HK Hamburg

BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

VORSORGEPLAN

„KRISEN, KATASTROPHEN, KONFLIKTE: WIE SIE IHR UNTERNEHMEN IN UNSICHEREN ZEITEN SCHÜTZEN“

Inhaltsverzeichnis

I. Einleitung 4

II. Rahmen einer Krisenvorsorge(-planung) 4
- 1.1 Szenarien als Stresstest 4
- 1.2 Komplexität von Krisen – die zeitliche Dimension 5
- 1.3 Fokus: Zivile Verteidigung 6

III. Kernmaßnahmen: Was Unternehmen jetzt tun sollten 7
- 2.1 Führung sicherstellen 7
- 2.2 Gesetze und Regelungen vorab prüfen 8
- 2.3 Lage erfassen und bewerten 8
- 2.4 Unternehmensinterne Vorbereitung und Vorplanung als Führungsaufgabe gestalten 8
- 2.5 Standortsicherheit und Objektschutz prüfen 9
- 2.6 Lieferketten aufrechterhalten 9
- 2.7 Betriebsinterne Infrastruktur sicherstellen 9
- 2.8 Personalplanung sichern und Einsatzfähigkeit erhalten 10
- 2.9 Spionage und Sabotage verhindern 10
- 2.10 Interne und externe Kommunikation aufrechterhalten 10
- 2.11 Chancen erkennen und Geschäftspotenziale im Krisenfall nutzen 11

Fazit 11

Anhang 12
- Militärische Konflikte – Spannungs-, Zustimmungs-, Bündnis- und Verteidigungsfall 12
- Ausgewählte Gesetze der Notstandsgesetzgebung 12

Weiterführende Informationen (Auswahl) 14
- Strategien, Konzepte, Dokumente 14
- Handreichungen 15

Checklisten für die Geschäftsführung 17

Impressum 24

Vorwort

Die vergangenen Jahre haben uns deutlich vor Augen geführt, wie eng wirtschaftliche Stabilität, gesellschaftliche Resilienz und Sicherheit miteinander verflochten sind. Der völkerrechtswidrige Angriff Russlands auf die Ukraine und die dadurch veränderte Sicherheitslage in Europa haben gezeigt, dass Krisenvorsorge und Widerstandsfähigkeit keine abstrakten Themen sind, sondern eine zentrale Zukunftsaufgabe für Staat, Wirtschaft und Gesellschaft darstellen.

Vor diesem Hintergrund übernimmt die Hamburger Wirtschaft Verantwortung und eine zentrale Rolle in der zivil-militärischen Zusammenarbeit mit dem Hamburger Senat und der Bundeswehr. Unsere Unternehmen – ob global vernetzte Konzerne oder mittelständische Betriebe – sichern mit Innovationskraft, Anpassungsfähigkeit und einem starken Gemeinschaftsgeist die Funktionsfähigkeit unserer Stadt auch unter schwierigen Rahmenbedingungen. Viele Betriebe verfügen bereits über erprobte Krisen- und Notfallpläne, passen ihre Strukturen flexibel an und tragen damit wesentlich zur Stabilität des Standorts bei.

Mit diesem gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) entwickelten Leitfaden wollen wir insbesondere kleine und mittlere Unternehmen ermutigen, ihre Krisenvorsorge systematisch zu überprüfen und weiterzuentwickeln. Szenarien, Stresstests und eine vorausschauende Planung sind keine Belastung, sondern ein strategischer Vorteil. Sie helfen, Risiken frühzeitig zu erkennen, betriebliche Abläufe zu sichern und im Ernstfall handlungsfähig zu bleiben.

Die Herausforderungen unserer Zeit – von geopolitischen Spannungen über Energiefragen bis zu Lieferkettenrisiken und Cybergefahren – sind groß. Doch sie eröffnen zugleich neue Chancen für Innovation, Zusammenarbeit und nachhaltiges Wachstum. Wenn Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft gemeinsam an Lösungen arbeiten, kann Hamburg seine Stärke als resilienter, verlässlicher und zukunftsorientierter Wirtschaftsstandort weiter ausbauen.

Wir verstehen diesen Vorsorgeplan als Beitrag zur Resilienz der Wirtschaft in Hamburg und dem gesamten Bundesgebiet. Wir danken allen, die sich engagiert an der Stärkung unserer gesamtgesellschaftlichen Widerstandskraft beteiligen – mit Tatkraft, Verantwortung und einem klaren Blick nach vorn.

Prof. Norbert Aust
Präses

Dr. Malte Heyne
Hauptgeschäftsführer

I. Einleitung

Der völkerrechtswidrige Angriffskrieg Russlands gegen die Ukraine hat die Sicherheitslage in Europa grundlegend verändert. Diese neue Realität zeigt, dass sich Deutschland gesamtgesellschaftlich resilienter aufstellen muss. Dabei erfordern die sicherheitspolitischen Entwicklungen im Kontext der Gesamtverteidigung nicht nur militärische Anstrengungen, sondern auch zivile Maßnahmen.

Eine gut vorbereitete Wirtschaft ist ein wichtiger Faktor für eine resiliente Gesellschaft und die Umsetzung der Zivilen Verteidigung. Bereits heute treffen Unternehmen verschiedene Maßnahmen, um operative und finanzielle Risiken zu steuern und Ereignisse und Krisen zu bewältigen. Angesichts der globalen Sicherheitslage ist es jedoch erforderlich, Entwicklungen in das unternehmerische Krisenmanagement einzubeziehen, die bislang noch nicht betrachtet wurden. Es gilt, die bestehenden Vorsorgepläne kritisch zu überprüfen und auszuweiten.

Diese Handreichung richtet sich insbesondere an kleine und mittlere Unternehmen (KMU). Sie bietet Ihnen einen kompakten Überblick über die zentralen Themen und Fragestellungen einer modernen Krisenvorsorgeplanung. Ergänzt wird sie durch eine strukturierte Checkliste mit konkreten Handlungsempfehlungen. Ziel ist es, dass Sie und Ihr Unternehmen aufbauend auf der Vorsorge für friedenszeitliche Krisen auch auf mögliche Szenarien der Zivilen Verteidigung vorbereitet sind.

II. Rahmen einer Krisenvorsorge(-planung)

Jedes Unternehmen setzt sich – bewusst oder unbewusst – mit seinen individuellen Risiken auseinander. Unabhängig davon, ob dies explizit als Risikomanagement bezeichnet wird, prüfen Betriebe mögliche Gefährdungen für die Aufrechterhaltung ihrer Betriebsfähigkeit und übertragen diese auf das eigene Unternehmen – teils situativ, teils strukturiert. Ebenso verfügt jedes Unternehmen über Ansätze, um Krisen zu bewältigen. Diese können im Kontext des Notfall- oder Krisenmanagements oder im Betrieblichen Kontinuitätsmanagements (BKM bzw. Business Continuity Management, BCM) geplant und umgesetzt werden.

Damit Sie sich im Rahmen des Risiko- und Krisenmanagements wirksam auf mögliche Ereignisse vorbereiten und bestehende Planungen regelmäßig überprüfen, ist das Denken in Szenarien ein bewährtes Instrument.[1] Szenarien helfen, mögliche zukünftige Situationen zu veranschaulichen – Ereignisse, die plötzlich oder mit Vorlauf eintreten können, nur kurz andauern oder sich über längere Zeit hinziehen und auf die ein Unternehmen reagieren muss, um seine Betriebsfähigkeit zu sichern.

Im Krisenmanagement gehören dazu klassische Szenarien wie Strom- oder IT-Ausfälle, Störungen in der Lieferkette, Gebäudeausfälle durch Naturereignisse oder technisch induzierte Gefahren sowie Personalausfälle infolge von Pandemien.

Dabei gilt: Szenarien stellen immer nur mögliche Zukünfte dar. Sie können nicht alle denkbaren qualitativen oder quantitativen Entwicklungen vollständig abbilden. Ihr Wert liegt vielmehr darin, Denkanstöße zu geben – und Unternehmen dazu zu ermutigen, über das einzelne Szenario hinauszudenken und eigene Handlungsoptionen zu entwickeln.

2.1 Szenarien als Stresstest

Anknüpfungspunkte für eine szenariobasierte Vorbereitung auf mögliche Krisenfälle können frühere Ereignisse sein, die das eigene Unternehmen betroffen und zu Ausfällen geführt haben. Diese Erfahrungen helfen, Parameter, Größenordnungen und reale Auswirkungen von Szenarien besser zu verstehen und einzuordnen. Szenarien sollen einerseits plausibel sein, andererseits aber auch die bestehenden Strukturen des Unternehmens herausfordern. So können Sie Handlungsfähigkeit im Ereignisfall sicherstellen und die Resilienz Ihres Unternehmens stärken.

Mit Blick auf Naturgefahren lassen sich lokale Ereignisse am Unternehmensstandort quantitativ hochskalieren: Bereiten Sie Szenarien auf in den Dimensionen der Elbeflut 2013 und der Flutkatastrophe 2021 an Ahr und Erft, der Orkantiefs Kyrill 2007 und Friederike 2018 oder den Hitzewellen 2003, 2015 und 2022. So können Sie die Auswirkung auf die eigene Betriebsfähigkeit durchspielen. Ziehen Sie vergleichbare Szenarien für Standorte von wichtigen Geschäftspartnern heran und untersuchen Sie diese auf Auswirkungen beispielsweise auf Lieferketten.

Für das Szenario Stromausfall gibt es eine Vielzahl von Ereignissen unterschiedlicher Ausbreitung und Dauer als Blaupause für Stresstests: durch Bauarbeiten oder Brandanschläge ausgelöste Stromausfälle von bis zu zwei Tagen (Berlin 2019 und 2025), ein mehrtägiger regionaler Stromausfall infolge von Schneelast (Münsterland 2005) oder ein landesweiter Stromausfall (Spanien 2025). Diese Beispiele zeigen, wie schwierig es ist, Eintritt, Dauer und Ausbreitung eines Stromausfalls abzuschätzen und sich auf die Folgen einzustellen (siehe Abschnitt B2).

