zulieferfirmen) besonders gefordert, da deren Funktionsfähigkeit als Teil der Verteidigungsfähigkeit Deutschlands betrachtet wird.

Jedes Unternehmen (auch außerhalb KRITIS) sollte prüfen:

1. Welche Leistungen sind für Gesellschaft/Militär im Verteidigungsfall relevant?
2. Welche Abhängigkeiten bestehen (z. B. Lieferketten)?
3. Wie wird die Notfallplanung an LV/BV-Szenarien angepasst?

Zu den wichtigsten Punkten zur Bedeutung von Zivilschutz für Unternehmen zählen:

Sicherung der Geschäftskontinuität

- Katastrophen wie Stromausfälle, Hochwasser oder Cyberangriffe können den Betrieb lahmlegen.
- Unternehmen, die präventiv Notfallpläne (BCM) und Schutzmaßnahmen entwickeln, können Ausfallzeiten minimieren und ihre Wettbewerbsfähigkeit sichern.

Schutz von Mitarbeitern

- Zivilschutz zielt auch auf die Sicherheit von Menschen ab. Unternehmen tragen Verantwortung für den Schutz ihrer Mitarbeiter im Ernstfall (Evakuierungspläne, Erste-Hilfe, Notunterkünfte).
- Dazu gehören auch psychologische Unterstützung und klare Kommunikationswege in Krisensituationen.

Abhängigkeit von kritischer Infrastruktur

- Unternehmen sind auf Energie, Wasser, Telekommunikation, Transport und IT angewiesen.
- Fällt diese Infrastruktur durch eine Krise aus, können selbst robuste Betriebe zum Stillstand kommen. Deshalb müssen Firmen eigene Notfallreserven (z. B. Notstrom, redundante Systeme, alternative Lieferketten) vorsehen.

Rechtliche und regulatorische Anforderungen

- In bestimmten Branchen (KRITIS-Sektoren von Gesundheitswesen, Energieversorgung, Telekommunikation, Finanzwesen) bestehen gesetzliche Verpflichtungen zum Schutz vor Krisen.
- Aber auch kleinere Unternehmen sollten sich an Standards wie ISO 22301 (Business Continuity Management) orientieren.

Reputations- und Vertrauensfaktor

- Kunden, Investoren und Partner erwarten, dass Unternehmen auf Krisen vorbereitet sind.
- Wer im Ernstfall handlungsfähig bleibt und soziale Verantwortung zeigt, stärkt sein Image und die Kundenbindung.

Beitrag zum gesamtgesellschaftlichen Schutz

- Unternehmen sind Teil der Zivilgesellschaft und tragen zur Resilienz der Region bei.
- Beispiele: Bereitstellung von Ressourcen (z. B. Maschinen, Fahrzeuge, Personal im Katastrophenfall), Kooperation mit Behörden und Hilfsorganisationen, Unterstützung bei Evakuierungen.

Zusammengefasst bedeutet dies: Zivilschutz ist nicht nur Aufgabe von Staat und Behörden, sondern betrifft Unternehmen direkt. Wer Zivilschutzaspekte in seine Notfall- und Krisenplanung integriert, schützt Mitarbeiter, sichert die eigene Existenz und trägt gleichzeitig zur Stabilität der gesamten Gesellschaft bei.

Unternehmen sollten diese neuen Inhalte in ihren Gefahrenabwehr-/Notfallplänen sowie in das Krisen-/BCM-management aufnehmen und dies regelmäßig neben Grundlagenausbildungen auch üben. Hierzu zählt der permanente Kontakt und der fachliche Austausch mit den zuständigen Behörden (Krisen-/Verwaltungsstäben) der jeweiligen Gebietskörperschaften.

Da die Rolle von Unternehmen im Kontext OPLAN DEU noch relativ neu und auch geheim ist, bedürfen sie einer vertiefenden Betrachtung. Da moderne Kriegsführung stark auf die zivile Infrastruktur zielt, kommt Unternehmen eine wesentliche Rolle zu.

Aufrechterhaltung von Versorgung und Dienstleistungen

- Energie, Wasser, Telekommunikation, IT-Dienste, Gesundheitswesen, Transport/Logistik, Finanzwesen sind unmittelbare Voraussetzung für militärische Operationen und die Zivilbevölkerung.
- Unternehmen müssen ihre Resilienzpläne (BCM, Notfallmanagement, Redundanzen) so ausrichten, dass sie auch in einer LV/BV-Lage funktionieren.

