BDSV

Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

Krisenhandbuch für die Industrie

Unternehmenssicherheit und Resilienz im Krisen- und Verteidigungsfall

Leitung

Andreas Nyga
BDSV

Julia Krauspe
Deloitte

Mitwirkende

Thomas Heincke
Bearingpoint

Lisa Bubert
Deloitte

Klaus-Jürgen Göz
Deloitte

Andre Hermann
Deloitte

Jacqueline Harfst
ESG-Consulting

Klaus Renger
ESG-Consulting

Oliver Kirschenhofer
HENSOLDT Group

Dennis Füller
INFODAS GmbH

Boris Polotzek
KNDS

Heiko Höpfler
MNRCH

Kristin Kellner
Rheinmetall

Mirko Schlepps
TKMS

Jasmin Adel
toolcraft

Sönke Jacobs
ZOES

Inhalt

Vorwort 4
Einleitung 5
Ausgangslage 5
Zielsetzung 5
Leitgedanken 5
Checkliste für Unternehmen 7
Krisenhandbuch 9
Schritt 1: Die eigene Rolle in der gesamtstaatlichen 9
Sicherheitsvorsorge verstehen 9
Schritt 2: Den rechtlichen Rahmen und Verpflichtungen erkennen 10
Schritt 3: Zusammenarbeit mit Staat, Behörden und Bundeswehr 11
verstehen und vorbereiten 11
Schritt 4: Bedrohungen, Risiken und Abhängigkeiten erkennen 12
Schritt 5: Kritische Prozesse und Leistungen identifizieren 13
Schritt 6: Business Continuity Management (BCM) aufbauen 14
Schritt 7: Cybersicherheit ausbauen 15
Schritt 8: Standortsicherheit stärken 16
Schritt 9: Personal auf den Krisenfall vorbereiten 17
Schritt 10: Psychologische Resilienz stärken 18
Schritt 11: Notfall- und Krisenmanagement sicherstellen 19
Schritt 12: Einen Beitrag zur Verteidigung leisten können 20
Ausblick: Aufbau eines Resilienz-Ökosystems 21
Weiterführende Literatur & Ressourcen 22
Impressum 23

Vorwort

Liebe Leserinnen und Leser,

die Verteidigungsfähigkeit Deutschlands ist nicht nur ein Auftrag für die Bundeswehr, sondern geht uns alle an. Eine leistungsfähige und resiliente Zivilgesellschaft und Wirtschaft sind essenziell, um die Gesamtverteidigung Deutschlands sicherzustellen. Dabei gilt: Gesamtverteidigung bedeutet, dass gleichzeitig sowohl militärische wie auch zivile und wirtschaftliche Vorbereitung auf den Ernstfall nötig ist.

Dieses Sicherheitsverständnis wird im Operationsplan Deutschland widergespiegelt, geht aber noch weit darüber hinaus. Da der OPLAN militärische und zivile Interaktion betrifft, unterliegt seine öffentliche Verfügbarkeit bestimmten Einschränkungen. Im Innenministerium wird derzeit an der zivilen Komplementärplanung zum OPLAN gearbeitet. Inwieweit dabei die Wirtschaft als tragende Säule der Gesamtverteidigung berücksichtigt wird, bleibt abzuwarten.

Das vorliegende Krisenhandbuch setzt nun auf einer niedrigschwelligeren Ebene an. Die Idee: So viele Unternehmen wie möglich auf praktischer Ebene dabei zu unterstützen, sich auf den Ernstfall vorzubereiten und damit einen Beitrag für die Gesamtverteidigung zu liefern. Was bislang Gegenstand einer abstrakten Diskussion war, wird nun konkret. Wir können die Vorbereitung auf den Ernstfall nicht allein Politik und Behörden überlassen. Denn klar ist: Unsere Unternehmen sind nicht nur einfache Ausrüster der Bundeswehr und der BOS – Behörden und Organisationen mit Sicherheitsaufgaben. Auch sie selbst - ihre Produktionsstätten, Fachkräfte, Lieferketten und logistischen Fähigkeiten - sind Teil der deutschen Verteidigungsfähigkeit.

Eine ganze Reihe konkreter Fragen, die sich bei einer schweren Krise, einem Spannungsfall oder erst recht im Verteidigungsfall stellen, müssen wir selbst beantworten. Dazu zählen unter anderem die Vorbereitung auf mögliche Ausfälle der Energie- und Kommunikationsinfrastruktur, der Schutz der Beschäftigten und Produktionsstätten in unseren Unternehmen, wie auch eine Störung bislang für selbstverständlich genommener Abläufe.

Um Unternehmen bei der Beantwortung dieser im Zweifel existenziell wichtigen Fragen zu unterstützen und die Wirtschaft resilienter aufzustellen, haben wir dieses Krisenhandbuch erarbeitet. Natürlich kann ein einziges Dokument nicht alle offenen denkbaren Katastrophenszenarien allein berücksichtigen. Sehr wohl aber kann es einen wichtigen Beitrag dabei leisten, Defizite in der Vorbereitung zu erkennen und dort zu schließen, wo dies schon heute möglich ist.

Dieser Prozess ist mit dem vorgelegten Krisenhandbuch keineswegs abgeschlossen. Auf dessen Basis müssen wir weiter im Austausch bleiben, voneinander lernen und unsere Anstrengungen weiter ausweiten. Der BDSV wird sich in diesem Prozess als Impulsgeber und Koordinationsstelle einbringen. Lassen Sie uns gemeinsam daran arbeiten, Deutschland und seine Bürgerinnen und Bürger bestmöglich für die Gesamtverteidigung fit zu machen.

Mit besten Grüßen

Ihr

H. C.

Einleitung

Ausgangslage

Die sicherheitspolitische Lage in Europa hat sich nachhaltig verändert. Unternehmen sind nicht mehr nur wirtschaftliche Akteure, sondern ein integraler Bestandteil der gesamtstaatlichen Sicherheitsvorsorge. Dadurch geraten zivile Unternehmen vermehrt in das Fadenkreuz staatlich gelenkter nichtstaatlicher Akteure. Als Antwort wurden durch die Bundesregierung in den jeweiligen Ressorts einzelne Strategien entwickelt, Gesetze verschärft und Leitfäden entworfen. Inhaltlich verbesserte das die Informationslage, doch ist die Menge an Informationen insbesondere für kleine und mittlere Unternehmen (KMU) nur schwer zu verarbeiten. Es fehlt eine leicht zugängliche Übersicht als erster Anlauf- und Abholpunkt, kein Sammelsurium, sondern eine priorisierende und entscheidungsorientierte Handlungshilfe. Die schwedische Broschüre „Preparedness for businesses – In case of crisis or war“ zeigt, wie sich Unternehmen vorbereiten und systematisch in die zivile Verteidigung eingebunden werden können. Damit ist sie ein Beispiel für eine gute niedrigschwellige Handreichung an zivile Unternehmen.

Zielsetzung

Dieses Krisenhandbuch hat sich zum Ziel gesetzt so einfach wie möglich, aber so komplex wie der Situation entsprechend zu sein. Es soll sowohl für Experten als auch Einsteigern eine erste Übersicht bieten. Ziel des Krisenhandbuchs ist es, einen übertragbaren, praxisnahen Leitfaden für Unternehmen in Deutschland zu entwickeln, der

1. Unternehmen bei der Stärkung ihrer Resilienz unterstützt und
2. die Rolle der Wirtschaft im Rahmen von Zivilschutz, Host Nation Support (HNS) und Gesamtverteidigung verdeutlicht.

Leitgedanken

Übertragen aus dem schwedischen Ansatz gilt auch in Deutschland: „Unternehmen sichern nicht nur ihre eigene Betriebsfähigkeit – sie sind Teil der nationalen Resilienz und tragen aktiv zur Aufrechterhaltung staatlicher Handlungsfähigkeit bei.“[1] Die Funktionsfähigkeit der Wirtschaft ist Grundpfeiler gesellschaftlicher Stabilität.