Qualitativ betrachtet stellen vernetzte Szenarien, die multiple Krisen simulieren, eine besondere Herausforderung dar. Gleichzeitig ermöglichen sie, Abhängigkeiten und blinde Flecken in der Risikoeinschätzung und -vorsorge aufzudecken. Hier treffen mehrere Ereignisse unterschiedlicher Art aufeinander, verstärken sich gegenseitig oder stehen bei der Bewältigung in Konkurrenz zueinander. Dies erschwert die Entscheidungsfindung erheblich. Beispiele für Szenarien sind etwa die Rückführung von Betriebsangehörigen aus Krisengebieten in Fernost während eines Komplettausfalls der IT nach einem Ransomware-Angriff oder ein mutwillig herbeigeführter Brand durch einen Innentäter in einem Großlager, in dem Zulieferteile zur Überbrückung bestehender Lieferengpässen gelagert waren.

2.2 Komplexität von Krisen – die zeitliche Dimension

Krisen können plötzlich und unerwartet eintreten – oder sich schleichend entwickeln. Auf beides sollte sich Ihr Unternehmen einstellen. Auch die Dauer von Krisen kann stark variieren, von wenigen Tagen bis hin zu Monaten und Jahren. Die Zeitspanne beeinflusst maßgeblich die Planungen und konkrete Maßnahmen zur Krisenbewältigung und damit auch den Umgang mit Krisen.

Vorlaufzeit für Kriseneintritt:

Akute Krisen entstehen durch ein plötzliches Initialereignis und lassen sich mit alltäglichen Maßnahmen zur Schadensvermeidung oder -minderung nicht mehr bewältigen. Beispiele hierfür sind Sturzfluten, Brände, Stromausfälle, Cyberangriffe oder Terroranschläge. Um in solchen Fällen handlungsfähig zu bleiben, sind vorgefertigte Notfall- und Krisenpläne („Schubladenpläne“) unverzichtbar. Sie sollten den Aufbau einer (Krisen-)Organisation, die Sicherstellung der Führung, klare Zuständigkeiten und Maßnahmen zur Krisenbewältigung umfassen, ebenso Konzepte einer internen und externen Krisenkommunikation.

Schleichende Krisen entwickeln sich über einen längeren Zeitraum. Anfangs werden sie oft nur als vorübergehende Veränderungen wahrgenommen Ab einem bestimmten Kipppunkt jedoch manifestieren sie sich als spürbare Krise – scheinbar plötzlichen, tatsächlich aber mit langem Vorlauf. Beispiele sind die Covid-19-Pandemie, anhaltende Trockenheit oder Dürreperioden, wirtschaftspolitische Spannungen oder sicherheitspolitische Eskalationen. Um auch diese Krisen frühzeitig zu erkennen und schnell handlungsfähig zu sein, ist eine gute Lagebeobachtung unabdingbar. Veränderungen müssen erfasst, mögliche zukünftige Entwicklungen antizipiert und Mitarbeitende für Warnsignale sensibilisiert werden.

Dauer der eingetretenen Krise:

Kurzfristige Krisen dauern in der Regel wenige Tage bis höchstens einen Monat. Mögliche Ursachen sind etwa Stromausfälle, Terroranschläge oder lokale Unwetter. In solchen Situationen geht es vor allem darum, den Notbetrieb aufrechtzuhalten, Ausfälle zu überbrücken – beispielsweise durch eine Notstromversorgung für 48 oder 72 Stunden – und die Sicherheit der Mitarbeitenden zu gewährleisten, um Schäden so gering wie möglich zu halten.

Mittelfristige Krisen, die sich über mehrere Wochen erstrecken, erfordern häufig eine Anpassung der Produktion oder zumindest eine Umstellung von Abläufen und Prozessen. Ziel ist es, den Geschäftsbetrieb trotz Einschränkungen so weit wie möglich aufrechtzuerhalten. Cyberangriffe, großflächige Hochwasserlagen oder Störungen in den Lieferketten können typische Auslöser solcher Krisen sein.

Langfristige Krisen, die sich über mehrere Monate bis hin zu Jahren ziehen, machen dagegen eine grundlegende Neuausrichtung erforderlich. In diesen Fällen kann es sinnvoll sein, Geschäftsprozesse umfassend anzupassen, neue Geschäftsfelder zu erschließen oder eine gesamtstrategische Neuausrichtung des Unternehmens vorzunehmen. Zu den möglichen Szenarien langfristiger Krisen zählen wirtschaftspolitische Entwicklungen ebenso wie militärische oder hybride Konflikte.

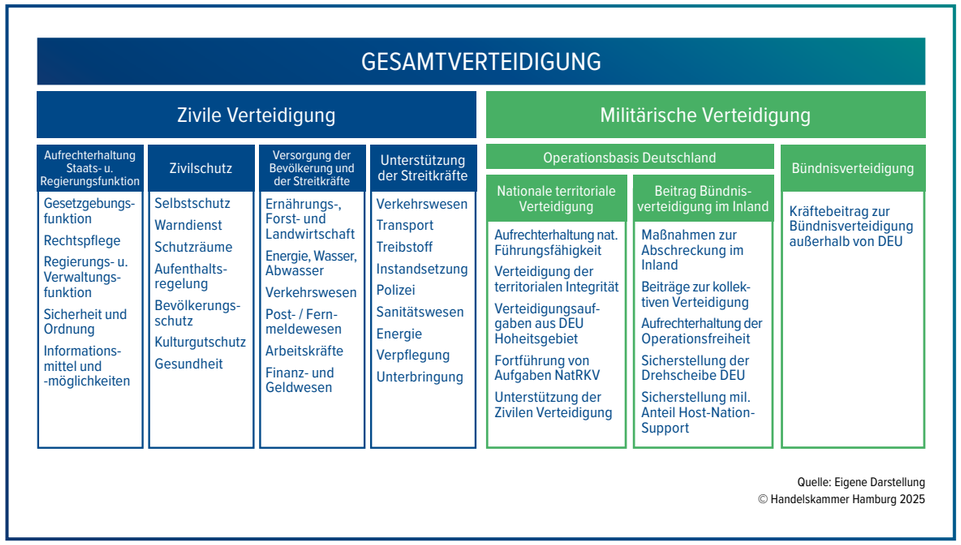
1 Siehe u. a. Institut für Zukunftsstudien und Technologiebewertung: Methoden der Zukunfts- und Szenarioanalyse. WerkstattBericht Nr. 103, Berlin 2008, https://www.izt.de/media/2022/10/IZT_WB103.pdf

2.3 Fokus: Zivile Verteidigung

Die veränderte sicherheitspolitische Lage macht es erforderlich, militärische Bedrohungen als mögliche Szenarien in der unternehmerischen Krisenvorsorge mitzudenken und in die Planungen einzubeziehen. Eine verantwortungsbewusste staatliche Vorsorgepolitik kann daher nicht auf die Fähigkeit zur Verteidigung verzichten. Dazu gehören sowohl die militärische als auch die Zivile Verteidigung – zwei organisatorisch voneinander unabhängige, aber gleichrangige Komponenten der Gesamtverteidigung, die demselben Ziel verpflichtet sind: der Sicherung von Staat und Gesellschaft im Krisen- oder Verteidigungsfall.

Diese enge Verzahnung von militärischer und ziviler Verteidigung findet Ausdruck in den 2024 überarbeiteten „Rahmenrichtlinien für die Gesamtverteidigung“[2] (RRGV). Ergänzend dazu bilden die „Konzeption Zivile Verteidigung“[3] (KZV, 2016) und die „Verteidigungspolitischen Richtlinien“[4] (VPR, 2023) zentrale Grundsatzdokumente, die die Rahmenrichtlinien sowohl aus ziviler als auch aus militärischer Perspektive flankieren.

Abbildung 1: Die zivile Verteidigung im Rahmen der Gesamtverteidigung



Quelle: Eigene Darstellung
© Handelskammer Hamburg 2025

Unternehmen als Akteur in der Zivilen Verteidigung

Die Konzeption Zivile Verteidigung definiert die Zivile Verteidigung als Aufgabe, alle Maßnahmen zu planen, vorzubereiten und durchzuführen, die zur Herstellung und Aufrechterhaltung der Verteidigungsfähigkeit erforderlich sind – einschließlich der Versorgung und des Schutzes der Zivilbevölkerung.

Damit wird auch die Wirtschaft zu einem zentralen Partner in der Gesamtverteidigung: Unternehmen tragen im äußeren Notstand dazu bei, den lebens- und verteidigungswichtigen Bedarf an Gütern und Dienstleistungen für die Zivilbevölkerung und die Bundeswehr sicherzustellen. Diese Verantwortung ist insbesondere in Säule 3 („(Not-) Versorgung“) der Konzeption verankert und wird in den Sicherstellungsgesetzen für verschiedene Wirtschaftssektoren konkretisiert.

Darüber hinaus unterstützt die Wirtschaft die Streitkräfte direkt bei der Herstellung und Aufrechterhaltung ihrer Verteidigungsfähigkeit und Operationsfreiheit (Säule 4, „Unterstützung der Streitkräfte“). Dazu zählt etwa die Verlegung und Versorgung verbündeter und eigener Streitkräfte an die Ostflanke der NATO – eine logistische Aufgabe, die ohne Mitwirkung privater Unternehmen nicht realisierbar wäre.

