OPAL ORGANISATION PERSONAL ARBEIT LEADERSHIP

Krisenresilienz deutscher Unternehmen

Tamara Böhm, Prof. Dr. Stefan Liebig und Prof. Dr. Wenzel Matiaske

Working Papers OPAL

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

Die Autoren:

Tamara Böhm, Freie Universität Berlin, Institut für Soziologie, Arbeitsbereich Empirische Sozialstrukturanalyse, E-Mail: t.boehm@fu-berlin.de

Prof. Dr. Stefan Liebig, Freie Universität Berlin, Institut für Soziologie, Arbeitsbereich Empirische Sozialstrukturanalyse, E-Mail: stefan.liebig@fu-berlin.de

Prof. Dr. Wenzel Matiaske, Institut für Personal und Arbeit (IPA) der HSU/Uni BwH und Research Fellow des DIW Berlin. Email: matiaske@hsu-hh.de

Working Papers des Forschungsclusters OPAL der Helmut-Schmidt-Universität

Working Papers No. 21, Hamburg 2026

ISSN 2512-8019 (online)
ISSN 2512-7950 (print)

Kontakt

Rebekka Hensen
Helmut-Schmidt-Universität / Universität der Bundeswehr
Holstenhofweg 85, Gebäude H1, Raum 2133
22043 Hamburg
Tel.: 040 / 65 41 22 32
Fax: 040 / 65 41 35 22

rebekka.hensen@hsu-hh.de
www.hsu-hh.de/opal

Redaktion

Prof. Dr. Wenzel Matiaske
Prof. Dr. Katharina Liebsch

Krisenresilienz deutscher Unternehmen

Executive Summary

Die Studie „Herausforderungen durch zukünftige Krisen und Katastrophen“ zeigt, wie unterschiedlich gut deutsche Unternehmen auf Krisen vorbereitet sind – und wo zentrale Schwachstellen bestehen. Betriebe sehen sich mit einer wachsenden Bedrohungslage konfrontiert, von Cyberangriffen über Lieferkettenstörungen bis hin zu Extremwetterereignissen. Die Befragung von 1.224 Unternehmen aller Branchen und Größen macht deutlich: Während einige Risiken – insbesondere im technologischen und geopolitischen Bereich – klar priorisiert werden, bestehen in der Vorsorge erhebliche Lücken, vor allem bei selteneren, aber potenziell gravierenden Szenarien.

Cyberangriffe und IT-Störungen: Höchstes Risiko, unvollständige Vorsorge

Cyberangriffe, IT-Störungen und Lieferkettenprobleme werden von den Betrieben als größte Gefahr wahrgenommen und treten bereits häufig auf. Fast die Hälfte der Unternehmen (44 %) war in den vergangenen fünf Jahren von IT-Ausfällen, Internetstörungen oder Lieferkettenunterbrechungen betroffen. Entsprechend haben 91 % der Betriebe nach eigenen Angaben Maßnahmen zur Erhöhung der IT-Sicherheit ergriffen. Darüber hinaus gehende Schritte planen jedoch nur 17 %. Besonders kritisch ist die Lage bei Betrieben kritischer Infrastrukturen, etwa in der Energieversorgung oder im Gesundheitswesen: Sie bewerten das Risiko von Angriffen und Infrastrukturausfällen deutlich höher als andere Branchen – ein Hinweis auf fragile, eng vernetzte Versorgungsstrukturen mit möglicher Domino-Wirkung. Hier besteht dringender Handlungsbedarf, insbesondere beim Ausbau von Backups, redundanten Systemen und bei der systematischen Schulung der Mitarbeitenden.

Großbetriebe vs. KMU: Strukturelle Vorteile und Verwundbarkeiten

Einen klaren Unterschied zeigt die Studie zwischen großen Unternehmen und kleinen und mittleren Unternehmen (KMU). Großbetriebe investieren systematischer in Krisenvorsorge, verfügen häufiger über Notstromaggregate (63 % gegenüber 35 % bei kleinen Betrieben) und haben eher strukturierte Risikoanalysen, Notfallpläne und Katastrophenschutzmaßnahmen etabliert. KMU sind finanziell wie organisatorisch schlechter aufgestellt: Zwar geben sie häufiger an, finanzielle Rücklagen für Krisen zu bilden (55 % gegenüber 38 % bei Großbetrieben), doch mangelt es oft an formalen Prozessen, an Kooperationen mit lokalen Behörden und an einer Diversifizierung der Lieferketten. Gerade KMU könnten ihre Resilienz mit vergleichsweise geringem Aufwand stärken – etwa durch die Nutzung staatlicher Förderprogramme im Bereich Cybersicherheit, durch branchenspezifische Leitfäden sowie durch eine stärkere Einbindung in lokale Netzwerke mit Behörden und Hilfsorganisationen.