Einbindung in gesamtstaatliche Planung

- Unternehmen sind Teil der Gesamtverteidigung nach Art. 87a GG i. V. m. Sicherheitsvorsorgegesetzen.
- OPLAN DEU sieht vor, dass die Bundeswehr und NATO-Streitkräfte auf zivile Infrastruktur zurückgreifen müssen (z. B. Häfen, Bahnhöfe, Flughäfen, Straßen, Energieversorgung).
- Unternehmen können in die Planung über ZMZ-Strukturen (z. B. über Krisenstäbe von Kommunen, Landkreisen, Ländern) eingebunden werden.

Mögliche Pflichten im Verteidigungsfall

- Bereitstellung von Ressourcen (z. B. Logistik, Transportkapazitäten [LKW, Container etc.], medizinisches Material).

- Arbeitsschutz/Arbeitskräftebereitstellung (historisch über Arbeitssicherstellungsgesetz vorgesehen) könnte wieder aktiviert werden.
- Duldung militärischer Nutzung (z. B. Infrastruktur, Flächen, Netze).

Risiko- und Bedrohungslage

- Unternehmen müssen sich darauf einstellen, dass sie Ziel hybrider Angriffe werden (Cyberangriffe, Sabotage, Desinformation).
- Besonders KRITIS-Unternehmen stehen im Fokus, weil deren Ausfall massive Effekte auf Militär und Gesellschaft hat.

Erwartete Beiträge der Unternehmen

- BCM auch auf Szenarien LV/BV erweitern (Blackout, Teilabschaltung Netze, Versorgungsknappheit).
- Kooperation mit Behörden und Bundeswehr im Krisenfall.
- Notfallkommunikation: Krisenstab-Fähigkeit, Ansprechbarkeit 24/7.
- Cyber-Resilienz verstärken.

V. Business Continuity Management in der Praxis

Fallbeispiel: Business Continuity Management in der Praxis

- **Hintergrund:** Ein mittelständisches Unternehmen im Bereich Maschinenbau, „Tech Machinery GmbH“, war auf die Produktion von hochspezialisierten Maschinen angewiesen. Eines Morgens wurde das Unternehmen Ziel eines unerwarteten Cyberangriffs, der die IT-Infrastruktur lahmlegte und den Zugriff auf wichtige Produktionsdaten verhinderte. Die Geschäftsführung musste schnell handeln, um die Auswirkungen auf die Produktion und die Lieferkette zu minimieren.
- **Herausforderung:** Der Cyberangriff führte zu einem kompletten Stillstand der Produktionslinien, was nicht nur zu finanziellen Verlusten führte, sondern auch die Beziehungen zu wichtigen Kunden gefährdete, die auf pünktliche Lieferungen angewiesen waren.
- **Lösung:** Tech Machinery hatte im Vorfeld ein umfassendes BCM implementiert, das folgende Schritte umfasste:
  - **Risikoanalyse und Notfallplanung:** Das Unternehmen hatte potenzielle Risiken identifiziert und Notfallpläne entwickelt, die spezifische Szenarien wie Cyberangriffe berücksichtigten.
  - **Etablierung eines Krisenmanagementteams:** Sofort nach dem Vorfall trat das Krisenmanagementteam in Aktion, um die Situation zu bewerten und die Notfallpläne umzusetzen.
  - **Datenwiederherstellung:** Tech Machinery hatte regelmäßige Backups seiner Daten in einem sicheren Cloud-Speicher. Das Team konnte schnell auf die letzten gesicherten Daten zugreifen und die IT-Systeme wiederherstellen.
  - **Kommunikation:** Die Geschäftsführung informierte proaktiv alle Stakeholder, einschließlich Mitarbeiter, Kunden und Lieferanten, über die Situation und die Maßnahmen, die ergriffen wurden, um die Produktion schnellstmöglich wieder aufzunehmen.
  - **Schulung und Sensibilisierung:** Nach dem Vorfall wurden zusätzliche Schulungen für Mitarbeiter durchgeführt, um das Bewusstsein für Cyberrisiken zu schärfen und sicherzustellen, dass alle Mitarbeiter die Sicherheitsrichtlinien kannten.

- **Ergebnis:** Dank des effektiven Business Continuity Managements konnte Tech Machinery die Produktion innerhalb von 48 Stunden wieder aufnehmen. Die schnelle Reaktion und die vorhandenen Notfallpläne minimierten die finanziellen Verluste und halfen, das Vertrauen der Kunden zu erhalten. Das Unternehmen lernte aus dem Vorfall und verbesserte seine Sicherheitsmaßnahmen, um zukünftige Angriffe besser abwehren zu können.