Die Handreichung richtet sich insbesondere an KMU und dient als niedrigschwelliger Einstieg in das Thema Krisen- und Verteidigungsfähigkeit. Sie versteht sich nicht als Ersatz bestehender gesetzlicher oder regulatorischer Vorgaben, sondern als strukturierende Orientierungshilfe, die vorhandene Informationen bündelt, priorisiert und in eine für Unternehmen handhabbare Form übersetzt. Der Ansatz ist modular aufgebaut und wurde in enger Abstimmung mit Vertretern aus Wirtschaft, Verbänden und staatlichen Stellen entwickelt, um eine hohe Praxisnähe und Anschlussfähigkeit sicherzustellen.

[1] Swedish Civil Defence and Resilience Agency: Preparedness for businesses – In case of crisis or war (2026)

Wie dieses Handbuch zu nutzen ist

Dieses Handbuch bietet eine praxisnahe Orientierung für Unternehmen, um ihre Handlungsfähigkeit in Krisen- und Verteidigungsszenarien zu stärken. Es ist aufgebaut in Schritten und kann je nach Ausgangslage selektiv genutzt werden. Nutzen Sie das Handbuch als Einstieg, zur Vertiefung oder zur strukturierten Weiterentwicklung bestehender Maßnahmen. Das Handbuch bietet somit einen geeigneten Startpunkt zur strategischen Ausrichtung der eignen Unternehmenssicherheit. Die Handlungsempfehlungen zu den einzelnen Kapiteln helfen bei der schrittweisen Umsetzung der wichtigsten Maßnahmen. Sie schärfen den Fokus auf die wesentlichen Risiken und Abhängigkeiten, definieren Mindestanforderungen und legen Verantwortlichkeiten fest. Dazu kann das Handbuch Kapitel für Kapitel gelesen werden, oder direkt zu einem relevanten Schritt gesprungen werden.

Checkliste für Unternehmen

1.	**Die eigene Rolle in der gesamtstaatlichen Sicherheitsvorsorge verstehen**
	Die eigene Rolle in Versorgungsprozessen sowie kritische Schnittstellen zu Behörden, Kunden und Lieferanten systematisch erfassen.
	Die Systemrelevanz des eigenen Unternehmens bewerten, indem unverzichtbare Leistungen identifiziert, priorisiert und zentrale Abhängigkeiten erfasst werden.
	Führungskräfte für die Auswirkungen von Krisen- und Verteidigungsszenarien sensibilisieren.
2.	**Den rechtlichen Rahmen und Verpflichtungen kennen**
	Gesetzliche Anforderungen (z. B. NIS-2, KRITIS, Sicherstellungsgesetze) identifizieren und eigene Betroffenheit sowie daraus ableitbare Verpflichtungen bewerten.
	Auswirkungen staatlicher Eingriffsmöglichkeiten auf Betrieb, Personal und Lieferketten analysieren und in die eigene Notfall- und Betriebsplanung integrieren.
	Vertrags- und Lieferkettenstrukturen prüfen und anpassen, um Verpflichtungen aus Vorsorgeklauseln in den Verträgen (z. B. Priorisierung, 24/7-Betrieb, Informationsrechte) umzusetzen.
3.	**Zusammenarbeit mit Staat, Behörden und Bundeswehr vorbereiten**
	Eine Übersicht der für Ihre Standorte relevanten Ansprechpartner auf Bundes-, Landes- und kommunaler Ebene erstellen, um im Krisenfall die nahtlose Abstimmung sicherzustellen.
	Austausch mit lokalen Behörden und zuständigen militärischen Stellen bestehenden Notfallplänen und Unterstützungsstrukturen für Unternehmen suchen.
	Offizielle Warnkanäle in die betriebliche Alarmierungskette einbinden, um bei Zivilschutzlagen zeitversetzungsfrei reagieren zu können.
	Vorbereitung einer sicheren Kommunikation zwischen Privatwirtschaft und dem öffentlichen Auftraggeber bzw. den Behörden sicherstellen.
4.	**Bedrohungen, Risiken und Abhängigkeiten erkennen**
	Mithilfe von verfügbare Lageinformationen einen Überblick über die Bedrohungslagen und zentralen Krisenszenarien erstellen, konstant aktualisieren und aufrechterhalten.
	Den Schutzbedarf des Unternehmens systematisch ermitteln, indem kritische Assets (IT, Produktion, Standorte, Personal) hinsichtlich der Bedrohungsintensität bewertet werden.
	Zentrale Abhängigkeiten kontinuierlich identifizieren (Personal, Energie, IT, Lieferketten).
5.	**Kritische Prozesse und Leistungen identifizieren**
	Unverzichtbare Produkte, Dienstleistungen und Geschäftsprozesse bestimmen.
	Ein realistisches Minimalniveau sowie die notwendigen Schritte zu dessen Aufrechterhaltung festlegen.
	Schlüsselpersonal und Prioritäten für den Krisenfall festlegen.
6.	**Business Continuity Management (BCM) aufbauen**
	Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungspläne erstellen und Ausweichprozesse sowie Redundanzen für den Not- und Krisenfall vorbereiten.
	Klare Strukturen inklusive Rollen, Verantwortlichkeiten und Abläufe etablieren und Meldewege sowie die Einbindung relevanter Behörden sicherstellen.
	Zuständiges Personal regelmäßig schulen und die Pläne in regelmäßigen Übungen auf Wirksamkeit und Aktualität überprüfen.
	Lagerbestände für kritische Materialien und Betriebsmittel strategisch aufbauen und Abhängigkeiten durch alternative Lieferanten reduzieren.

7.	**Cybersicherheit ausbauen**
	Den Cyber-Schutzbedarf sowie die Systeme ermitteln, die kritische Produkte, Dienstleistungen und Geschäftsprozesse unterstützen.
	Technische Mindeststandards umsetzen, insbesondere für Informationstechnologie und Betriebstechnologie (IT/OT-) Systeme, die kritische Produkte, Dienstleistungen und Geschäftsprozesse unterstützen.
	Etablierung von Prozessen, die die dauerhafte Umsetzung und Einhaltung der Mindeststandards sicherstellen (z.B. Informationssicherheitsmanagementsysteme (ISMS), Cyber Incident Response, etc.).
8.	**Standortsicherheit stärken**
	Zutrittskontrollen implementieren und verbindliche Regeln für Besucher einführen.
	Serverräume, Leitstellen und vergleichbare sensible Bereiche durch zusätzliche Maßnahmen wie Zutrittsbeschränkungen, Protokollierung und bauliche Trennung sichern.
	Führungskräfte und Mitarbeiter bzgl. sensibler Informationen und Spionage schulen.
9.	**Personal auf den Krisenfall vorbereiten**
	Vertretungsregelungen für alle Schlüsselfunktionen dokumentieren und auf freiwilliger Basis (vertraulich!) erfassen, welche Mitarbeiter im Krisenfall durch staatliche Pflichten bei der Bundeswehr oder Rettungsorganisationen gebunden sein könnten.
	Positionen auf UK-Stellungsbedarf prüfen und daraufhin frühzeitig Kontakt zur Bundesagentur für Arbeit aufnehmen.
	Ein Insider-Risikoprogramm mit Vier-Augen-Prinzip bei sensiblen Prozessen, geprüften Dienstleisterzugängen und einen vertraulichen Meldekanal etablieren.
10.	**Psychologische Resilienz stärken**
	Mitarbeiter (insbesondere Führungskräfte) auf Krisenkommunikation und Belastungssituationen vorbereiten.
	Schulungen zur Erkennung von und Reaktion auf Desinformation einführen.
	Eine transparente und aktive Kommunikationsstrategie für den Ernstfall entwickeln.
	Unterstützungsangebote und Ansprechpersonen festlegen, die auch nach einem Krisenfall eine psychologische Betreuung sicherstellen können.
11.	**Notfall- und Krisenmanagement sicherstellen**
	Festlegung von Rollen, Verantwortlichkeiten (Aufbauorganisation) sowie Prozessen und Abläufen (Ablauforganisation) im Krisenmanagement
	Vorbereitung von Hilfsmitteln und Vorgehensweisen für eine strukturierte Lagebewertung, -visualisierung und -bewältigung
	Regelmäßige Schulungen und Übungen für die gesamte Krisenorganisation sicherstellen
12.	**Im Krisenfall einen Beitrag zur Verteidigung leisten können**
	Rechtliche Verpflichtungen aus Wirtschaftssicherstellungsgesetz (WiSiG) und Arbeitssicherstellungsgesetz (ASG) prüfen und diese in Notfall- und Continuity-Planung integrieren.
	Bedarf an zusätzlichen Lager- bzw. Depotflächen prüfen oder Möglichkeiten zur Bereitstellung solcher Flächen evaluieren.