Regionale Unterschiede: Ländliche Regionen sind besser vernetzt – Städte müssen aufholen

Deutliche regionale Unterschiede treten ebenfalls zutage. In ländlichen und dünn besiedelten Regionen ist das Bewusstsein für die Bedeutung von Katastrophen- und Zivilschutz deutlich ausgeprägter: 41 % der Betriebe dort haben den Austausch mit lokalen Akteuren des Krisen- und Katastrophenschutzes ausgebaut oder entsprechende Kooperationen intensiviert – in Städten sind es nur 34 %. Ländliche Unternehmen sind zudem stärker mit Hilfsorganisationen vernetzt, berichten von regelmäßiger Kooperation und zeigen eine höhere Bereitschaft, im Krisenfall Personal, Technik oder Transportmittel zur Verfügung zu stellen. In städtischen Regionen ist die Vernetzung mit Hilfsorganisationen dagegen schwächer, und die Einbindung der Belegschaft in Katastrophenschutzthemen fällt geringer aus. Städte hinken insbesondere bei der

Zusammenarbeit mit Behörden und bei der Sensibilisierung der Mitarbeitenden hinterher. Hier sind gezielte Initiativen erforderlich, etwa zur Förderung ehrenamtlichen Engagements, zum Aufbau und Ausbau von Krisennetzwerken sowie zur Durchführung gemeinsamer Übungen.

Kritische Lücke: Kaum Vorbereitung auf militärische und hybride Bedrohungen

Eine besonders gravierende Lücke besteht in der Vorbereitung auf militärische Krisen und hybride Bedrohungen. Sektorübergreifend verfügen nur sehr wenige Unternehmen – selbst im systemrelevanten quartären Sektor (IT, Energie, Gesundheit) – über spezifische Reaktionspläne für den Verteidigungsfall; insgesamt geben lediglich rund 10 % an, entsprechende Pläne zu besitzen. Angesichts steigender geopolitischer Spannungen und hybrider Kriegsformen, bei denen Cyberangriffe, Desinformation und physische Sabotage kombiniert auftreten können, ist dies eine deutliche Schwachstelle. Unternehmen sollten daher prüfen, ob sie im Krisen- oder Verteidigungsfall eine besondere Rolle spielen, und gegebenenfalls Notfallkonzepte entwickeln – etwa für den Ausfall kritischer Infrastruktur, für längerfristige Energieunterbrechungen oder für den Umgang mit gezielten Desinformationskampagnen.

Schlussfolgerung: Krisenvorsorge als Bestandteil vorausschauender Unternehmensführung

Insgesamt wird deutlich, dass Krisen- und Katastrophenvorsorge bislang stark von der eigenen Betroffenheit, der Unternehmensgröße, der Branche und der geografischen Lage abhängen. Die Analysen legen nahe, dass Sensibilisierung, Planung und Vernetzung deutlich intensiviert werden müssen. Dazu gehören:

- ein höheres Bewusstsein für Zivil- und Katastrophenschutz in allen Belegschaftsgruppen,
- die systematische Umsetzung und regelmäßige Übung von Notfallplänen,
- klar definierte Benachrichtigungs- und Entscheidungswege sowie
- der gezielte Ausbau der Zusammenarbeit mit lokalen Katastrophenschutzbehörden und Hilfsorganisationen.

Insbesondere in städtischen Regionen mit hoher Bevölkerungsdichte sollte die Resilienz von Betrieben und Organisationen gegenüber Krisen- und Katastrophensituationen strategisch gestärkt werden. Für Unternehmen bedeutet dies, Krisenvorsorge nicht nur als Reaktion auf bereits erlebte Ereignisse zu verstehen, sondern als integralen Bestandteil vorausschauender Unternehmensführung – denn die Studie zeigt: Wer heute in Resilienz investiert, reduziert morgen Ausfallrisiken und sichert seine Handlungsfähigkeit im Wettbewerb.