Dieses Fallbeispiel zeigt, wie wichtig ein gut strukturiertes Business Continuity Management ist, um die Resilienz eines Unternehmens gegenüber unerwarteten Störungen zu erhöhen.

Fazit

Schwerwiegende Schadenslagen im Sinne von Krisen und Katastrophen können – wenn sie eintreten und eine Prävention versagt hat – sowohl Unternehmen als auch das öffentliche Leben nachhaltig treffen und zu hohen Opferzahlen sowie zu extremen Sachschäden und letztendlich zu einem nachhaltigen Reputationsschaden führen. Es muss daher Ziel eines strategisch ausgerichteten Krisen- bzw. Resilienzmanagements und einer vorausschauenden strategischen Präventionsplanung sein, möglichst vor einer Krise – und nicht erst in der eingetretenen Krisenlage – die Auswirkungen aller denkbaren Schadenslagen zu erkennen und deren Folgen weitgehend abzufedern, damit sich diese Lage nicht zu einer Katastrophe entwickelt. Dies gilt auch für sogenannte „neue Gefahrenlagen" aufgrund einer veränderten Sicherheitslage in Deutschland und mögliche Bedrohungen von außen, z. B. durch Russland. Zugleich bedarf die Anpassung von Gefahrenabwehr- und Notfallplänen unter Berücksichtigung neuer Gesetzesvorgaben eine vorausschauende strategische Ausrichtung, um sich besser für Krisen wappnen zu können.

Um sich nicht nur im Problematisieren zu verlieren, sondern prägnante Handlungshilfen zu liefern, wurden angepasste Schulungs- und Übungskonzepte vorgestellt, nach denen die mit Schadenslagen beauftragten Führungs- und Funktionskräfte in Krisen- und Notfallstäben erste Musteranweisungen für den täglichen Gebrauch in der Praxis bekommen.

Hieraus lassen sich vier Anforderungen an ein gutes und angepasstes Krisenmanagement definieren:

1. Analyse der vorhandenen Alarmierungs- und Notfallpläne einschließlich neuer sogenannter „Blackout-Vorsorgemaßnahmen".
2. Aufzeigen und Bewerten der bisher eingeleiteten Maßnahmen in den strategischen Stellen von Unternehmen und deren Krisen-/Notfallstäben: getätigte Maßnahmen des Krisenmanagements, Ziele und erreichte Zwischenschritte im Verhältnis zum Einsatz der Mittel.
3. Bewertung der Effektivität der getroffenen und eingeleiteten Entscheidungen
   - → Maßnahmen zum Krisen-/Notfallmanagement

- Beurteilung, ob bestehende Notfallpläne und andere Schutzpläne, u. a. auch Blackout-Vorsorgepläne, entsprechend angewandt wurden
- Vorschläge zur Besetzung der bestehenden Krisen-/Notfallteams (Struktur des Krisen- und Notfallstabs)
- Überprüfung der Zielvorgaben für den Business-Continuity-Plan und des Grades seiner Umsetzung in der Praxis
- Prüfung der Entscheidungsgrundlagen, auf deren Basis strategische Entscheidungen auch im Verhältnis zur Kompetenz getroffen wurden
- Reaktion auf außergewöhnliche, nicht vorhersehbare Entwicklungen und Rückmeldungen von nächsthöheren Organisationen
- Prüfung der durchgeführten Presse- und Öffentlichkeitsarbeit und der Rückmeldung von Kunden des Unternehmens
- Überlegungen zum effektiven Einsatz von Stabs- und Führungssystemen (Technikeinsatz) und zur Frage, ob sich dadurch kurzfristig auch sichere Entscheidungen ableiten lassen (Überlegungen zum Einsatz von „KI")
- Generelles Abwägen, was „gut" funktioniert hat und welche Maßnahmen bzw. Handlungen „erschwerend" und/oder sogar „hinderlich" für das Krisen-/Notfallmanagement gewirkt haben

4. Folgerungen für ein zukünftiges optimiertes Krisen- und Notfallmanagement
   - Abwägung der bestehenden und sich wandelnden Risiken weiterer Gefahrenlagen und deren Veränderungen
   - Aufzeigen konkreter Handlungsoptionen mit Schwerpunkt auf neue „Chancen", die sich aus der derzeitigen Krise für Unternehmen und deren Notfallstäbe ergeben