Krisenhandbuch

Schritt 1: Die eigene Rolle in der gesamtstaatlichen Sicherheitsvorsorge verstehen

Im Krisen- oder Verteidigungsfall spielen Unternehmen eine entscheidende Rolle für die Funktion unserer Gesellschaft. Als Unternehmer sind Sie Teil der Zivilen Verteidigung und leisten einen Beitrag, indem Sie Ihren Betrieb so weit wie möglich aufrechterhalten. Damit stärkt die Resilienz eines Unternehmens die Widerstandsfähigkeit der Gesellschaft. Der Staat kann kritische Infrastrukturen nicht allein sichern. Die Bundesregierung erwartet deshalb von Unternehmen, ihre Funktionsfähigkeit zu erhalten, Risiken zu analysieren und Vorsorge zu treffen. Wichtig ist dabei zu unterscheiden, in welcher Form diese Erwartung für das eigene Unternehmen gilt:

- **Als allgemeine Erwartungshaltung** gilt sie für nahezu alle Unternehmen – unabhängig von Größe oder Branche. Wer die eigene Funktionsfähigkeit im Krisenfall sichert, reduziert Ausfall- und Haftungsrisiken und positioniert sich als verlässlicher Partner gegenüber Kunden, Lieferanten und Behörden.
- **Als konkrete gesetzliche Pflicht** gilt sie bislang vor allem für Betreiber kritischer Infrastrukturen (KRITIS). Das im Januar 2026 in Kraft getretene KRITIS-Dachgesetz richtet sich in erster Linie an größere, systemrelevante Unternehmen; mittelständische Betriebe außerhalb dieses Kreises sind bislang nur begrenzt unmittelbar gesetzlich verpflichtet, auch wenn sie faktisch stark betroffen sein können, etwa als Zulieferer.

Wichtig ist deshalb zunächst die ehrliche Selbsteinschätzung: Gehört mein Unternehmen zu den KRITIS-Betreibern oder deren unmittelbaren Zulieferern – oder handelt es sich eher um eine allgemeine unternehmerische Verantwortung, die nicht sanktioniert, aber strategisch sinnvoll ist? Auch die Bundeswehr ist ohne zivile Netze nicht einsatzfähig. Ein Großteil der militärischen Transporte läuft über kommerzielle Infrastrukturen und kritische Ressourcen stammen weitgehend aus dem zivilen Markt. Logistik-, Energie- und Kommunikationsunternehmen werden im Verteidigungsfall zu strategischen Partnern, rechtlich abgesichert durch Rahmenverträge und die Rahmenrichtlinien für die Gesamtverteidigung (RRGV). Für KRITIS-Betreiber bedeutet dies, dass Versorgungssicherheit zur nationalen Aufgabe wird, Fallback- und Notbetriebspläne mit staatlichen Stellen kompatibel sein müssen und Kommunikations- sowie Alarmierungswege vorab zu definieren sind.

Quick Win: Erstellen Sie eine Übersicht über Ihren Beitrag zur Resilienz. Welche kritischen Leistungen stellen Sie bereit, die im Krisen- oder Verteidigungsfall nicht ausfallen dürfen? Benennen Sie eine verantwortliche Person für die Krisenvorsorge mit direktem Berichtsweg zur Geschäftsführung. In kleinen Unternehmen kann diese Rolle mit bestehenden Funktionen kombiniert werden.

Lesetipp: BAKS: Unternehmen in der gesamtstaatlichen Sicherheitsvorsorge

Schritt 2: Den rechtlichen Rahmen und Verpflichtungen erkennen

Krisen-, Spannungs- und Verteidigungsfälle verändern die Anforderungen an Unternehmen der Sicherheits- und Verteidigungsindustrie grundlegend. Geschäftsführungen müssen Risiken für Fortbestand, Lieferfähigkeit und verteidigungsrelevante Aufträge frühzeitig steuern. Neben Compliance rücken Vorsorge, Business Continuity Management (BCM), Lieferketten, Cyber- und Objektschutz sowie klare Melde- und Entscheidungswege in den Fokus.

Den staatlichen Rahmen setzen die Rahmenrichtlinien für die Gesamtverteidigung. Sie regeln das Zusammenwirken militärischer und ziviler Verteidigung, etwa in Versorgung, Cyberabwehr, Verkehr, Energie und Personal. Unternehmensleistungen können in Krisen damit Teil gesamtstaatlicher Resilienz werden.

Zentral ist der Schutz digitaler und physischer Betriebsfähigkeit. Nach dem BSI-Gesetz, welches auf der NIS-2-Richtlinie beruht müssen erhebliche Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden (Erstmeldung nach 24h, Folgemeldung nach 72h und Abschlussmeldung nach 1 Mon.). Ergänzend setzt das KRITIS-Dachgesetz Anforderungen an die physische Resilienz kritischer Anlagen.

Auch vertragliche Pflichten gegenüber öffentlichen Auftraggebern können erheblich sein. Besonders relevant ist die Vorsorgeklausel B 077 des Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). Auftragnehmer können zur Leistungserweiterung, Beschleunigung, Datenbereitstellung oder Meldungen verpflichtet sein. Dies sollte auch in Unteraufträgen und Lieferantenbeziehungen abgesichert werden.

Im Spannungs- und Verteidigungsfall können zudem Sicherstellungsgesetze greifen. Das WiSiG ermöglicht Maßnahmen für Güter, Leistungen, Produktionsmittel, Energie und Werkleistungen. Das ASG regelt Arbeitsleistungen: Es kann nicht nur die Beendigung von Arbeitsverhältnissen zustimmungsbedürftig machen, sondern unter bestimmten Voraussetzungen auch Personen in ein anderes Arbeitsverhältnis verpflichten. Dadurch kann eine Fachkräfte- und Ressourcenknappheit entstehen, wenn Schlüsselpersonal zeitweise nicht verfügbar ist.

Unternehmen sollten frühzeitig Transparenz über kritische Funktionen, Schlüsselpersonal, Kapazitäten, Lagerbestände, Abhängigkeiten und Ausweichprozesse schaffen. Dazu gehört ein Lagebild zu kritischen Rollen sowie zu Vertretungs-, Qualifizierungs- und Priorisierungsmaßnahmen. So werden rechtliche Anforderungen schneller handhabbar.

Quick Win: Erstellen Sie eine Rechts- und Pflichtenmatrix für den Krisen-, Spannungs- und Verteidigungsfall, die den Unternehmensfunktionen, Meldewegen und Verantwortlichkeiten zentrale Anforderungen (NIS-2, KRITIS-Dachgesetz, B 077, WiSiG, ASG etc.) zuordnet.