2 Rahmenrichtlinien für die Gesamtverteidigung, www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.pdf?__blob=publicationFile&v=1
3 Konzeption Zivile Verteidig, www.bmi.bund.de/DE/themen/bevoelkerungsschutz/zivil-und-katastrophenschutz/konzeption-zivile-verteidigung/konzeption-zivile-verteidigung-node.html
4 VerteidigungspolitischenRichtlinien,https://www.bmvg.de/de/aktuelles/verteidigungspolitische-richtlinien-2023-veroeffentlicht-5701338

Um diese „Drehscheiben-Funktion“ als Staat im Zentrum Europas umsetzen zu können, hat die Bundeswehr 2024 den „Operationsplan Deutschland“[5] (OPLAN DEU) entwickelt. Dieses als geheim eingestufte Dokument führt die zentralen militärischen Anteile der Landes- und Bündnisverteidigung mit den notwendigen zivilen Unterstützungsleistungen in einem operativen Gesamtplan zusammen. Es empfehlen sich Informationsveranstaltungen oder Gespräche mit der Wirtschaft, um die Zusammenarbeit im Krisen- und Verteidigungsfall gezielt zu stärken.

Militärische Konflikte – Spannungs-, Zustimmungs-, Bündnis- und Verteidigungsfall

Um auf eine Verschärfung der internationalen Lage mit potenziellen Auswirkungen auf die sicherheitspolitische Lage des deutschen Staates reagieren zu können, sieht das Grundgesetz ein abgestuftes Verfahren zur Inkraftsetzung von Notstandsregelungen vor (siehe Abschnitt E1). Jede dieser Phasen – vom Zustimmungs- und Spannungsfall über den Bündnisfall bis hin zum Verteidigungsfall – hat unterschiedliche Auswirkungen auf Staat, Gesellschaft und Wirtschaft.

Für Unternehmen ist es daher wichtig, die Unterschiede zu kennen und mögliche Folgen für den eigenen Geschäftsbetrieb frühzeitig zu bedenken. Schon die Feststellung des Bündnisfalls kann beispielsweise dazu führen, dass Betriebsangehörige aus anderen NATO-Staaten aufgrund nationaler Meldevorschriften zurückgerufen werden und damit dem Unternehmen kurzfristig nicht mehr zur Verfügung stehen.

Ebenso kann bereits der Spannungsfall praktische Auswirkungen auf Unternehmen haben – etwa durch verstärkte Grenzkontrollen oder zeitweise Grenzschließungen, die Logistikketten beeinträchtigen oder die Verfügbarkeit von Mitarbeitenden in Grenzregionen einschränken können. Unternehmen sollten sich daher im Rahmen ihrer Krisenvorsorgeplanung mit diesen Szenarien auseinandersetzen und prüfen, wie sich Personal, Logistik und Produktion in solchen Situationen anpassen lassen.

III. Kernmaßnahmen: Was Unternehmen jetzt tun sollten

Die oberste Aufgabe der Geschäftsführung ist es, den Fortbestand des Unternehmens zu sichern. Dazu gehört, Risiken frühzeitig zu erkennen, zu vermeiden oder zu minimieren sowie Maßnahmen zur Stärkung der Resilienz zu prüfen und umzusetzen. Angesichts der aktuellen geopolitischen Lage bedeutet das auch, potenziell krisenrelevante Entwicklungen im Blick zu behalten und sich gezielt auf Störungen oder Ausfälle im operativen Geschäft, auf finanzielle oder wirtschaftspolitische Krisen sowie auf Image- und Reputationsrisiken vorzubereiten.

Im Folgenden werden elf zentrale Handlungsfelder für ein wirksames Risiko- und Krisenmanagement vorgestellt. Zu jedem Handlungsfeld finden Sie in den begleitenden Checklisten (siehe Anlage) konkrete Maßnahmenvorschläge. Der Fokus liegt dabei auf der Stärkung der unternehmerischen Resilienz, insbesondere mit Blick auf Szenarien der Zivilen Verteidigung. Die Umsetzung dieser Maßnahmen erhöht jedoch zugleich die Resilienz gegenüber anderen Risiken – ob bekannt oder unvorhersehbar. Die systematische Bearbeitung der Checklisten unterstützt Unternehmen dabei, ihre Vorsorgeschritte strukturiert zu planen, Fortschritte zu dokumentieren und Handlungsbedarfe gezielt zu erkennen.

3.1 Führung sicherstellen

Leitfragen: Wie kann Führung und Verantwortung im Unternehmen auch in Krisenzeiten sichergestellt werden? Welche Leitentscheidungen muss die Geschäftsführung treffen? Welche (Entscheidungs-)Kompetenzen werden einer Krisenorganisation übertragen?

Die Verantwortung für das Unternehmen liegt auch in Krisen, Not- und Katastrophenfällen bei der Unternehmensleitung. Sie trägt die Gesamtverantwortung für ein funktionierendes Krisenmanagement und damit für die Handlungsfähigkeit des Unternehmens in außergewöhnlichen Lagen.

Da Krisen meist komplex, dynamisch und mit hohem Koordinierungsaufwand verbunden sind, lassen sie sich nicht mit den üblichen Strukturen der Alltagsorganisation bewältigen. Für den Ernstfall sollte daher eine gesonderte Krisenorganisation eingerichtet werden – mit entsprechenden Ressourcen

5 Operationsplan Deutschland, https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland

und klar definierten Rollen und Zuständigkeiten. Der Leitung sollten die notwendigen Kompetenzen sowie Entscheidungsbefugnisse übertragen werden. Entscheidend ist zudem ein regelmäßiger Austausch zwischen Krisenorganisation und Unternehmensleitung, damit Entscheidungen schnell abgestimmt und wirksam getroffen werden können.

Vorgehen:
- Prüfen Sie, ob Krisen mit den bestehenden Strukturen bewältigt werden können oder ob eine eigene Krisenorganisation erforderlich ist.
- Legen Sie fest, wer im Krisenfall führt, wer entscheidet und wer informiert.
- Stellen Sie sicher, dass Führungsfunktionen und Entscheidungsbefugnisse klar geregelt sind.
- Richten Sie strukturierte Kommunikations- und Informationswege zwischen Unternehmensleitung und Krisenstab ein.

3.2 Gesetze und Regelungen vorab prüfen

Leitfragen: Welche Bereiche der Notstandsgesetzgebung betreffen das Unternehmen? Welche Herausforderungen, aber auch welche Möglichkeiten können sie für das Unternehmen haben?

Prüfen Sie regelmäßig Gesetze, Verordnungen sowie Standards im Bereich der Betriebsführung und der allgemeinen Unternehmenssicherheit. Das gehört zu den grundlegenden Aufgaben jeder Geschäftsleitung. Dabei sollten Sie nicht nur die gängigen Regelwerke des Unternehmensalltags berücksichtigen, sondern auch besondere Rechtsvorschriften (Notstandgesetze), die in Krisen- oder Verteidigungsfällen relevant werden können.

Hierzu zählen vor allem die Vorsorgegesetze, mit denen der Staat durch wirtschaftslenkende Maßnahmen auf friedenszeitliche Krisen reagiert – etwa auf Versorgungsengpässe im Transport- oder Logistikbereich. Darüber hinaus sind die sogenannten Sicherstellungsgesetze zu beachten, die erst im Spannungs-, Zustimmungs-, Bündnis- oder Verteidigungsfall Anwendung finden. Sie ermöglichen, die Versorgung von Bevölkerung und Streitkräften mit notwendigen Gütern und Dienstleistungen durch staatliche Eingriffe sicherzustellen. Gerade mit Blick auf die Anforderungen der Zivilen Verteidigung sind Regelungen für Unternehmen von besonderer Bedeutung.

Vorgehen:
- Verschaffen Sie sich einen Überblick über die relevanten Vorsorge- und Leistungsgesetze sowie über die Sicherstellungsgesetze.
- Prüfen Sie, welche Regelungen und Pflichten im Krisen- oder Verteidigungsfall Ihr Unternehmen betreffen könnten.

3.3 Lage erfassen und bewerten

Leitfragen: Wie können relevante Ereignisse für das Unternehmen beobachtet und Krisen frühzeitig erkannt werden? Welche Faktoren im Weltgeschehen sollten aktiv beobachtet werden?

Ein wirksames Risiko- und Krisenmanagement setzt ein aktuelles und verlässliches Lagebild voraus. Unternehmen sollten daher die für sie relevante Entwicklungen auf nationaler und internationaler Ebene systematisch beobachten. Gerade im Kontext der Zivilen Verteidigung ist eine kontinuierliche Betrachtung der internationalen sicherheitspolitischen Entwicklungen unerlässlich. Ziel ist es, potenziell gefährdenden Ereignisse und Entwicklungen frühzeitig zu erkennen, um rechtzeitig Anpassungsmaßnahmen einzuleiten und die Auswirkung möglicher Krisen zu begrenzen.

Ein gut strukturiertes Lagebild ermöglicht der Geschäftsführung einen schnellen Überblick über relevante Geschehnisse. Es sollte klare Indikatoren für aufziehende Krisen enthalten und deren mögliche Auswirkung auf den eigenen Betrieb sichtbar machen. Auf der Grundlage dieses individuellen Lagebilds hat das Unternehmen die aktuellen relevanten Ereignisse und Gefahren im Blick, deren Ergebnisse wiederum in die Risikobewertung einfließen.

Vorgehen:
- Etablieren Sie ein Monitoring relevanter nationaler und internationaler Entwicklungen, um Krisen frühzeitig zu erkennen.

3.4 Unternehmensinterne Vorbereitung und Vorplanung als Führungsaufgabe gestalten

Leitfragen: Welche Befugnisse und Ressourcen sind für die Umsetzung erforderlich? Was sind die wichtigsten Dienstleistungen, Produkte und Geschäftsprozesse des Unternehmens? Existieren Pläne, um die Betriebsfähigkeit auch im Ereignisfall sicherzustellen zu können?

Um in Krisen handlungsfähig zu bleiben, müssen Unternehmen sich frühzeitig mit der Planung und Vorbereitung von Maßnahmen zur Krisenbewältigung befassen. Die Geschäftsleitung trägt hierbei die Gesamtverantwortung: Sie sollte den Prozess initiieren, strategische Ziele einer Vorbereitung und Vorplanung auf unerwartete Ereignisse festlegen und einen Auftrag zur Ausplanung einschließlich eines Zeitrahmens für Implementierung und Umsetzung formulieren.