Unter Anwendung der vier Punkte und des spezifischen Ableitens gemeinsamer Vorstellungen zu vorhandenen und neuen strategischen Überlegungen können Unternehmen ihr Sicherheits- und Notfallmanagement besser und somit nachhaltiger für die Zukunft aufstellen. Sie werden somit in die Lage versetzt, gestärkt auf Krisenlagen und neue, in sich kaskadierende komplexe Schadenslagen zu reagieren und ausreichende Präventionsmaßnahmen für eine veränderte Gesetzesgrundlage mit dem NIS-2-Gesetz und dem KRITIS-Dach-Gesetz auszuführen.

Literaturverzeichnis

Monographien und Bücher

Haake, Florian / Endress, Christian (Hrsg.) (2022): Risiko Blackout: Krisenvorsorge für Wirtschaft, Behörden und Kommunen. Stuttgart: Richard Boorberg Verlag.

Latza, Mark (2025): Kritische Infrastrukturen aus versicherungstechnischer Sicht. Handbuch für KRITIS, BCM und ESG. Ahrensburg: tredition GmbH.

Naujoks, Uwe/Grete, Patrick (Hrsg.) (2023): Arbeitsbuch Business Continuity und Notfallmanagement in Banken. Heidelberg: Springer.

Petermann, Thomas/Bradke, Harald/Lüllmann, Arne/Poetzsch, Maik/Riehm, Ulrich (2010): Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. Berlin: TAB-Studien (Arbeitsbericht Nr. 141).

Rühl, Uwe (2021): Quick Guide Erfolgreiches Business-Continuity Management. Wie Sie Geschäftsunterbrechungen überleben und gestärkt in die Zukunft gehen. Berlin: Springer Gabler Verlag.

Aufsätze in Zeitschriften

Borries, Hans-Walter (2023): Gasmangel-Blackout – realistische Gefahr der Versorgungssicherheit oder nur Panikmache? In: Crisis Prevention, Heft 1/2023, S. 26-30.

Borries, Hans-Walter (2023): Gefahrenlage: Kritische Infrastrukturen und Blackouts – Eine neue Aufgabe für das Krisenmanagement von Krisen und Verwaltungsstäben. In: Transforming Cities, Heft 1/2023, S. 64-68.

Borries, Hans-Walter (2024): Alle KRITIS-Sektoren prüfen. In: stadt + werk Politik und Strategie, Heft 5-6/2024, S. 14-15.

Borries, Hans-Walter (2025): Krisenmanagement und KRITIS-Gefahrenlagen mehr ernst nehmen. In: Behörden Spiegel Jahrbuch 2025 (Moderner Katastrophenschutz) u. a. zu „Epochenwende Gefahrenabwehr – Die große Chance durch

Sondervermögen und Grundgesetzänderung für Feuerwehr – Rettungsdienst – Katastrophenschutz – Zivilschutz", S. 18-19.

Borries, Hans-Walter (2025): Kritische Infrastrukturen besser schützen. In: Kommunalpolitische Blätter (KOPO), Heft 1-2/2025, S. 39-41.

Borries, Hans-Walter (2025): Facetten der Resilienz – zwischen handfestem Schutz und Empowerment. In: Behörden Spiegel, April 2025, S. 37.

Köppe, Mario (2020): „Als in Köpenick das Licht ausging" – ein Erfahrungsbericht. In: BBK-Bevölkerungsschutz, Heft 1/2020, S. 18-19.

Pislar, Marko (2014): Blackout in Slowenien. Erster Teil. In: Truppendienst. Magazin des Österreichischen Bundesheeres, Nr. 340.

Berichte und Studien

Allianz für Sicherheit in der Wirtschaft e.V. ASW Bundesverband/Allianz für Sicherheit in der Wirtschaft Norddeutschland e.V./Bayerischer Verband für Sicherheit in der Wirtschaft e.V. (2025): Sonderheft – Operationsplan Deutschland News für Unternehmen – Handlungsempfehlungen und Praxiswissen. In: Sicher – Das Magazin, Heft 1/2025. Berlin, Hamburg, München.

Borries, Hans-Walter (2025): Stellungnahme zur Sachverständigen-Anhörung der Enquetekommission „Krisen und Notfallmanagement – durch die Lehren der Vergangenheit die Zukunft sicher gestalten" (Klimawandel/staatliche Ebenen) am 3. Juni 2024. Hg. v. Institut für Wirtschafts- und Sicherheitsstudien FIRMITAS (Witten). Landtag NRW, in: Landtag Nordrhein-Westfalen, Drucksache 18/15420, 18. Wahlperiode vom 25.08.2025.