Lesetipp: vbw: Die Rolle der Wirtschaft im Verteidigungsfall

Schritt 3: Zusammenarbeit mit Staat, Behörden und Bundeswehr verstehen und vorbereiten

Die **Zivile Verteidigung** ist integraler Bestandteil der Gesamtverteidigung, ergänzt die militärische Verteidigung durch zivile Maßnahmen und beruht auf vier Säulen: Aufrechterhaltung staatlicher Handlungsfähigkeit, Schutz der Bevölkerung, Versorgung von Bevölkerung und Streitkräften sowie Unterstützung der Streitkräfte durch Verwaltung und Wirtschaft. Die Verantwortung für den Schutz der Zivilbevölkerung im Verteidigungsfall liegt beim Bund, der sich dabei auf Länder, Kommunen sowie Behörden und Organisationen mit Sicherheitsaufgaben stützt. Länder und Kommunen übernehmen vor allem Aufgaben der Schadensbewältigung und des Katastrophenschutzes. Landkreise und kreisfreie Städte koordinieren das Zusammenwirken verschiedener Akteure. Auf dieses bestehende System greift der Bund im Zivilschutzfall zurück. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ist die zentrale Bundesbehörde für den Bevölkerungsschutz. Es unterstützt das Krisenmanagement, betreibt Warnsysteme, stellt Ausstattung für den Zivilschutz bereit, stärkt die Trinkwassernotversorgung und fördert Vorsorge, Selbsthilfe sowie den Schutz Kritischer Infrastrukturen. Ergänzend übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Aufgaben im Bereich Cybersicherheit, insbesondere bei Prävention, Krisenmanagement und Sicherheitsvorgaben für KRITIS-Unternehmen.

Die **militärische Verteidigung** ist Aufgabe der Bundeswehr. Im Rahmen der zivil-militärischen Zusammenarbeit unterstützt sie zivile Stellen, etwa im Katastrophenschutz oder bei Rettungseinsätzen. Zentrale Ansprechstelle für Bund und Länder ist das Operative Führungskommando der Bundeswehr (OpFüKdoBw). Es verantwortet die operative Planung und Führung, koordiniert Amtshilfe und sichert im Bündnis- oder Verteidigungsfall die Rolle Deutschlands als logistische Drehscheibe im Rahmen des OPLAN. Der Host Nation Support umfasst zivile und militärische Unterstützungsleistungen für verbündete Streitkräfte auf deutschem Staatsgebiet unter Einbindung auch der Privatwirtschaft. Den Landesregierungen und zivilen Stellen stehen die Landeskommandos als wichtigste Schnittstellen zur Bundeswehr zur Verfügung. Ihnen nachgeordnet sind Kreis- und Bezirksverbindungskommandos, die überwiegend aus Reservisten bestehen und Krisenstäbe beraten. Das Kommando Zivil-Militärische Zusammenarbeit der Bundeswehr bündelt Expertise, erstellt Lagebilder und unterstützt die militärische Führung.

Quick Win: Sie sollten frühzeitig klären, welche Ansprechstellen bei Kommunen und Katastrophenschutzbehörden sowie beim jeweiligen Landeskommando relevant sind. Zudem sollten Sie prüfen, ob und wie das Unternehmen im Ernstfall eingebunden werden kann, etwa durch Produkte, Dienstleistungen, Personal, Fahrzeuge, Geräte oder Räumlichkeiten.

Lesetipp: Konzeption Zivile Verteidigung (KZV), Grünbuch ZMZ 4.0

Schritt 4: Bedrohungen, Risiken und Abhängigkeiten erkennen

Wie erkenne ich Bedrohungen?

(Hybride) Bedrohungsszenarien sind über alle Stufen zwischen Frieden und Krieg real. Cyberangriffe, Ransomware, Spionage etc. können sich zu realwirtschaftlich wirksamen Operationen verbinden. Da sich Bedrohungen laufend verändern, sollten Unternehmen verlässliche Informationskanäle etablieren und regelmäßig prüfen.

Wie erkenne ich relevante Risiken?

Der Schutz vor gezielter Einflussnahme setzt eine Schutzbedarfsermittlung voraus. Er beginnt mit der Bewertung möglicher Einfallstore und der Einbindung geopolitischer Risiken in Sicherheits- und Beschaffungsentscheidungen. Der Schutzbedarf ergibt sich aus dem Zusammenspiel von:

1. Bedrohungsintensität (z. B. Angriffsvektoren, Eintrittswahrscheinlichkeit, Exposition) und
2. Kritikalität (z. B. finanzielle Schäden, Versorgungsrelevanz, Reputationsverlust)

Erst die Verbindung von Bedrohung und Schwachstelle schafft ein konkretes Risiko. Ziel ist es, unerwünschte Einflussnahme frühzeitig zu erkennen, zu begrenzen und die organisationale Handlungsfähigkeit zu sichern. Dafür ist ein kontinuierliches Lagebild unerlässlich.

Wie erkenne ich kritische Abhängigkeiten?

Grundlage aller Maßnahmen ist ein klares Verständnis der eigenen Betroffenheit, kritischer Pfade und zentraler Abhängigkeiten bei Personal, Energie, IT, Transport, Logistik und Lieferketten. Unternehmen sollten dabei nicht nur direkte Auswirkungen auf Standorte, Geschäftsbereiche und kritische Assets betrachten, sondern auch indirekte Effekte militärischer Konflikte oder großflächiger Truppenbewegungen durch Deutschland einbeziehen. Dazu zählen überlastete Transport- und Kommunikationsnetze, Verkehrsumleitungen, Zugangsbeschränkungen im Umfeld militärischer Infrastruktur sowie Engpässe bei Treibstoff, Betriebsmitteln und Logistik. Diese Effekte können auch Unternehmen treffen, die selbst kein Ziel sind, aber auf stabile Verkehrs-, Kommunikations-, Energie- und Versorgungsketten angewiesen bleiben.

Zur Identifikation kritischer Abhängigkeiten helfen folgende Leitfragen:

- Welche direkten und indirekten Auswirkungen betreffen Betrieb, Standorte, Geschäftsbereiche und kritische Assets?
- Welche Abhängigkeiten (z.B. bei Personal, Energie, IT, Logistik, Lieferketten) gibt es?
- Welche Wechselwirkungen können zwischen einzelnen Auswirkungen entstehen?

Quick Win: Erstellen Sie zum Einstieg eine einfache Schutzbedarfsübersicht. Listen Sie die Top 5 Assets auf und bewerten Sie jedes hinsichtlich der dazugehörigen Bedrohungsintensität.

Lesetipp: Lageberichte und Warnmeldungen des BSI über Allianz für Cyber-Sicherheit und Wirtschaftsschutzangebote des Verfassungsschutzes, DIN SPEC 14027, Abschnitt 5 und 6, Initiative Wirtschaftsschutz, VSW Bundesverband

Schritt 5: Kritische Prozesse und Leistungen identifizieren

Wie werden kritische Geschäftsprozesse & Organisationswerte identifiziert?

Grundlage jeder Resilienzstrategie ist die strukturierte Erfassung aller wesentlichen Assets eines Unternehmens. Dazu zählen insbesondere Personal, Informationen, IT-Systeme, Liegenschaften, Produktionsmittel und Geschäftsprozesse. Zentrale Leitfrage ist: Welche Leistungen und Prozesse sind für die Funktionsfähigkeit des Unternehmens in einer Krisenlage unverzichtbar und zeitkritisch? Ziel ist es, kritische Abhängigkeiten frühzeitig zu erkennen und abzusichern. Eine Prozesslandkarte mit den wichtigsten Prozessen des Unternehmens verschafft Ihnen einen guten Überblick. Strukturierte und transparente Prozesse mit Zuordnung der Prozessrisiken, Abhängigkeiten zu vor- und nachgelagerten Prozessen sowie benötigten Ressourcen ermöglichen die erforderliche Analyse und Reaktionsfähigkeit.