Die folgenden Abschnitte beschreiben zunächst die Anlage der Studie und anschließend die zentralen empirischen Ergebnisse im Detail.

Herausforderungen durch zukünftige Krisen und Katastrophen

Anlage der Studie

Die Studie „Herausforderungen durch zukünftige Krisen und Katastrophen“ untersucht, wie gut deutsche Unternehmen auf verschiedene Krisen vorbereitet sind und wie sie mit Bedrohungen umgehen. Sie wurde von der Freien Universität Berlin, der Helmut-Schmidt-Universität/Uni Bw Hamburg (HSU) und dem Sozio-oekonomischen Panel am DIW Berlin (SOEP) gemeinsam durchgeführt und lief vom 26. März 2025 bis zum 20. Januar 2026.
Im Mittelpunkt steht die Frage, wie widerstandsfähig (resilient) deutsche Betriebe gegenüber verschiedenen Risiken sind – etwa gegenüber Naturkatastrophen oder technischen Ausfällen. Die Studie betrachtet,

- wie Unternehmen solche Gefahren einschätzen,
- wie anfällig sie dafür sind und
- wie sie darauf reagieren – etwa durch Vorsorgemaßnahmen oder durch Vernetzung mit Einrichtungen des Zivil- und Katastrophenschutzes.

Diese Themen gewinnen an Bedeutung, da sich Extremwetterereignisse häufen und sich die geopolitische Lage verändert hat. Eine politische Antwort darauf ist das „KRITIS-Dachgesetz“, das unter anderem Mindeststandards für den Schutz wichtiger Anlagen festlegt, damit diese besser gegen verschiedene Gefahren gewappnet sind. Trotzdem bleibt es in erster Linie Aufgabe der einzelnen Unternehmen, sich bestmöglich vorzubereiten und nach einer Krise schnell wieder funktionsfähig zu werden.

Für die Studie wurden wirtschaftlich aktive Unternehmen in ganz Deutschland aus allen Branchen zufällig ausgewählt; 1.224 Betriebe haben an der Befragung teilgenommen. Ihre Antworten zeigen,

- wie Betriebe Risiken einschätzen,
- welche Maßnahmen sie bereits ergriffen haben und
- wie sie sich auf zukünftige Krisen vorbereiten.

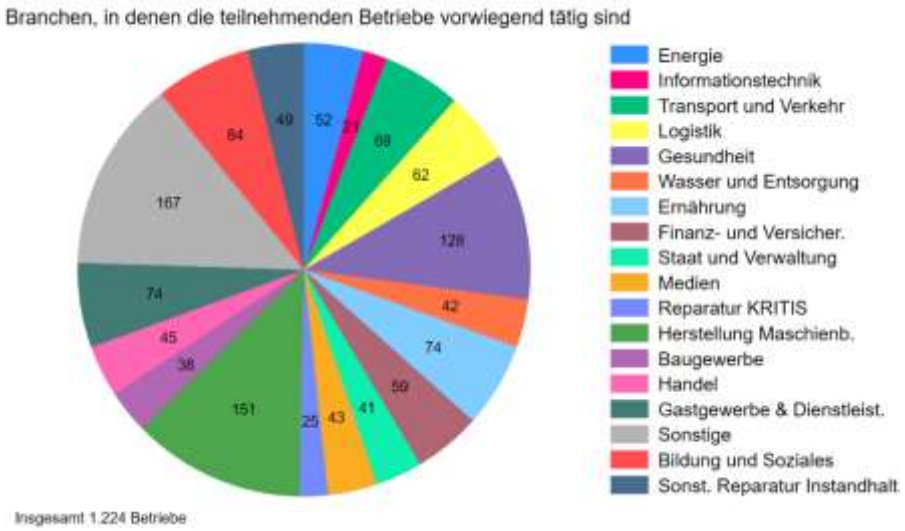


Abbildung 1: Anzahl der Betriebe aus verschiedenen Sektoren, die an der Befragung teilgenommen haben.