Bubendorfer-Licht, Sandra/Eckert, Leon/Hahn, André/Krings, Günter/Schäfer, Ingo (2025): Grünbuch ZMZ 4.0. Zivil-Militärische Zusammenarbeit 4.0 im militärischen Krisenfall. Eine Situationsbeschreibung, Analyse und Handlungsempfehlungen. Berlin: Zukunftsforum Öffentliche Sicherheit e.V.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)/Bundesinstitut für Risikobewertung (BfR) (2022): Risikokommunikation: Ein Handbuch für die Praxis. Bonn.

Bundesministerium des Innern (2022): Eckpunkte für das KRITIS-Dachgesetz. Berlin, 07.12.2022.

Bundesministerin des Innern und für Heimat/Bundesminister der Verteidigung (2024): Rahmenrichtlinien für die Gesamtverteidigung (RRGV). Berlin, 05.06.2024.

Bundesministerium für Verteidigung (2023): Verteidigungspolitische Richtlinien (VPR). Berlin, 09.11.2023.

Bundesministerium für Verteidigung (2024): Operationsplan Deutschland – Eine gesamtstaatliche und gesellschaftliche Aufgabe. Berlin.

Bundesministerium für Wirtschaft (2019): Notfallplan Gas. Berlin, 17.09.2019.

Bundesministerium für Wirtschaft und Klimaschutz (2023): Notfallplan Erdgas für die Bundesrepublik Deutschland. Berlin, 22.05.2023.

Die Bundesregierung (2023): Nationale Sicherheitsstrategie „Integrierte Sicherheit für Deutschland". Berlin, 14.06.2023.

DIN e. V. (2023): Whitepaper: Normierung und Standardisierung bei der Ausgestaltung des KRITIS-Dachgesetz. Berlin.

Deutscher Bundestag (2013): Unterrichtung durch die Bundesregierung. Bericht zur Risikoanalyse im Bevölkerungsschutz 2012 – Risikoanalyse Pandemie durch Virus Modi-SARS. Berlin (Drucksache 17/12051, 03.01.2013).

EU-NATO-Task Force (2023): On the Resilience of Critical Infrastructure – Final Assessment Report. Brüssel, Juni 2023.

EWI & BET (2025): Energiewende. Effizient. Machen. – Monitoringbericht zum Start der 21. Legislaturperiode, im Auftrag des Bundesministeriums für Wirtschaft und Energie.

Internetquellen

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: KRITIS-Gefahren. URL: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/KRITIS-Gefahrenlagen/kritis-gefahrenlagen_node.html [Zugriff: 25.08.2025].

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Kritische Infrastrukturen. URL: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html [Zugriff: 25.08.2025].

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Stromausfall. URL: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/KRITIS-Gefahrenlagen/Stromausfall/stromausfall_node.html [Zugriff: 25.08.2025].

Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-4. Business Continuity Management. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [Zugriff: 25.08.2025].

Bundesnetzagentur: Veröffentlichung des Versorgungssicherheitsmonitorings. URL: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2025/20250903_Versorgungsmonitoring.html [Zugriff: 22.09.2025].

DIN e.V. (2025): DIN SPEC 14027. URL: https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth:din21:382621796. Dokument im Erscheinen. [Zugriff: 19.11.2025].

Fekonja, Stefanie/Lehmann, Marcel/Wiersch, Marius: KRITIS: BCM und Business Resilienz für kritische Dienstleistungen. URL: https://www.ibcrm.de/wp-content/uploads/2020/03/IBCRM_Grundlagendokument-KRITIS-und-BCM_V1.0.pdf [Zugriff: 25.08.2025].

IT-Magazine: Strommangellage: Wie kann eine KMU seine Resilienz stärken? URL: https://www.itmagazine.ch/artikel/78141/Strommangellage_Wie_kann_ein_KMU_seine_Resilienz_staerken.html [Zugriff: 25.08.2025].

Wisler, Andreas: ISO 22301 – Vorbereitung auf den Ernstfall – Business Continuity. URL: https://27001.blog/iso-22301-vorbereitung-auf-den-ernstfall-business-continuity [Zugriff: 25.08.2025].