Wie kann eine Mindestbetriebsfähigkeit sichergestellt werden?

Im Ernstfall verändern sich für Unternehmen und ihre Prozesse die Prioritäten: Es ist vorrangig wichtig, dass weiter produziert werden kann. Unternehmen müssen definieren, welche Prozesse aufrechtzuerhalten sind. Dazu gehört die Festlegung eines realistischen Minimalbetriebs sowie die Vorbereitung organisatorischer Grundlagen für dessen Aufrechterhaltung.

Wie gestaltet sich eine Geschäftsauswirkungsanalyse (Business Impact Analysis, BIA)?

Um geschäftskritische Prozesse und Leistungen zu identifizieren, kategorisieren Sie diese anhand von Wertschöpfung und Kundennutzen. Identifizieren Sie essenzielle Prozesse (direkte Wertschöpfung), Unterstützungsprozesse (keine langfristige Behinderung von Produktion und Auslieferung bei Ausfällen) und Prozesse, die in Krisensituationen vernachlässigbar sind.

Wie können Redundanzen, Vorratshaltung und Alternativlösungen realisiert werden?

Für geschäftskritische Prozesse und Leistungen, ist eine tiefergehende Analyse erforderlich: Welche Mindestanforderungen müssen erfüllt sein, damit der jeweilige Prozess funktioniert? Welche Grundbedarfe bestehen z.B. an Material, Strom, Wasser, spezielle personelle Ressourcen etc. Identifizieren Sie wesentliche Aktivitäten sowie wichtige Schlüsselpositionen und -qualifikationen. Prüfen Sie, ob die erforderlichen (auch personellen) Ressourcen im Ernstfall zur Verfügung stehen oder die Verfügbarkeit vorhersehbar eingeschränkt sein wird. Berücksichtigen Sie dabei auch, welche kritischen Betriebsmittel durch Vorratshaltung abgesichert werden können; als Orientierungsgröße kann eine Eigenversorgung für mindestens 72 Stunden dienen. Leiten Sie anschließend Maßnahmen zur Absicherung der Prozesse / Leistungen ab.

Quick Win: Führen Sie einen Check Ihrer Liefer- und Wertschöpfungskette durch. Identifizieren Sie Single-Sources und legen Sie hierfür Alternativen fest.

Lesetipp: DIN SPEC 14027, Abschnitt 5 Schutzbedarfsermittlung und Abschnitt 6 Sicherheitslagebild

Schritt 6: Business Continuity Management (BCM) aufbauen

BCM beschreibt die Maßnahmen, mit denen Unternehmen ihre Handlungsfähigkeit in Krisen sichern und den Betrieb kontrolliert aufrechterhalten. Im Gegensatz zu anderen Schritten in diesem Handbuch geht es hier nicht um einzelne Gefahren oder technische Schutzmaßnahmen, sondern um die organisatorische Gesamtarchitektur: Wer entscheidet was, wie lange hält Ihr Betrieb durch, und wie kommunizieren Sie, wenn reguläre Systeme ausfallen?

Wie werden Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungspläne erstellt?

Bestimmen Sie zuerst die Prozesse, die in einer Krise unbedingt weiterlaufen müssen, und wie lange Sie ohne diese auskommen können. Orientieren Sie sich an zwei Zeithorizonten: Innerhalb der ersten 72 Stunden sind Minimal- und Notfunktionen ohne externe Unterstützung sicherzustellen, bspw. durch Notstrom, Ersatzpersonal, reduzierte Systeme und manuelle Prozesse. Anschließend steht der Wiederanlauf kritischer Prozesse, ggf. mit externer Unterstützung, im Fokus. Entsprechend sind Lieferketten, Ausweichstandorte, Lieferanten und Recovery Time Objectives (RTOs) je kritischem System frühzeitig zu berücksichtigen.

Wie werden klare Rollen, Verantwortlichkeiten und Abläufe etabliert?

Im Ernstfall sind klare Entscheidungs-, Vertretungs- und Meldewege entscheidend. Strukturieren Sie den Krisenstab an bewährten deutschen Führungs- und Stabsstrukturen, etwa nach der Feuerwehr-Dienstvorschrift 100 oder entlang der S-Gliederung. Standardisierte Sprachregelungen und die Einbindung von Behörden, Kunden und Medien beugen Desinformation und Panik vor.

Wie lässt sich Personal regelmäßig schulen und wie können Pläne getestet werden?

Mitarbeiter sind regelmäßig zu Prozessen, Rollen und alternativen Kommunikationsmitteln (z. B. Satellitentelefon, UKW-Funk, papierbasierte Kontaklisten) zu schulen. Krisenübungen testen die Pläne und ermöglichen deren Anpassung an neue Risiken und Rahmenbedingungen.

Wie lassen sich Lagerbestände strategisch aufbauen und Abhängigkeiten reduzieren?

Für die Minimal- und Notfunktionen sind Vorräte unverzichtbarer Materialien und Betriebsmittel (z.B. Notstromaggregate, Ersatzteile oder Kommunikationsgeräte) unerlässlich. Gleichzeitig wird die Lieferanten-Diversifizierung vorangetrieben, indem für jede kritische Komponente mindestens ein alternativer Zulieferer identifiziert wird.

Quick Win: Listen Sie die drei wichtigsten Prozesse in Ihrem Unternehmen auf, die auch im Ernstfall weiterlaufen müssen. Aktualisieren Sie Ihre BCM-Pläne bzgl. Szenarien wie IT-, Gebäude-, Personal-, Strom- und Lieferantenausfälle.

Lesetipp: Identifizierung und Priorisierung innerhalb von Kritischen Infrastrukturen, BSI-Standard 200-4 BCM

Schritt 7: Cybersicherheit ausbauen

Cyberangriffe zählen zu den häufigsten Krisenursachen für Unternehmen jeder Größe und treffen KMU oft stärker als Großkonzerne. Staatliche Angreifer testen Systeme bereits im Frieden systematisch auf Schwachstellen. Im Spannungsfall kann aus Aufklärung oft Sabotage werden. Für mehr Cyber-Resilienz beachten Sie die nachfolgenden Schritte:

Was muss geschützt werden?

Zuerst ist der Cyber-Schutzbedarf systematisch zu ermitteln, denn Grundlage jeder Maßnahme ist das Wissen, welche Systeme, Daten und Prozesse kritisch sind. Dazu sollten kritische Produkte, Dienstleistungen und zeitkritische Geschäftsprozesse sowie die zugehörigen IT-/OT-Systeme einschließlich ihrer Abhängigkeiten zu Dienstleistern und Lieferanten (Supply-Chain-Risiken) identifiziert und dokumentiert werden. Ebenso wichtig sind die Inventarisierung kritischer IT-/OT-Assets, privilegierter Zugänge sowie relevanter Firmware- und Softwarestände zur Kritikalitätsbewertung. Verantwortlichkeiten für Systeme, Daten, Schnittstellen und Schutzziele sollten eindeutig zugewiesen werden.

Wie setzen wir Mindeststandards um?

Auf Basis der ermittelten Kritikalität sind technische und organisatorische Mindeststandards umzusetzen. Dazu zählen insbesondere rollenbasierte Zugriffsrechte nach dem Least-Privilege-Prinzip, die Absicherung kritischer Konten und Fernzugriffe, Netzwerksegmentierung sowie die Trennung von IT- und OT-Netzen. Ergänzend sollte eine operative Cybersicherheit etabliert oder extern eingebunden werden, wie etwa zur kontinuierlichen Überwachung, Bewertung und Eskalation von Sicherheitsereignissen. Backups sind nach der 3-2-1-Regel abzusichern, regelmäßig zu testen und konsequent vom Produktionsnetz zu trennen.