Für die operativen Umsetzung empfiehlt es sich, auf bereits bestehende Managementsysteme wie das Business Continuity Management aufzubauen und neue Planungsergebnisse dort zu integrieren. Gleichzeitig sollte ein Team gebildet werden, das den Prozess der konkrete Ausplanung und Umsetzung koordiniert. Dazu gehören beispielsweise eine Bestandsaufnahme der wichtigsten Geschäftsprozesse und Komponenten, die Analyse geschäftskritischer Lieferketten sowie die Prüfung von Redundanzen. So entsteht ein belastbarer Überblick über zeitkritische Abläufe und Ressourcen, die für die Aufrechterhaltung des Geschäftsbetriebs entscheidend sind.

Vorgehen:
- Identifizieren Sie (zeitkritische) Geschäftsprozesse und Komponenten Ihres Unternehmens.
- Erstellen Sie Pläne und Maßnahmen, um deren Aufrechterhaltung im Krisenfall sicherzustellen.
- Planen Sie hierfür ausreichend Personal ein.

3.5 Standortsicherheit und Objektschutz prüfen

Leitfragen: Wie muss das Betriebsgelände und der Zutritt zu diesem geschützt werden? Für welche Bereiche ist ein Grundschutz ausreichend und wo sind aufgrund besonders sensibler Bereiche zusätzliche Maßnahmen erforderlich?

Die physische Sicherheit des Standorts und betriebsrelevanter Objekte ist eine zentrale Voraussetzung für eine ununterbrochene Geschäftstätigkeit. Ziel ist es, den Standort vor den Auswirkungen von Unfällen, Sachbeschädigung, Einbruch, Diebstahl, unbefugtem Zutritt sowie vor Naturgefahren zu schützen. Die Standortsicherheit umfasst Maßnahmen, die die Resilienz gegenüber identifizierten Gefahren erhöhen und so Ausfälle oder Einschränkungen von Geschäftsprozessen und Dienstleistung verhindern. Die Auswahl der Schutzmaßnahmen erfolgt stets objekt- und standortspezifisch – in Abhängigkeit von Nutzung, ermittelten und bewerteten Risiken und dem angestrebten Sicherheitsniveau.

Vorgehen:
- Prüfen Sie das Betriebsgelände und die Anlagen und bewerten Sie den physischen Schutzbedarf.
- Treffen Sie geeignete Maßnahmen im Bereich des Perimeterschutzes, der Zutrittssicherung und der baulichen Härtung.[6]

3.6 Lieferketten aufrechterhalten

Leitfragen: Welche Lieferketten sind für die Geschäftsprozesse und Dienstleistungen des Unternehmens unverzichtbar? Sind diese Lieferketten durch bestimmte Krisen anfällig für Engpässe oder Ausfälle? Wo können Redundanzen geschaffen werden?

Lieferanten und Dienstleister tragen wesentlich zur Aufrechterhaltung der Funktionsfähigkeit eines Unternehmens bei, damit die eigenen Dienstleistungen oder Produkte dauerhaft bereitgestellt werden können. Störungen in der Lieferketten oder der Ausfall von Zulieferern und externen Dienstleistungen können unmittelbare oder zeitlich verzögerten Auswirkungen auf den Geschäftsbetrieb haben. Die Gründe hierfür sind vielfältig: kurzfristige Streiks in einer „Just-in-Time"-Wirtschaft, Grenzschließungen oder Betriebsausfälle etwa während der Covid-19-Pandemie, Engpässe bei Rohstoffen, zollpolitische Entscheidungen sowie Sanktionen gegenüber Staaten infolge politischer oder militärischer Konflikte. Zur Erhöhung der Versorgungssicherheit sollten mit Lieferanten und Dienstleistern Abmachungen zur Krisenvorsorge getroffen sowie – wo möglich – Lagerbestände aufgebaut werden.

Vorgehen:
- Analysieren Sie mögliche Schwachstellen in Ihren Lieferketten.
- Reduzieren Sie die Abhängigkeit von diesen Lieferketten.

3.7 Betriebsinterne Infrastruktur sicherstellen

Leitfragen: Sind die notwendigen Unterstützungsprozesse jederzeit verfügbar? Welche Auswirkungen hätte ein Ausfall dieser Unterstützungsprozesse? Wie kann ein Ausfall kompensiert werden?

Um die wichtigsten Geschäftsprozesse, Dienstleistungen und Anlagen des Unternehmens aufrechtzuerhalten, ist die durchgängige Verfügbarkeit von Energie, Kommunikation, Daten und Informationen unerlässlich. Der Ausfall dieser unterstützenden Systeme kann plötzlich eintreten – ohne oder mit nur geringer Vorwarnzeit. Beispiele hierfür sind der Stromausfall in Berlin-Köpenick 2019 und in Spanien 2025, Cyberangriffe auf das Universitätsklinikum Essen 2016 oder auf einen auf KMU spezialisierten IT-Dienstleister in Lübeck 2024 sowie die mutwillige Zerstörung von Kommunikationskabeln. Eine unterbrechungsfreie Stromversorgung, hochverfügbare

6 Härtung: Erhöhung der Widerstandsfähigkeit von Gebäuden gegenüber äußeren Einwirkungen durch bauliche Ertüchtigungsmaßnahmen am, im und um das Gebäude.

IT-Systeme und Telekommunikation sowie eine zuverlässige Wasserversorgung sind entscheidend für die Funktionsfähigkeit der betriebsinternen Infrastruktur – und damit für die Aufrechterhaltung des Geschäftsbetriebs.

Vorgehen:

- Sichern Sie die für die Betriebsfähigkeit erforderlichen Versorgungsinfrastrukturen und Unterstützungsprozesse ab und investieren Sie in notwendige Redundanzen.

3.8 Personalplanung sichern und Einsatzfähigkeit erhalten

Leitfragen: Welches Personal könnte im Ereignisfall ausfallen? Wie kann die Personalplanung an unterschiedliche Szenarien angepasst werden? Welche Schulungen und Maßnahmen erhöhen die Sicherheit der Mitarbeitenden?

Die Covid-19-Pandemie hat verdeutlicht, wie entscheidend eine strukturierte Personalplanung, eine kontinuierliche Übersicht über die personelle Verfügbarkeit und eine belastbare Personaleinsatzplanung sind, insbesondere in zeitkritischen Geschäftsprozessen für die Fortführung der Unternehmenstätigkeit. Auch im Szenario einer Zivilen Verteidigung kann es zu erheblichen Personalengpässen kommen – etwa wenn Mitarbeitende in Katastrophenschutzorganisationen tätig sind, Freiwillige und Angehörige der Reserve zu Wehrübungen herangezogen werden oder eine allgemeine Wehrpflicht wieder in Kraft tritt.

Um die Betriebsfähigkeit sicherstellen zu können, sind frühzeitig Maßnahmen zur Vorbereitung auf mögliche Personalausfälle treffen. Diese sollten sowohl das eigene Personal als auch Beschäftigte von Dienstleistern und Dritten einbeziehen, etwa durch klare vertragliche Regelungen zur Sicherstellung von Leistungen im Krisenfall. Ebenso sind Fragen des Arbeits- und Gesundheitsschutzes einschließlich der geschützten Unterbringung von Mitarbeitenden in Schlüsselfunktionen intern zu regeln. Unternehmen können zudem ihre Beschäftigten in der privaten Vorsorge unterstützen, um deren Sicherheit und Einsatzfähigkeit auch in Ausnahmesituationen zu stärken.

Vorgehen:

- Prüfen Sie Ihren Personalbestand auf mögliche Ausfälle im Ereignisfall. Berücksichtigen Sie insbesondere die gesetzlichen Regelungen in der Notstandsgesetzgebung.
- Erstellen Sie Pläne, um kritische Geschäftsprozesse auch im Ereignisfall mit Personal versorgen zu können.

3.9 Spionage und Sabotage verhindern

Leitfragen: Kann das Unternehmen grundsätzlich Ziel von Spionage oder Sabotage sein? Wie kann ich es vor Ausspähung und dem Abfluss von wichtigen Informationen von innen und von außen schützen?

Nicht nur große Konzerne, sondern auch kleine und mittlere Unternehmen geraten zunehmend ins Visier von Spionage und Sabotage – sei es durch kriminelle oder politisch motivierte Personen von außen oder durch bewusst oder unbewusst handelnde Personen im eigenen Umfeld, etwa Mitarbeitende, Kundschaft oder Dienstleister. Die Motive sind abhängig vom Geschäftsmodell vielfältig: innovative Produkte oder Dienstleistungen, die Rolle als Zulieferer für eigentliche Zielunternehmen oder schlicht geringes Risikobewusstsein und begrenzte Sicherheitsressourcen. Mitunter werden Unternehmen als „Beifang“ auch zufällig Opfer großflächiger Cyberangriffe. Die Folgen solcher Sabotage- oder Spionageangriffe, die sich oft schleichend und unbemerkt entwickeln, können verheerend sein – bis hin zur existenziellen Gefährdung des Unternehmens.

Vorgehen:

- Berücksichtigen Sie potenzielle Gefährdungen durch Ausspähung, Manipulation oder gezielten Abfluss von Informationen und integrierend Sie diese in Ihr Lagebild.
- Setzen Sie empfohlene Maßnahmen zum Spionage- und Sabotageschutz – etwa des Verfassungsschutzes – konsequent um.

3.10 Interne und externe Kommunikation aufrechterhalten

Leitfragen: Wie kann auch in Krisen Vertrauen in das Unternehmen aufrechterhalten werden? Was sind Kernbotschaften des Unternehmens in einer Krise? Welche Informationsbedürfnisse bestehen bei Mitarbeitenden und Externen?

Ein wesentlicher Bestandteil des Krisenmanagements ist die Kommunikation nach innen und außen. Gerade in unsicheren Lagen kann eine offene, transparente und zielgerichtete Kommunikation Stabilität geben, Verlässlichkeit schaffen und Vertrauen stärken.