Abkürzungsverzeichnis

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCP	Business Continuity Plan
BCM	Business Continuity Management
BfR	Bundesinstitut für Risikobewertung
BIA	Business Impact Analyse
BLG	Bundesleistungsgesetz
BMVg	Bundesverteidigungsministerium
BMWE	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BOS	Behörden und Organisationen mit Sicherheitsaufgaben/ Blaulichtorganisationen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BW	Bundeswehr
CER	Critical Entities Resilience
DECT	Digital Enhanced Cordless Telecommunications
DRK	Deutsches Rotes Kreuz e. V.
EnSiG	Energiesicherungsgesetz
ESVG	Ernährungssicherstellungs- und -vorsorgegesetz
ETB	Einsatztagebuch

FGL	Fachgruppenleiter
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GG	Grundgesetz
IIS	Fraunhofer-Institut für Integrierte Schaltungen
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IUK	Information und Kommunikation
KGS/LVK	Koordinierungsgruppe/Lage-Versorgung-Koordination
KRITIS	Kritische Infrastrukturen
LBG	Landesbeschaffungsgesetz
LVE	Lagevortrag zur Vorbereitung einer Entscheidung
LVU	Lagevortrag zur Unterrichtung
NATO	North Atlantic Treaty Organization
NIS2	Network and Information Systems Security
OPLAN DEU	Operationsplan Deutschland
PDCA	Plan-Do-Check-Act
PSG	Postsicherstellungsgesetz
SAE	Stab für außergewöhnliche Ereignisse
SAIDI	System Average Interruption Duration Index
SchBerG	Schutzbereichsgesetz

TAB	Technikfolgenabschätzung beim Deutschen Bundestag
THW	Technisches Hilfswerk
USV	Unterbrechungsfreie Stromversorgung
VerkSiG	Verkehrssicherstellungsgesetz
VOIP	Voice over Internet Protocol
WasSiG	Wassersicherstellungsgesetz
WiSiG	Wirtschaftssicherstellungsgesetz
ZMZ	Zivil-Militärische Zusammenarbeit

Impressum

Dieses Kompendium wurde im Auftrag der Stiftung Familienunternehmen von Experten verfasst.

Hans-Walter Borries: Dr. rer. nat., Diplom-Geograph, Direktor des Instituts für Wirtschafts- und Sicherheitsstudien FIRMITAS und Lehrbeauftragter an den Hochschulen Magdeburg-Stendal und an der FOM Hochschule für Oekonomie & Management, Essen. Dem Bundesverband für den Schutz Kritischer Infrastrukturen BSKI e. V. gehört er als Stellvertretender Vorstandsvorsitzender an. Borries ist Oberst der Reserve und Mitglied im Rat der Sachverständigen der Enquetekommission II Krisen- und Notfallmanagement im Kontext von Klimawandel (staatliche Ebenen) des Landtages NRW. Er ist Herausgeber und Verfasser von Fachpublikationen, u. a. zu Sicherheitspolitik, Bevölkerungsschutz und Krisenmanagement.

Volker Buß: Als Chief Security Officer (CSO) und Chief Information Security Officer (CISO) der Merck Group trägt er die Gesamtverantwortung für alle sicherheitsrelevanten Prozesse weltweit. Er verfügt über langjährige Erfahrung in der Bewältigung von Krisenlagen sowie dem Aufbau und dem Betrieb von BCM-Prozessen in komplexen Unternehmensstrukturen.

Stiftung Familienunternehmen
Prinzregentenstraße 50
D-80538 München
Tel.: +49 89 12 76 400 02
info@familienunternehmen.de
www.familienunternehmen.de

Rund 90 Prozent aller Unternehmen in Deutschland sind Familienunternehmen. Die gemeinnützige Stiftung Familienunternehmen setzt sich für den Erhalt dieser Familienunternehmenslandschaft ein. Sie ist der bedeutendste Förderer wissenschaftlicher Forschung auf diesem Feld und Ansprechpartner für Politik und Medien in wirtschaftspolitischen, rechtlichen und steuerlichen Fragestellungen. Zweck der Stiftung ist die Förderung, Information, Bildung und Erziehung sowie der wissenschaftliche Erfahrungsaustausch auf dem Gebiet des Familienunternehmertums in Europa.

Stiftung Familienunternehmen

Prinzregentenstraße 50
D-80538 München

Telefon + 49 (0) 89 / 12 76 400 02
E-Mail info@familienunternehmen.de

www.familienunternehmen.de

Preis: 9,90 €
ISBN: 978-3-948850-71-5