Wie sichern wir das dauerhaft ab?

Zudem müssen Prozesse zur dauerhaften Absicherung etabliert werden. Dazu gehören ein Informationssicherheits-Managementsystem (ISMS, z. B. angelehnt an ISO 27001) sowie ein Cyber-Incident-Response-Plan inklusive OT-Notfall- und Wiederanlaufplan mit klar geregelten Zuständigkeiten. Ergänzend sollten Krisenrollenkarten auch offline verfügbar sein. Besonders wichtig ist die Festlegung interner Melde- und Eskalationswege. Darüber hinaus sind externe Meldewege je nach Branche, Bundesland und geltender Regulatorik zu definieren, z.B. an BSI, BBK, BMWE, BfV/LfV, CERTs aus Landes- und Bundesebene und / oder die jeweilige Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes. Prozesse müssen regelmäßig geübt, Mitarbeiter geschult und Hochrisiko-Gruppen gezielt sensibilisiert werden.

Quick Win: Wer Schutzbedarfe kennt, kann Mindeststandards umsetzen. Für jede Maßnahme gilt: Verantwortliche benennen, Startdatum festlegen und Abnahmekriterium definieren.

Lesetipps: BSI: 10 Tipps zur Cybersicherheit für Unternehmen

Schritt 8: Standortsicherheit stärken

Zutrittskontrolle, Schutz kritischer Bereiche und Sensibilisierung für Spionage bilden das Fundament physischer Resilienz. Physische Sicherheit umfasst weit mehr als Perimeterschutz, Videoüberwachung oder Gebäudetechnik. Ein wirksames Standortsicherheitskonzept kombiniert organisatorische, bauliche und technische Maßnahmen. Die nachfolgenden Maßnahmen lassen sich überwiegend organisatorisch umsetzen, wirken unmittelbar risikomindernd und schaffen die Grundlage für weitergehende Investitionen.

Wer hat Zutritt?

Ein erster Ansatzpunkt ist die Einführung von Zutrittskontrollen und verbindlichen Besucherregelungen. Zutrittsberechtigungen sollten regelmäßig überprüft und auf das notwendige Maß beschränkt werden. Ergänzend empfiehlt sich ein Schlüssel- und Berechtigungsverzeichnis, um verlorene oder missbräuchlich genutzte Schlüssel und Karten zeitnah sperren zu können. Ein verbindliches Besucherverfahren mit Anmeldung, Begleitung und Kennzeichnung betriebsfremder Personen sollte etabliert werden. Serverräume, Leitstellen und vergleichbare Bereiche sind besonders zu schützen. Zutrittsrechte sollten auf einen definierten Personenkreis beschränkt, Zutritte nachvollziehbar protokolliert und kritische Bereiche baulich vom übrigen Betrieb getrennt werden.

Welche Informationen dürfen geteilt werden?

Ein weiterer Baustein ist die Sensibilisierung von Führungskräften und Mitarbeitern für den Umgang mit sensiblen Informationen, Spionageversuche und Social-Engineering-Taktiken wie Tailgating. Hierzu gehören klare Vorgaben zur Klassifikation, Weitergabe und Freigabe von Informationen sowie eine eindeutige Definition, welche Informationen das Unternehmen nicht verlassen dürfen.

Standortsicherheit mit wenig Aufwand?

Mit geringem Aufwand lassen sich weitere Sicherheitsgewinne erzielen: Außenbeleuchtung überprüfen, Sichtachsen freihalten, Kameras und Alarmanlagen auf Funktionsfähigkeit kontrollieren sowie Fremdfirmenpersonal in Zutritts- und Meldewege einbinden. Zudem ist eine Inventarliste sicherheitsrelevanter Ausstattung, regelmäßige Security Walks sowie die Prüfung und Nachrüstung von Schlössern, Fenstersicherungen und Zufahrtssperren sinnvoll.

Quick Win: Zutrittskontrolle, Schutz kritischer Bereiche und Sensibilisierung für Spionage bilden gemeinsam die Grundlage physischer Resilienz. Für jede Maßnahme gilt: Verantwortliche Person benennen, Umsetzungsfrist festlegen und ein geeignetes Abnahmekriterium definieren. Diese sind ohne nennenswerte Kosten umsetzbar und schließen unmittelbare Lücken, bevor größere bauliche oder technische Investitionen angegangen werden.

Lesetipp: DIN SPEC 14027, Abschnitt 11 Standortsicherheit

Schritt 9: Personal auf den Krisenfall vorbereiten

Personal ist im Krisen- und Verteidigungsfall eine der kritischsten Ressourcen jeder Organisation: Die Betriebsfähigkeit hängt davon ab, dass Schlüsselrollen verfügbar, vertreten und handlungsfähig bleiben.

Wer ist verfügbar?

Der BSI-Standard 200-4 und die ISO 22301 benennen Personalausfälle als wesentliche Gefährdung; bereits einzelne Kopfmonopole können kritische Prozesse beeinträchtigen, wenn Wissen, Zugänge oder Entscheidungswege nicht dokumentiert und geübt sind. Personalverfügbarkeit sollte daher integraler Bestandteil von BCM, ISMS und Krisenmanagement sein. Dabei sind neben organisatorischen Aspekten auch rechtliche Rahmenbedingungen wie das ASG zu berücksichtigen. Es kann im Spannungs- oder Verteidigungsfall Auswirkungen auf Arbeitsverpflichtungen und die Verfügbarkeit von Beschäftigten haben und ist damit ein relevanter Planungsparameter.

Wie können Schlüsselpersonen, Kopfmonopole und Vertretungen abgesichert werden?

Organisationen sollten analysieren, welche Funktionen für Betrieb, Versorgung und Schutzaufgaben unverzichtbar sind, welche Beschäftigtengruppen betroffen sein könnten und wie arbeitsrechtliche Vorgaben, behördliche Anforderungen und interne Notfallprozesse ineinandergreifen.

Ausgangspunkt ist eine realistische Bestandsaufnahme kritischer Funktionen: Wer verfügt über Schlüsselwissen, Systemzugänge, Anlagenkenntnisse, Behördenkontakte oder Wiederanlaufkompetenz? Für diese Rollen müssen Vertretungen nicht nur benannt, sondern durch Berechtigungen, Dokumentation, Schulungen und Übungen tatsächlich befähigt werden. Zudem sind erforderliche Mindestbesetzungen festzulegen sowie interne und externe Schnittstellen regelmäßig zu erproben.

Handlungsfähigkeit mit Präsenz- und Fernarbeit?

Remote-Arbeit kann die Resilienz erhöhen, setzt jedoch getestete Fernzugriffe, belastbare Authentifizierung, Notfallberechtigungen und sichere Kommunikationswege voraus. Alarmierungswege, Kontaktlisten, Schichtpläne und Wiederanlaufanweisungen sollten redundant (digital und analog) aktuell und geschützt verfügbar sein. Für längere Krisenlagen sind Präsenzpflichten, Ablösungen und remote-fähige Aufgaben vorab festzulegen.

Quick Win: Liste der kritischsten Funktionen erstellen. Je Funktion Vertretung, Zugriffe und Dokumentation prüfen. Vertretungen in Übungen praktisch erproben und Cross-Skilling langfristig etablieren.

Lesetipp: BAGFW_Handreichung_Krisenkonzepte.pdf

Schritt 10: Psychologische Resilienz stärken

Psychologische Resilienz ergänzt Business Continuity Management, Informationssicherheit und Krisenmanagement. Neben technischen Ausfällen oder physischen Schäden können auch Desinformation, Gerüchte und manipulierte Narrative Vertrauen schwächen, Unsicherheit erhöhen und die Funktionsfähigkeit der Mitarbeiter beeinflussen.