Unternehmensintern werden regelmäßig informierte Mitarbeitende Maßnahmen, die sie unmittelbar betreffen, eher akzeptieren und Veränderungen in den Abläufen besser nachvollziehen können. Ergänzende handlungsleitende Empfehlungen für das persönliche Umfeld der Mitarbeitenden können zusätzliche Sicherheit schaffen und die Einsatzfähigkeit des Personals stärken. Nach außen kann eine aktive Krisenkommunikation dazu beitragen, Kundenbindung zu sichern, die Zusammenarbeit durch frühzeitige Absprachen unter anderem mit Zulieferern zu erleichtern und die Sichtbarkeit beispielsweise gegenüber Behörden zu erhöhen.

Vorgehen:

- Identifizieren Sie die relevanten Zielgruppen für die interne und externe Kommunikation.
- Definieren Sie Ziele Ihrer Krisenkommunikation.
- Bereiten Sie Kommunikationsinhalte für den Ernstfall vor.

3.11 Chancen erkennen und Geschäftspotenziale im Krisenfall nutzen

Leitfragen: Welche Produkte oder Dienstleistungen könnten im Rahmen der Zivilen Verteidigung benötigt oder verstärkt nachgefragt werden? Eröffnen Geschäftsprozesse des Unternehmens Möglichkeiten, Produkte oder Dienstleistungen in der Krise an neue Bedarfe anzupassen?

In sicherheitspolitischen Krisen müssen nicht nur bestehende Geschäftsprozesse priorisiert und angepasst werden. Gesellschaft und Sicherheitskräfte entwickeln oft neue Bedarfe für Produkte und Dienstleistungen, die Unternehmen als Chance für neue Geschäftsmodelle nutzen können. Ein Beispiel: Während der Covid-19-Pandemie haben viele Unternehmen ihre Produktion auf spezifische Produkte wie Desinfektionsmittel oder Infektionsschutz umgestellt oder neue Dienstleistungen im Rahmen des Social Distancing angeboten. Wer solche Potenziale frühzeitig erkennt und Wertschöpfungsprozesse anpasst, hat die Chance, gut durch die Krise zu kommen.

Vorgehen:

- Identifizieren Sie potenzielle neue Geschäftsfelder – kurz-, mittel- und langfristig.
- Bereiten Sie die Umsetzung dieser neuen Angebote vor.

Fazit

Eine gute Vorbereitung auf Katastrophen und Krisen kostet zwar Zeit und Ressourcen, sie ist aber niemals vergeblich. Unternehmen, die sich aktiv mit ihren Risiken auseinandersetzen und in Systeme und Maßnahmen zur Krisenbewältigung investieren, können ihre Geschäftsmodelle und Wertschöpfungsprozesse an neue Rahmenbedingungen anpassen, Mitarbeitende kompetent durch Krisen führen und sind besser gerüstet, auch unerwartete Ereignisse zu bewältigen.

Wer vorbereitet ist, überlebt nicht nur, sondern kann Krisen als Chance begreifen: mit klaren Szenarien, einer robusten Personal- und Lieferkettenplanung sowie dem Blick für neue Geschäftspotenziale. So stärken Unternehmen ihre Resilienz – und können auch in unsicheren Zeiten stabil und erfolgreich handeln.

Anhang

Militärische Konflikte – Spannungs-, Zustimmungs-, Bündnis- und Verteidigungsfall

Im Falle eines äußeren Notstands mit militärischem Konfliktpotential verfügt der Staat über grundgesetzlich abgesicherte differenzierte Reaktionsmöglichkeiten, die abgestuft auf unterschiedliche Intensitäten einer Gefahren- oder Spannungslage reagieren. Das Grundgesetz unterscheidet dabei vier Stufen, um auf eine eskalierende Bedrohungslage zu reagieren: den Zustimmungsfall, den Spannungsfall, den Verteidigungsfall sowie den Bündnisfall, der je nach Lage auf unterschiedlichen Stufen eintreten kann.

Spannungsfall (Artikel 80a Grundgesetz)

Der Spannungsfall ist – anders als der Verteidigungsfall – im Grundgesetz nicht definiert. Er ist dem Verteidigungsfall vorgelagert und beschreibt eine Situation, in der eine hinreichende Wahrscheinlichkeit besteht, dass eine außenpolitische Konfliktlage eskaliert und es zu einem bewaffneten Angriff auf das Bundesgebiet kommt. Eine das Staatwesen derart gefährdende Spannungslage wird vom Deutschen Bundestag mit einer Zweidrittelmehrheit der abgegebenen Stimmen festgestellt. Damit können Notstandsgesetze wie das Arbeits- und weitere Sicherstellungsgesetze in Kraft gesetzt („entsperrt“) werden. Zudem kann der Einsatz der Streitkräfte im Innern zugelassen werden, etwa zum Schutz lebens- und verteidigungswichtiger Infrastruktur oder zur Regelung des Verkehrs.

Zustimmungsfall (Artikel 80 a Absatz 1 Satz 1 Grundgesetz)

Der Zustimmungsfall ist eine Alternative zum Spannungsfall. Im Unterschied zur allgemeinen Freisetzung des Notstandsrechts infolge der Feststellung des Spannungsfalls ermöglicht der Zustimmungsfall eine dosierte und parlamentarisch kontrollierte Freigabe einzelner Bestimmungen des Notstandsrechts. Auf dieser Grundlage kann der Deutsche Bundestag im Einzelfall der Anwendung konkreter Notstandsregelungen – etwa einzelner Sicherstellungs- und Vorsorgegesetze – mit einfacher Mehrheit zustimmen (ausgenommen sind Verpflichtungen nach Artikel 12 Absatz 3 und Artikel 12a Absatz 6 Satz 1 Grundgesetz).

Bündnisfall (Artikel 80a Absatz 3 Satz 1 Grundgesetz)

Der Bündnisfall ist separat von den nationalen Vorstufen des Verteidigungsfalls geregelt. Er tritt ein, wenn das zuständige NATO-Organ einen bewaffneten Angriff gegen eine Vertragspartei feststellt, koordinierte Verteidigungsmaßnahmen beschließt und die Bundesregierung diesem NATO-Beschluss zustimmt.

Im Bündnisfall reicht ein Beschluss der Bundesregierung, um verteidigungsvorbereitende Rechtsvorschriften des einfachen Rechts – etwa Sicherstellungs- oder Vorsorgegesetze – zu entsperren. Ziel ist es, Vorbereitungsmaßnahmen zur Herstellung der Verteidigungsbereitschaft im Rahmen des NATO-Bündnisses zu aktivieren. Die Entsperrung verfassungsrechtlich geregelter Maßnahmen, wie der Einsatz von Streitkräften im Innern (Artikel 87a Absatz 3 Grundgesetz) oder Eingriffe in die Berufsfreiheit durch Dienstverpflichtungen (Artikel 12a Grundgesetz), ist nicht möglich.

Verteidigungsfall (Artikel 115a Grundgesetz)

Der Verteidigungsfall wird festgestellt, wenn das Bundesgebiet mit Waffengewalt angegriffen wird oder ein solcher Angriff unmittelbar droht. Dies erfolgt durch den Deutschen Bundestag mit einer Zweidrittelmehrheit der abgegebenen Stimmen, mindestens jedoch mit der absoluten Mehrheit der Mitglieder. Der Bundesrat muss der Feststellung mit absoluter Mehrheit der Stimmen zustimmen. Der Antrag auf Feststellung wird von der Bundesregierung gestellt.

Ausgewählte Gesetze der Notstandsgesetzgebung

Vorsorge- und Sicherstellungsgesetze sind Bundesgesetze, die dem Ziel dienen, besondere Gefahrenlagen zu bewältigen. Sie unterscheiden sich insbesondere im Anwendungsbereich: Vorsorgegesetze greifen in friedenszeitlichen Gefahrenlagen, Sicherstellungsgesetze kommen im äußeren Notstand zum Einsatz.

- **Vorsorgegesetze** sind in besonderen Gefahrenlagen wie Naturkatastrophen oder schweren Unglücksfällen/Großschadenslagen anwendbar, sofern die Versorgung etwa mit Nahrungsmitteln oder Transportkapazitäten auf anderem Weg nicht sichergestellt werden kann. Es handelt sich im Wesentlichen um wirtschaftslenkende Maßnahmen, die zeitlich befristet wirtschaftsrechtliche und wettbewerbliche Regelungen außer Kraft setzen können.
- **Sicherstellungsgesetze**, wie etwa das Wirtschafts- oder Energiesicherstellungsgesetz, dienen der Grundversorgung der Bevölkerung und der Streitkräfte mit lebens- und verteidigungswichtigen Gütern und Dienstleistungen verschiedener Wirtschaftsbereiche in einem äußeren Notstand. Sie gehen über wirtschaftslenkende Maßnahmen hinaus: Zusätzlich können sie einige Grundrechte, wie Freizügigkeit oder Unverletzlichkeit der Wohnung, vorübergehend einschränken.

Sicherstellungsgesetze dürfen grundsätzlich nur angewendet werden, wenn die Voraussetzungen des Zustimmungs-, Spannungs-, Verteidigungs- oder des Bündnisfalls erfüllt sind (Anwendungsvorbehalte nach Artikel 80a, 115a Grundgesetz). Sie wurden zwar vom Deutschen Bundestag verabschiedet und sind in Kraft, bleiben jedoch „gesperrt“, bis eine der genannten Krisensituationen in der Regel durch parlamentarischen Beschluss mit Zweidrittelmehrheiten festgestellt wird.

Nachfolgend werden ausgewählte Sicherstellungsgesetze mit branchenübergreifender Bedeutung vorgestellt und ihre Ziele, Anwendungsbereiche sowie mögliche Auswirkungen auf die Wirtschaft skizziert.

Bundesleistungsgesetz (BLG), 1956

Ziel	Sicherstellung des Bedarfs an Leistungen vielfältiger Art (u. a. bewegliche Sachen, bauliche Anlagen, unbebaute Grundstücke, freie Flächen, Funk- und Fernsprechanlagen, Werkleistungen)
Regelungsgegenstand	**Anforderung von Leistungen nach § 1, u. a.:** • für Zwecke der Verteidigung • zur Erfüllung der Verpflichtungen des Bundes aus zwischenstaatlichen Verträgen über die Stationierung und die Rechtsstellung von Streitkräften auswärtiger Staaten im Bundesgebiet • zur Unterbringung von Personen oder einer wegen Inanspruchnahme von Grundstücken für die o. g. Zwecke notwendigen Verlegung von Betrieben und öffentlichen Einrichtungen **Regelungen im Rahmen von Manövern oder Übungen (§§ 66–75):** • Duldung von Grundstücksüberquerung, -benutzung, -sperrung (in definierten Fällen nur mit Einwilligung der Berechtigten) • Bereitstellung der Unterbringung von Dienststellen, Personen, Tieren, Fahrzeugen, Waffen sowie Gerät
Relevanz für die Wirtschaft	**Beispielsweise:** • Verpflichtung zur Erbringung der in (§ 2 konkretisierten Leistungen) • Duldung der Maßnahmen nach dem „Manöverrecht“

Gesetz über die Sicherstellung von Leistungen auf dem Gebiet der gewerblichen Wirtschaft sowie des Geld- und Kapitalverkehrs – Wirtschaftssicherstellungsgesetz (WiSiG), 1965

Ziel	Sicherstellung der für Zwecke der Verteidigung erforderlichen Versorgung u. a. mit Gütern und Dienstleistungen, insbesondere zur Deckung des Bedarfs der Zivilbevölkerung und der Streitkräfte
Regelungsgegenstand	**Ermächtigung zum Erlass von Rechtsverordnungen:** • über Güter und Dienstleistungen der gewerblichen Wirtschaft sowie von Werkleistungen zu Instandsetzungen und Instandhaltung, Herstellung und Veränderung von Bauwerken und technischen Anlagen, von der Produktion über die Zulieferung bis zur Verteilung an Endverbrauchende • zum Erlass von Buchführungs- und Meldepflichten hinsichtlich der Güter und Leistungen, über die nach § 1 BLG Vorschriften erlassen werden können, sowie hinsichtlich der Leistungsfähigkeit von Betrieben der gewerblichen Wirtschaft • von Vorschriften über die Lagerung und Vorratshaltung der in § 1 BLG genannten Waren und Erzeugnissen, soweit dies erforderlich ist, um eine ausreichende Versorgung sicherzustellen
Relevanz für die Wirtschaft	**Beispielsweise:** • ggf. Umsetzung von Vorschriften über Lagerung, Vorratshaltung • ggf. Umsetzung von Buchführungs- und Meldeverpflichtungen über gelagerte Waren

Gesetz zur Sicherstellung von Arbeitsleistungen für Zwecke der Verteidigung einschließlich des Schutzes der Zivilbevölkerung – Arbeitssicherstellungsgesetz (ASG), 1968

Verordnung über die Feststellung und Deckung des Arbeitskräftebedarfs nach dem Arbeitssicherstellungsgesetz (ArbSv), 1989

Ziel	Sicherstellung von Arbeitsleistungen für Zwecke der Verteidigung einschließlich des Schutzes der Zivilbevölkerung
Regelungs-gegenstand	**Regelungen zur Deckung eines im äußeren Notstand entstehenden Personalbedarfs bei der Wahrnehmung lebens- und verteidigungswichtiger Aufgaben durch Einschränkung des Grundrechts der Berufsfreiheit nach Artikel 12 Grundgesetz:** • Einschränkung des Rechts zur Beendigung von Arbeitsverhältnissen (Kündigung/Entlassung) in den in § 4 gelisteten Behörden, Unternehmen und Einrichtungen • Einschränkung des Rechts auf freie Berufswahl durch Verpflichtung in Arbeitsverhältnisse (Wehrpflichtige: generell in den in § 4 gelisteten Behörden, Unternehmen und Einrichtungen, Frauen: nur Sanitätsdienste, Heilwesen, Lazarette)
Relevanz für die Wirtschaft	**Beispielsweise:** • Einschränkungen des Rechts zur Beendigung von Arbeitsverhältnissen durch Kündigung der Arbeitnehmenden • Möglichkeit der in § 4 ASG gelisteten Unternehmen und Einrichtungen, nach § 1 Absatz 1 der ArbSv einen Ersatz- und Zusatzbedarf an Arbeitnehmenden festzustellen und bei der zuständigen Agentur für Arbeit anzumelden

Gesetz zur Sicherstellung des Verkehrs – Verkehrssicherstellungsgesetz (VerkSiG), 1965

Ziel	• Sicherstellung von zum Zweck der Verteidigung erforderlichen lebenswichtigen Verkehrsleistungen, insbesondere zur Versorgung der Zivilbevölkerung und der Streitkräfte • Bestmögliche Ausnutzung vorhandener Transportkapazitäten e
Regelungs-gegenstand	**Ermächtigung zum Erlass von Rechtsverordnungen u. a. über:** • die Benutzung und den Betrieb einschließlich der Ausrüstung von Verkehrsmitteln, -wegen, -anlagen und -einrichtungen • die Lenkung, Beschleunigung und Beschränkung der Beförderung von Personen und Gütern, des Umschlags und der An- und Abfuhr sowie über die Behandlung von Gütern im Verkehr • den Bau, die Instandsetzung und die Unterhaltung von Verkehrswegen, -anlagen und -einrichtungen • die Zulassung, die personelle Besetzung und die Reihenfolge der Instandsetzungen von Verkehrsmitteln sowie über die technischen Anforderungen an Verkehrsmittel • die Begründung, Erweiterung oder Beschränkung von Betriebs- und Beförderungspflichten
Relevanz für die Wirtschaft	**Relevanz für Verkehrsunternehmen, Speditionen etc.:** • Auswirkungen aufgrund verkehrslenkender Maßnahmen bei der Beförderung von Personen, Gütern und im Güterumschlag

Weiterführende Informationen (Auswahl)

Strategien, Konzepte, Dokumente

Gesamtverteidigung

- Rahmenrichtlinien für die Gesamtverteidigung, Beschluss des Bundeskabinetts vom 5. Juni 2024

https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/RRGV.html

- Bundesministerium des Innern (Hrsg.), Konzeption Zivile Verteidigung, Kabinettsbeschluss vom 24. August 2016

https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/zivil-und-katastrophenschutz/konzeption-zivile-verteidigung/konzeption-zivile-verteidigung-node.html

- Bundesministerium der Verteidigung (Hrsg.): Verteidigungspolitische Richtlinien 2023

https://www.bmvg.de/de/aktuelles/verteidigungspolitische-richtlinien-2023-veroeffentlicht-5701338

- Operatives Führungskommando der Bundeswehr (Hrsg.): Operationsplan Deutschland

https://www.bundeswehr.de/de/organisation/operatives-fuehrungskommando-der-bundeswehr/auftrag-und-aufgaben/operationsplan-deutschland

https://www.bundeswehr.de/resource/blob/5920008/5eb62255741addec3f38d49a443d0282/booklet-operationsplan-deutschland-data.pdf

Handreichungen

Risiko- und Krisenmanagement, Krisenvorsorge, Krisenmanagement

- Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden, Berlin 2011

https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI07326-kritis-leitfaden.html

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Vorsorgen für Krisen und Katastrophe, Bonn 2025

https://www.bbk.bund.de/DE/Warnung-Vorsorge/Vorsorge/Ratgeber-Checkliste/ratgeber-checkliste_node.htmlStandortsicherheit

- Bundesministerium des Innern, Deutsches Institut für Normung e.V. (Hrsg.): DIN SPEC 14027 – Corporate Security – Anforderungen zur Stärkung physischer Resilienz von Organisationen. Berlin 2026

https://www.dinmedia.de/de/technische-regel/din-spec-14027/400565136

Unternehmensinterne Infrastruktur

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Notstromversorgung in Unternehmen und Behörden, Bonn 2024

https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-13-notstromversorgung-unternehmen-behoerden.pdf?__blob=publicationFile&v=15IT-Sicherheit

- Bundesamt für Sicherheit in der Informationstechnik: Kleine und mittlere Unternehmen. Informationen und Hilfestellungen für KMU

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html

Sabotage/Spionage

- Bundesministerium für Wirtschaft und Energie: Themenportal Geheim- und Sabotageschutz in der Wirtschaft

https://www.bmwk-sicherheitsforum.de/start/

- Initiative Wirtschaftsschutz

https://www.wirtschaftsschutz.info/DE/Home/home_node.html

- Ministerium des Innern des Landes Nordrhein-Westfalen (Hrsg.): Wirtschaftsspionage – So schützen Sie Ihr Unternehmen, Düsseldorf 2022

https://www.im.nrw/system/files/media/document/file/broschuere_wirtschaftsspionage_so_schuetzen_sie_ihr_unternehmen_nrw_.pdf

Krisenkommunikation

- Bundesministerium des Innern (Hrsg.): Leitfaden Krisenkommunikation, Berlin 2014

https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI08313-leitfaden-krisenkommunikation.html

Angebote

- Schulungsangebot der HKBiS: Notfall- und Krisenmanagement IHK

https://hkbis.de/kurs/notfall-und-krisenmanagement-ihk/

Checklisten für die Geschäftsführung

Nutzen Sie diese elf Checklisten als praktische Hilfe, um Ihr Unternehmen gezielt auf Krisen und Katastrophen vorzubereiten. Der Fokus liegt auf Ereignisfällen der Zivilen Verteidigung. Viele der vorgeschlagenen Maßnahmen tragen jedoch auch dazu bei, Ihr Unternehmen gegen andere Szenarien krisenfest zu machen – und damit die allgemeine Resilienz zu stärken.