Wie verhalten sich Mitarbeiter in Krisen?

Unternehmen sollten Orientierung, Kommunikationsfähigkeit und die individuelle Widerstandskraft ihrer Mitarbeiter stärken. Gerade in langanhaltenden Krisen hängt die Handlungsfähigkeit einer Organisation davon ab, wie gut Beschäftigte mit Unsicherheit, Stress, Informationsüberlastung und hoher Arbeitsbelastung umgehen können. Regelmäßige Resilienz-Trainings sollten daher ein fester Bestandteil der Personal- und Krisenvorsorge sein. Ergänzend unterstützen Maßnahmen zur Stressbewältigung, Selbstfürsorge und Entscheidungsfähigkeit unter Druck sowie eine psychosoziale Notfallversorgung (PSNV) vor und nach belastenden Ereignissen. Das Ziel sind handlungsfähige Teams auch in Krisensituationen.

Wie gehen wir mit Desinformationen um und bilden Vertrauen?

Resiliente Unternehmen begegnen Desinformation mit klaren Meldewegen, definierten Verantwortlichkeiten und regelmäßiger Sensibilisierung. Mitarbeiter sollten Quellen kritisch prüfen, emotionalisierende Inhalte nicht ungeprüft weitergeben und bei Unsicherheit interne Ansprechstellen einbinden. Verdachtsfälle müssen schnell eingeordnet, kommunikative Risiken bewertet und abgestimmte Reaktionen vorbereitet werden. Vertrauen entsteht durch konsistentes, nachvollziehbares und glaubwürdiges Handeln. Dafür braucht es klare Rollen, vorbereitete Krisenkommunikationsstrategien, abgestimmte Botschaften und eine aktive Kommunikation nach innen und außen. Eine Kommunikationsmatrix hilft, Informationsbedürfnisse zielgruppengerecht zu adressieren. Dies stärkt die psychologische Sicherheit der Mitarbeiter und fördert handlungsfähige Entscheidungen unter Belastung.

Was muss nach einer Krise passieren?

Nach Krisen sollten psychische Belastungen und organisatorische Herausforderungen systematisch ausgewertet werden. Die Erkenntnisse sind in konkrete Verbesserungsmaßnahmen mit klaren Verantwortlichkeiten zu überführen und in Schulungen, Resilienz-Trainings, Kommunikationsbausteine, Meldewege sowie Krisenpläne einfließen zu lassen. So wird die Organisation schrittweise widerstandsfähiger gegenüber künftigen Krisenlagen.

Quick Win: Awareness-Formate etablieren: Stressreaktionen in Krisen, persönliche Resilienzstrategien, Erkennen von Desinformation, interne Meldewege sowie verfügbare Unterstützungsangebote. Dies stärkt die Handlungsfähigkeit und reduziert Fehlentscheidungen.

Lesetipp: BMI: Leitfaden Krisenkommunikation

Schritt 11: Notfall- und Krisenmanagement sicherstellen

Krisen lassen sich nicht immer verhindern, ihre Folgen aber begrenzen. Dafür müssen Unternehmen auch unter Zeitdruck handlungs- und entscheidungsfähig bleiben. Da reguläre Führungs- und Kommunikationsstrukturen bei Cyberangriffen, Stromausfällen, Lieferkettenstörungen, Sabotage oder sicherheitspolitischen Eskalationen oft nicht ausreichen, sollten klare Krisenstrukturen frühzeitig etabliert und regelmäßig erprobt werden.

Wer wendet Krisen ab?

Jedes Unternehmen sollte einen festen Krisenstab benennen, der im Ereignisfall die zentrale Steuerung und Koordination übernimmt. Seine Aufgabe ist es, die Lage zu bewerten, Entscheidungen vorzubereiten, Maßnahmen zu priorisieren und die Kommunikation zu steuern. Der Krisenstab soll negative Auswirkungen (finanziell, Reputation, Geschäftsfortführung) und Krisenauslösende Faktoren abwenden. Entscheidungen dürfen nicht von einzelnen Personen oder „Kopfmonopolen“ abhängen. Ergänzend empfiehlt sich eine Stabsassistenz für Lageführung, Protokollierung und Nachverfolgung von Maßnahmen.

Was braucht ein Krisenmanagement?

Ein Krisenstab kann nur wirksam arbeiten, wenn Rollen, Abläufe und Befugnisse bereits vor einer Krise definiert wurden. Dazu sollten Unternehmen ein Krisenmanagement-Handbuch mit Alarmierungswegen, Kontaktlisten, Eskalationsstufen, Rollenbeschreibungen und Kommunikationsvorgaben erstellen. Ebenso wichtig ist die Festlegung, wann ein Vorfall zur Krise wird, wer den Krisenstab aktiviert und wie Entscheidungen dokumentiert werden. Klare Regeln schaffen Orientierung, reduzieren Unsicherheit und beschleunigen die Reaktion im Ereignisfall.

Übung macht die Profis, oder?

Krisenmanagement bleibt nur wirksam, wenn es regelmäßig geübt wird. Für kleinere und mittlere Unternehmen reichen zum Einstieg bereits kurze „Was-wäre-wenn?“-Fragen im Teammeeting, um Szenarien wie Cyberangriffe, Stromausfälle, Lieferengpässe oder Personalausfälle zu durchdenken und erste Reaktionsmuster zu entwickeln. Darauf aufbauend können einfache halbtägige Tabletop-Übungen mit Bordmitteln zentrale Abläufe, Rollen, Kommunikationswege und Entscheidungen anhand realistischer Szenarien testen. Umfangreichere Übungen mit Beobachtung, Dokumentation oder externer Moderation können nachfolgen. Für eine stetige Verbesserung ist es wichtig, Übungen und reale Ereignisse systematisch auszuwerten und Erkenntnisse in Handbücher, Prozesse und Schulungen zu überführen.

Quick Win: Etablierung eines Krisenstabs mit klaren Rollenverteilung. Erstellung von Leitlinien und Handbüchern mit Eskalations-, Alarmierungs- und Bewältigungsprozessen.

Lesetipp: Praxishandbuch Krisenmanagement (Sartory, Senn, Zimmermann, Mazumder) & Krisenmanagement in der Praxis (Rosenlieb, Dreher).

Schritt 12: Einen Beitrag zur Verteidigung leisten können

Wie gelingt die Umstellung der Produktion im Ernstfall?

Im Spannungs- oder Verteidigungsfall wird Ihr Unternehmen rechtlich in die Gesamtverteidigung eingebunden. Das WiSiG sichert hierbei Ressourcen und Produktionskapazitäten und das ASG bindet Ihre Fachkräfte in kritischen Funktionen (vgl. Schritt 2). Ihr Unternehmen wird ebenso unter Umständen in OPLAN-Arbeitsgruppen eingebunden und zur Teilnahme an Übungen verpflichtet (vgl. Schritt 3).

Welche Dual-Use-Fähigkeiten sind für zivile und militärische Resilienz relevant?

Viele Unternehmen fallen gleichzeitig unter zivile Anforderungen (NIS-2, KRITIS-Dachgesetz) und militärisch relevante Verpflichtungen im Verteidigungsfall. Ist Ihr Unternehmen als Logistikunternehmen, das heute unter NIS-2 fällt, zu kategorisieren, dann wird es im Spannungsfall zum Host-Nation-Support-Anbieter. Sind Sie Energieversorger, Telekommunikationsanbieter, Bank- oder IT-Dienstleister, bilden Sie das Rückgrat der zivilen Verteidigungsfähigkeit. Fällt eines dieser Glieder aus, geraten Staat, Versorgung und Kommunikation unter Druck. Aktiv gestärkte Widerstandsfähigkeit trägt dabei nicht nur zu Ihrer Sicherheit bei, sondern sichert Ihnen auch Wettbewerbsvorteile und Vertrauen bei Ihren Kunden und Investoren.