Wenn Ihr Unternehmen bereits ein Risiko- und Krisenmanagement, eine Notfallplanung oder ein Business Continuity Management aufgesetzt hat, können Sie die Checklisten leicht intergieren und bei Bedarf gezielt ergänzen. Sie dienen als praktische Arbeitsgrundlage und helfen dabei, vorhandene Strukturen zu überprüfen und weiterzuentwickeln.

Bitte beachten Sie: Die Checklisten sind nicht abschließend. Ergänzen oder aktualisieren Sie diese regelmäßig – insbesondere nach Übungen, realen Ereignissen oder betrieblichen Veränderungen. So bleiben ihre Planungen wirksam. Einzelne Checklisten oder Teilbereiche können Sie an zuständige Mitarbeitende zur Umset-zung delegieren. Die Gesamtverantwortung für die Umsetzung der Maßnahmen sollte jedoch klar in einer Hand liegen.

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
1. Führung sicherstellen			
1a	Überlegen Sie, welche Aufgaben im Rahmen der Vorbereitung auf und Bewältigung von Krisen durch die Geschäftsführung selbst wahrgenommen werden müssen und welche Aufgaben delegiert werden sollen.		
1b	Benennen Sie eine verantwortliche Person oder richten Sie eine Organisationseinheit (z. B. einen Krisenstab) für die Krisenvorbereitung ein und legen Sie deren Funktionen sowie die Leitungsrolle fest (➔ Checkliste 4a zur Vorplanung). *Hinweis: Die für die Vorbereitung zuständige Organisationseinheit kann zugleich Aufgaben der Krisenbewältigung übernehmen.*		
1c	Prüfen Sie, welche Kompetenzen die Leitung der Organisationseinheit benötigt, um kritische Dienstleistungen und Prozesse (➔ Checkliste 4a zur Vorplanung) im Ereignisfall aufrechterhalten zu können.		
1d	Kommunizieren Sie Aufgaben, Zuständigkeiten und Befugnisse der Krisenorganisation innerhalb des Unternehmens (➔ Checkliste 10b zur Kommunikation).		
...	...		
2. Gesetze prüfen			
2a	Halten Sie Gesetze, Standards, Regelwerke etc. zur Unternehmenssicherheit auf dem aktuellen Stand.		
2b	Machen Sie sich mit den Vorsorge- und Sicherstellungsgesetzen vertraut.		
2c	Prüfen Sie, welche Auswirkungen die geltenden Gesetze auf Ihren Betrieb haben können, wenn es zum Ereignisfall kommt.		
2d	Etablieren Sie Zuständigkeiten und Pläne, wie diese Anforderungen, wenn es zum Ereignisfall kommt, umgesetzt werden.		
2e	Arbeiten Sie mit Behörden, Organisationen im Zivil- und Katastrophenschutz sowie anderen Stellen zusammen, sollten diese auf Sie zukommen.		
...	...		

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
3. Lagebild erfassen			
3a	Setzen Sie eine Lagebeobachtung auf – personell, technisch und organisatorisch. *Hinweis: Beauftragen Sie alternativ Dienstleister, die zielgerichtet Informationen beisteuern oder aufbereiten können.*		
3b	Identifizieren Sie für den Betrieb wichtige Faktoren, die es zu beobachten gilt. *Hinweis: Hierzu zählen auch die Sanktions- und Zollpolitik, Verfügbarkeiten der Lieferketten und Reiserestriktionen.*		
3c	Identifizieren Sie potenzielle Quellen, die Informationen der geopolitischen Entwicklung (möglichst branchenbezogen) bewerten bzw. diese Bewertung ermöglichen.		
3d	Prüfen Sie diese Quellen regelmäßig und bewerten Sie Ihre eigene Betroffenheit, z. B. für Ihre Branche, Ihre Lieferkette, Ihre Wertschöpfung. *Hinweis: Nutzen Sie alternativ entsprechende externe Dienste, z. B. der Branchenverbände.*		
...	...		
4. Unternehmensinterne Vorbereitung und Vorplanung			
4a	Halten Sie Gesetze, Standards, Regelwerke etc. zur Unternehmenssicherheit auf dem aktuellen Stand.		
4b	Machen Sie sich mit den Vorsorge- und Sicherstellungsgesetzen vertraut.		
4c	Prüfen Sie, welche Auswirkungen die geltenden Gesetze auf Ihren Betrieb haben können, wenn es zum Ereignisfall kommt.		
4d	Etablieren Sie Zuständigkeiten und Pläne, wie diese Anforderungen, wenn es zum Ereignisfall kommt, umgesetzt werden.		
4e	Arbeiten Sie mit Behörden, Organisationen im Zivil- und Katastrophenschutz sowie anderen Stellen zusammen, sollten diese auf Sie zukommen.		
4f	Setzen Sie Pläne auf, wie diese Prozesse geschützt und/oder wiederhergestellt werden können.		
4g	Überlegen Sie, welche Maßnahmen notwendig sind, um die Betroffenheit des eigenen Unternehmens zu reduzieren; z. B. Kontakt zu alternativen Lieferanten, Einberufung des Krisenstabs (Feststellung der Betroffenheit ➔ Checkliste 3b zum Lagebild).		
4h	Prüfen Sie, ob es Netzwerke zwischen Unternehmen gibt, die Ihnen in der Umsetzung mit Informationen, Standardisierungen und Erfahrungen weiterhelfen können (z. B. durch die IHKs, Branchenverbände etc.).		
...	...		
5. Standortsicherheit und Objektschutz			
5a	Überlegen Sie, welche Maßnahmen Ihr Betriebsgelände sicherer begrenzen und schützen können (Umzäunung, Kameraüberwachung, Beleuchtung oder ähnlich anerkannte technische Maßnahmen). *Hinweis: Die nachfolgenden Maßnahmenvorschläge dieser Checkliste können sich auch an die beauftragte Person bzw. Organisationseinheit (➔ Checkliste 4a) richten.*		

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
5b	Konzipieren Sie mögliche Barrieren gegen potenzielle Angriffe und den Einfluss von Naturgefahren auf das Betriebsgelände (bauliche Anlagensicherung).		
5c	Überprüfen Sie, ob Außenwände und Dach so konstruiert und instandgehalten sind, dass sie dem Eindringen von außen standhalten.		
5d	Überprüfen Sie, ob das Gelände einen Wachschutz bzw. Kontrollgänge benötigt.		
5e	Stellen Sie sicher, dass Zugänge und Zutrittsstellen zu Räumlichkeiten, Anlagen und Gebäuden den orts- und infrastrukturgegebenen Möglichkeiten angepasst sowie durch physische Zutrittskontrollen gesichert und überwacht werden.		
5f	Sofern möglich, trennen Sie kritische Einrichtungen, Anlagen und Dienstleistungen von öffentlich zugänglichen Bereichen (➔ Checkliste 4a–c zur Identifizierung).		
5g	Legen Sie im Rahmen der Zutrittsregelung fest, wie der Zutrittsschutz bei Einschränkungen, Unterbrechungen und/oder Vorfällen sichergestellt werden kann.		
5h	Führen Sie für Externe (Besuch, Lieferanten, Dienstleister) eine Steuerung ein, die an die jeweilige Sicherheitszone sowie die orts- und infrastrukturgegebenen Möglichkeiten angepasst ist (Identifizierung, Kontrolle der Zu-/Abgänge etc.).		
5i	Prüfen Sie den besonderen Schutz von kritischen Anlagen oder kritischen physischen Komponenten (➔ Checkliste 4c zur Identifizierung).		
5j	Prüfen Sie, ob Räumlichkeiten mit kritischen Anlagen oder kritischen physischen Komponenten einer besonderen Härtung – auch zum Schutz des Personals – bedürfen.		
...	...		
6. Lieferketten aufrechterhalten			
6a	Sammeln Sie alle Meldungen über mögliche Lieferengpässe (➔ Checkliste 3 zum Lagebild), werten Sie diese mit Blick auf die Relevanz für Ihre Geschäftsprozesse aus und berücksichtigen Sie diese Informationen und Auswertungen im Lagebild.		
6b	Legen Sie einen besonderen Fokus auf wirtschaftlich relevante Krisenregionen (z. B. Osteuropa, Taiwan, China, Südamerika) sowie auf wirtschaftliche bzw. politische Entscheidungen mit Auswirkungen auf die Lieferkette, z. B. in Zollfragen. Analysieren Sie alle Verbindungen Ihres Unternehmens in und zu diesen Regionen..		
6c	Klären Sie mit Lieferanten, wie und in welchem Umfang Lieferungen auch im Krisenfall aufrechterhalten werden können.		
6d	Schließen Sie zusätzliche Service Level Agreements (SLA), um die Lieferung im Rahmen von besonderen Ereignissen zu regeln.		
6e	Ergänzen Sie vertraglichen Vereinbarungen im Bedarfsfall um Vertraulichkeits- und Geheimhaltungsklausel zum Schutz sensibler Informationen.		
6f	Reduzieren Sie Abhängigkeiten von „Just-in-Time"-Lieferketten.		
6g	Investieren Sie in sichere Lagerhaltung (➔ Checkliste 5 zur Standortsicherheit) und alternative Transportwege.		

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
6h	Prüfen Sie ggf. Möglichkeiten einer betriebsübergreifenden Beschaffung und Lagerhaltung.		
6i	Klären Sie, ob für besonders zeitkritische Produkte und Dienstleistungen (➔ Checkliste 4a, b, d zur Identifizierung) Vertragsabschlüsse mit weiteren Lieferanten und Dienstleistern möglich sind und ob die Bereitstellung unabhängig von den primären Lieferanten und Dienstleistern erfolgt.		
6j	Prüfen Sie, ob und inwieweit Produkte und Dienstleistungen externer Lieferanten im Bedarfsfall auch im eigenen Betrieb bereitgestellt werden können.		
...	...		
7. Sicherstellung der Infrastruktur			
7a	Prüfen Sie die Anschaffung von Notstromaggregaten. *Hinweis: Notstromaggregate sollten so dimensioniert sein, dass sie kritische Systeme und Prozesse für mindestens einige Stunden versorgen können, im besten Fall für 48 bis 72 Stunden. Dazu gehören in der Regel die IT-Infrastruktur, wichtige Fertigungslinien und kritische Kühlketten.*		
7b	Klären Sie Möglichkeiten einer Treibstoffversorgung. *Hinweis: Das kann die Lagerung von Treibstoff auf dem eigenen Gelände sein oder auch ein Zusammenschluss mehrerer Unternehmen, vertragliche Vereinbarungen mit Treibstofflieferanten etc..*		
7c	Sichern Sie sensible Bereiche durch eine unterbrechungsfreie Stromversorgung (USV) *Hinweis: Die USV schützt empfindliche Elektronik vor den sofortigen Auswirkungen eines Stromausfalls und überbrückt die Zeit, bis der Notstromgenerator anspringt. Für kritische Datenzentren oder Serverräume sollte das USV-System ausreichend dimensioniert sein, um einen nahtlosen Betrieb zu ermöglichen.*		
7d	Testen Sie Kommunikationswege (normal und redundant) unternehmensintern mit dem Personal im In- und Ausland.		
7e	Testen Sie Kommunikationswege (normal und redundant) mit Zulieferern, Dienstleistern, Sicherheitsunternehmen etc.		
7f	Testen Sie Kommunikationswege (normal und redundant) mit der Kundschaft.		
7g	Beschäftigen Sie sich mit IT-Risiken und den möglichen Auswirkungen eines Angriffs oder Ausfalls auf Ihr Unternehmen.		
7h	Schulen Sie Ihre Mitarbeitenden (➔ Checkliste 9a zur Spionageabwehr) und simulieren Sie IT-Vorfälle und Cyberangriffe als Trainingsmaßnahme.		
7i	Erstellen Sie kontinuierlich Back-ups der wertvollsten Daten an einem sicheren Ort.		
7j	Implementieren Sie eine Zwei-Faktor-Authentifizierung.		
7k	Führen Sie regelmäßige Updates und Patches für Software und Systeme durch.		
7l	Legen Sie für die wichtigsten Dokumente zur Aufrechterhaltung des Betriebs sowie für die wichtigsten Kontakte physische Unterlagen an, die Sie an einem oder mehreren geschützten Orten aufbewahren.		
...	...		

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
8. Personalplanung und Einsatzfähigkeit			
8a	Erstellen Sie eine Übersicht über die Arbeitszeitmodelle Ihrer Mitarbeitenden, insbesondere von denen, die in (zeit-)kritischen Prozessen (➔ Checkliste 4a zur Identifizierung) beschäftigt sind, und halten Sie diese aktuell.		
8b	Führen Sie eine freiwillige Erhebung durch, um Mitarbeitende zu identifizieren, die in der Reserve, bei der Feuerwehr, dem THW oder anderen Blaulichtorganisationen tätig sind – diese könnten in der Krise nicht verfügbar sein.		
8c	Identifizieren Sie Personal, das im Krisenfall ggf. nicht verfügbar sein könnte. *Hinweis: Gründe könnten z. B. der Arbeitsweg oder die Familiensituation sein; Es gibt auch Gründe, die das Personal aus anderen Staaten betreffen, etwa nationale Vorgaben zur Wehrpflicht/Einberufung, Grenzschließungen oder sonstige, situationsbezogene Hindernisse.*		
8d	Erstellen Sie einen Plan für betriebsnotwendige Funktionen und stellen Sie sicher, dass das erforderliche Personal für diese Funktionen verfügbar ist. *Hinweis: Planen Sie z. B. doppelte Besetzungen ein, nutzen Sie Personaldienstleister, setzen Sie Mitarbeitende von einem zweiten Standort mit den gleichen Fähigkeiten (z. B. im Ausland) ein und automatisieren Sie Prozesse, sodass diese auch ohne Personal funktionieren.*		
8e	Entwickeln Sie Strategien für die schnelle Integration von Ersatzpersonal, falls Mitarbeitende ausfallen.		
8f	Prüfen Sie die Notfallwege und Sammelpunkte im Unternehmen.		
8g	Benennen Sie Ersthelfende bzw. führen Sie regelmäßige Schulungen durch.		
8h	Führen Sie regelmäßig unangekündigte Räumungsübungen durch.		
8i	Bieten Sie Ihren Mitarbeitenden Hilfestellung für die Krisenvorsorge im privaten Bereich an (➔ Checkliste 10b zur Kommunikation).		
...	...		
9. Spionageabwehr			
9a	Sensibilisieren und schulen Sie das Personal im Hinblick auf Spionage- und Sabotageaktivitäten, auch im Bereich der IT-Sicherheit.		
9b	Informieren Sie sich und Ihre Mitarbeitenden bei Reisen über die aktuelle Lage im jeweiligen Land sowie über Reise- und Sicherheitshinweise. *Hinweis: Das Auswärtige Amt veröffentlich unter „Sicher Reisen" staatenbezogene Sicherheitshinweise und bietet auch die Möglichkeit an, sich in der Krisenvorsorgeliste ELEFAND zu registrieren.*		
9c	Überprüfen Sie Ihre eigene Internetpräsenz und frei verfügbare Daten auf deren Sensibilität.		
9d	Prüfen Sie, ob eine (IT-)Sicherheits- oder Integritätsprüfung nötig ist, um die Risiken für Ihr Unternehmen zu reduzieren.		
9e	Prüfen Sie, ob bei Mitarbeitenden mit sicherheitsempfindlichen Tätigkeiten potenzielle Sicherheitsrisiken bestehen könnten (Zuverlässigkeit, Erpressbarkeit etc.).		

Nr.	Maßnahme	Prüfungsintervall	Umsetzungsstand
	Beschreibung der zu prüfenden und umzusetzenden Maßnahmen	Zeitlicher Rahmen für die der Maßnahmen-grundlage und Umsetzung	• Noch nicht begonnen • In Vorbereitung • Geprüft und für nicht zutreffend befunden • Geprüft und in Umsetzung • Umgesetzt
9f	Klären Sie, ob bei Mitarbeitenden, die sicherheitsempfindliche Tätigkeiten wahrnehmen, eine Sicherheitsüberprüfung im Rahmen des vorbeugenden personellen Sabotageschutzes durch das Bundesministerium für Wirtschaft und Energie durchgeführt werden soll.		
...	...		
10. Interne und externe Kommunikation			
10a	Machen Sie sich Ihrer verschiedenen Zielgruppen in der Kommunikation bewusst und legen Sie Ziele für die Kommunikation mit den jeweiligen Zielgruppen fest.		
10b	Überlegen Sie, für welche Kernbotschaften Sie Mitarbeitende im Zusammenhang mit Risiken sensibilisieren wollen. Kommunizieren Sie diese klar und geben Sie Handlungsempfehlungen. *Hinweis: Handlungsempfehlungen können sich sowohl auf die betrieblichen Abläufe fokussieren als auch auf die private Vorsorge für verschiedene Krisen.*		
10c	Klären Sie die Zuständigkeiten in der Kommunikation mit internen und externen Akteuren sowohl in der Vorbereitungszeit als auch im Ereignisfall. *Hinweis: Besonders wichtig sind klare Zuständigkeiten zwischen der Geschäftsführung, der beauftragten Person bzw. Organisationseinheit in der Krise (➔ Checkliste 1c) und den für die Kommunikation zuständigen Einheiten. Sorgen Sie für eine einheitliche Kommunikationslinie.*		
10d	Bereiten Sie die Kommunikation für den Ereignisfall bestmöglich vor. *Hinweis: Die Vorbereitungen können von Sprachregelungen und vorbereiteten Materialien bis zu Kommunikationsstrategien reichen.*		
10e	Legen Sie Kanäle der Kommunikation für den Ereignisfall im Vorfeld fest und testen Sie diese (➔ Checkliste 7d–f zur Infrastruktur).		
...	...		
11. Chancen erkennen			
11a	Identifizieren Sie frühzeitig, welche Geschäftsfelder oder Produkte in den definierten Krisenszenarien zusätzlich nachgefragt werden könnten. *Beispiele: Notfallprodukte, alternative Logistiklösungen, Krisenmanagement-beratung, mögliche Anforderungen aus Sicherstellungsgesetzen, Unterstützung der Bundeswehr etc.*		
11b	Nehmen Sie frühzeitig, ggf. schon im Vorfeld, Kontakt zu potenziellen Bedarfsträgern auf.		
11c	Bereiten Sie neue Geschäftsfelder für Krisenszenarien vor, um sie im Ereignisfall schnell realisieren zu können.		
...	...		

Notizen

Diskutieren Sie mit! Finden Sie weitere Informationen zum Stand des Projekts, Ideen und Impulse für Hamburg im Jahr 2040 – und die Möglichkeit, sich einzubringen auf

www.hamburg2040.de

Herausgeber:
Handelskammer Hamburg
Adolphsplatz 1 | 20457 Hamburg
Postfach 11 14 49 | 20414 Hamburg
Telefon 040 36138-138 | Fax 040 36138-270
service@handelskammer-hamburg.de
www.handelskammer-hamburg.de

Autorinnen:
Dr. Monika John-Koch, Kristina Pape, Dr. Eva-Katharina Platzer (BBK) /
Tobias Bock, Christian Graf, Philip Koch (HK)

Grafiken:
Alle Grafiken © Handelskammer Hamburg

Lektorat:
Katrin Meyer

Gestaltung und Layout:
MaschmannFautzHuff GmbH
Paulinenallee 32 | 20259 Hamburg
Telefon 040 2109146-40 | info@agentur-mfh.de

Stabsbereich International
service@handelskammer-hamburg.de

Dezember 2025

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Dokument die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.