Wie bauen Unternehmen belastbare Schnittstellen zu staatlichen Stellen und kritischen Sektoren auf?

Ihre Ansprechpartner sind vor allem das Bundesamt für Sicherheit in der Informationstechnik (BSI), das BBK und die entsprechenden Landeskommandos der Bundeswehr. Direktkanäle zu Behörden und Verbänden sind bisher nur teils aufgebaut, weswegen eine eigenständige Kontaktaufnahme zu empfehlen ist.

Quick Win: Prüfen Sie frühzeitig, welche Ihrer Produktions- oder Dienstleistungskapazitäten im Krisen- und Verteidigungsfall für die Gesamtverteidigung relevant sein könnten und bereiten Sie entsprechende Umstellungsszenarien vor. Prüfen Sie Ihre Personalverfügbarkeit im Hinblick auf die mögliche Einberufung von Reservisten sowie Angehörige des Zivilschutzes (THW, Rettungsdienste, Feuerwehren). Klären Sie die Möglichkeiten von Unabkömmlichkeitsanträgen für Ihr Personal.

Lesetipp: Konzeption Zivile Verteidigung (KZV), Kapitel 7 und 8, Deutscher Bundestag Drucksache 20/10476 --- Bericht zur Risikoanalyse für den Zivilschutz 2023

Ausblick: Aufbau eines Resilienz-Ökosystems

Unternehmen, die Resilienzmaßnahmen isoliert umsetzen, bleiben im Krisenfall verwundbar. Widerstandsfähigkeit entsteht im Wesentlichen erst durch Vernetzung mit Behörden, Branchenpartnern, Forschungseinrichtungen und sonstigen Organisationen.

Welche Netzwerke unterstützen Unternehmen in der Krisenvorsorge?

Für den Austausch mit Behörden und Unternehmen bestehen bereits etablierte Formate. Für KRITIS-Betreiber, ihre Verbände und zuständige Behörden bietet die Plattform UP KRITIS einen Rahmen für Informationsaustausch und Kooperation. Für KMU, die in der Regel keinen Zugang hierzu haben, ist die Allianz für Cyber-Sicherheit des BSI ein zentraler Einstiegspunkt. Sie bietet Leitfäden, Warnmeldungen und praxisnahe Unterstützungsangebote. Ergänzend ermöglichen IHK-Arbeitskreise zur Krisenvorsorge den Austausch mit Unternehmen in vergleichbaren Situationen. Skandinavien zeigt auf, dass früh aufgebaute Strukturen schnelle Krisenreaktionen erleichtern und Unternehmen als Teil staatlicher Vorsorge nutzbar machen.

Wie können Plattformen, Cluster und gemeinsame Übungen die Resilienz stärken?

Technologie- und Sicherheitscluster bündeln Kompetenzen, vernetzen Wirtschaft, Behörden und Einsatzorganisationen und erleichtern kleineren Betrieben den Zugang. Gemeinsame Übungen machen Schnittstellen, Zuständigkeiten und Unterstützungsbedarfe sichtbar. Beispiele sind Red Storm, Medic Quadriga 2026 und die Länder- und Ressortübergreifenden Krisenmanagementübungen (LÜKEX). Ergänzend ermöglichen Threat-Intelligence-Plattformen den skalierbaren Austausch von Bedrohungsinformationen zwischen Betreibern und Behörden.

Wie lassen sich Resilienzmaßnahmen fördern und finanzieren?

Das BAFA-Programm „Förderung von Unternehmensberatungen für KMU“ mit Frist bis zum 31.12.2026 kann relevant sein, wenn externe Beratung zu wirtschaftlichen, finanziellen, personellen oder organisatorischen Fragen der Unternehmensführung erfolgt. Förderfähig sind bis zu fünf Beratungen pro Unternehmen, höchstens zwei pro Jahr. Der Fördersatz hängt von Standort und Fallgestaltung ab und kann ausnahmsweise bis zu 80 Prozent betragen. Richtlinienstand und Förderfähigkeit sollten vor Antragstellung geprüft werden. Auf EU-Ebene können der European Defence Fund (EDF) und das European Defence Industry Programme (EDIP) Förderzugänge eröffnen. Investitionen in Resilienzstrukturen, zertifizierbare Managementsysteme und regulatorische Konformität, etwa nach ISO 22301 oder NIS-2, verbessern zudem die Anschlussfähigkeit an öffentliche Ausschreibungen.

Quick Win: Registrieren Sie Ihr Unternehmen bei der Allianz für Cyber-Sicherheit unter bsi.bund.de/ACS und abonnieren Sie die Lageinformationen des BSI.

Lesetipp: BSI: Leitfaden zur Methodik Grundschutz++

Weiterführende Literatur & Ressourcen

Grundlagendokumente

BMI: Konzeption Zivile Verteidigung

BMI: Rahmenrichtlinien für die Gesamtverteidigung (RRGV) - Gesamtverteidigungsrichtlinien

DIN SPEC 14027 Corporate Security – Anforderungen zur Stärkung physischer Resilienz von Organisationen

Unterrichtung durch die Bundesregierung: Bericht zur Risikoanalyse für den Zivilschutz 2023

Praxisleitfäden und Handlungsempfehlungen

BAGFW_Handreichung_Krisenkonzepte.pdf

BBK: Ratgeber: Vorsorgen für Krisen und Katastrophen

BBK: Identifizierung und Priorisierung innerhalb von Kritischen Infrastrukturen

BMI: Leitfaden Krisenkommunikation

BSI-Standard 200-4: Business Continuity Management

BSI: Informationen und Hilfestellungen für KMU

DSLV: Leitfaden zum Anwendungsbereich des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Zukunftsforum Öffentliche Sicherheit: Grünbuch ZMZ 4.0

Cybersicherheit

BSI: 10 Tipps zur Cybersicherheit für Unternehmen

BSI: IT-Grundschutz-Kompendium

BSI: Ein Praxis-Leitfaden für IS-Penetrationstests

Bitkom: Leitfaden Cyberversicherung und -sicherheit

BSI: Leitfaden zur Methodik Grundschutz++

Branchenspezifisch / Sonstiges

BAAINBw: Anlageblatt Vorsorgeklausel

BAFA: Förderung von Unternehmensberatungen für KMU (Stand: Juni 2025)

BAKS: Unternehmen in der gesamtstaatlichen Sicherheitsvorsorge

OpFüKdo: Booklet zum Operationsplan Deutschland

vbw: Die Rolle der Wirtschaft im Verteidigungsfall

Impressum

Herausgeber

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V. (BDSV)

Friedrichstraße 60

10117 Berlin

Verantwortlich für den Inhalt

Hans Christoph Atzpodien

Hauptgeschäftsführer BDSV e. V.

Redaktion und Koordination

Andreas Nyga

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V. (BDSV)

Stand

September 2026

Kontakt

E-Mail: bdsv@bdsv.eu

Internet: https://www.bdsv.eu/

Haftungshinweis

Das Krisenhandbuch dient der allgemeinen Information und Orientierung für Unternehmen. Die enthaltenen Hinweise und Empfehlungen erheben keinen Anspruch auf Vollständigkeit und ersetzen keine rechtliche, sicherheitsfachliche oder unternehmensspezifische Beratung. Die Umsetzung der dargestellten Maßnahmen liegt in der Verantwortung des jeweiligen Unternehmens.

Urheberrecht

Alle Inhalte dieses Handbuchs sind urheberrechtlich geschützt. Eine Vervielfältigung, Bearbeitung oder Weitergabe – auch auszugsweise – bedarf, soweit nicht anders gekennzeichnet, der Zustimmung des Herausgebers.

© 2026 Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V. (BDSV)