Befragt wurden vorwiegend die Geschäftsführungen sowie Angestellte aus der Personal-, IT- oder Krisen-/Sicherheitsabteilung. Ihre Antworten zeigen, wie Betriebe Risiken einschätzen, welche Maßnahmen sie bereits ergriffen haben und wie sie sich auf zukünftige Krisen vorbereiten. In diesem Bericht werden die wichtigsten Ergebnisse dieser Befragung vorgestellt. Abbildung 1 zeigt, in welchen Branchen die teilnehmenden Betriebe überwiegend tätig sind.

Zentrale Ergebnisse

In Anlehnung an aktuelle Empfehlungen zum Schutz wichtiger Einrichtungen, zur allgemeinen Risikovorsorge und an wissenschaftliche Konzepte dazu, wie Unternehmen widerstandsfähiger werden können, haben wir in diesem Bericht bestimmte Schwerpunkte gesetzt. Uns interessiert vor allem,

- wie Unternehmen verschiedene Risiken und Gefahren einschätzen,
- welche Erfahrungen sie damit bereits gemacht haben und
- welche konkreten Maßnahmen sie in den letzten fünf Jahren ergriffen haben, um sich besser auf solche Ereignisse vorzubereiten.

Außerdem betrachten wir, inwieweit Unternehmen sich der Bedeutung von Katastrophenschutz und Zivilschutz bewusst sind und wie sie sich darauf vorbereiten. In den vorliegenden Analysen werden die Wahrnehmungen und Maßnahmen der befragten Betriebe anhand folgender Merkmale verglichen:

- Betriebe der kritischen und nicht kritischen Infrastrukturen,
- Branchen, zusammengefasst zu Sektoren,
- Betriebsgröße sowie
- städtische und ländliche Regionen.

Zu den Einrichtungen und Betrieben kritischer Infrastrukturen zählen technische Anlagen, Dienstleistungen sowie Organisationen, die für die Versorgung, Sicherheit und das Funktionieren der Gesellschaft unerlässlich sind. Dazu gehören insbesondere die Wirtschaftsbranchen Energie, Transport und Verkehr, Finanzwesen, Sozialversicherung und Grundsicherung, Ernährung, Gesundheitswesen, Informationstechnik, Wasser- und Abfallwirtschaft sowie der Bereich Weltraum [11; 20].

1. Fünf Arten von Risiken, Betroffenheit sowie konkrete Anpassungs- bzw. Reaktionsmaßnahmen

In der Befragung wurden die Unternehmen gebeten einzuschätzen, wie groß ihrer Meinung nach das Risiko ist, in den nächsten fünf Jahren von 21 verschiedenen Ereignissen betroffen zu sein (auf einer Skala von 0 bis 10). Anschließend wurden sie gefragt, ob sie solche Ereignisse bereits erlebt haben und ob sie Maßnahmen ergriffen haben, um sich in Zukunft besser zu schützen. Die untersuchten Risiken haben wir fünf Kategorien zugeordnet:

- technologische und geopolitische Risiken (z. B. Lieferkettenprobleme, Ausfall von IT oder Internet)
- Angriffe (z. B. Cyberangriffe oder gezielte Falschinformationen)
- Naturkatastrophen (z. B. schwere Unwetter)
- Ausfälle wichtiger Infrastruktur (z. B. Ausfälle von Strom-, Gas-, Wasser- oder Verkehrsnetzen)
- Unfälle (z. B. Brände) und Pandemien

Da die Einschätzungen dieser fünf Risikoarten bei Betrieben der kritischen und der nicht kritischen Infrastrukturen unterschiedlich ausfallen, werden die Risikoeinschätzungen für beide Gruppen getrennt dargestellt. Die

durchschnittlichen Risikoeinschätzungen der Betriebe der kritischen und nicht kritischen Infrastrukturen sind in Abbildung 2 gegenübergestellt. Bei den ersten beiden Risikoarten – „technologische und geopolitische Risiken“ sowie „Risiko eines Angriffs (z. B. Cyberangriffe oder gezielte Falschinformationen)“ – zeigen sich keine Unterschiede. Die Kategorie „Risiko eines Angriffs“ wird jedoch von Betrieben der kritischen wie auch der nicht kritischen Infrastrukturen als das höchste Risiko eingeschätzt.

Bei den weiteren drei Risikokategorien bestehen signifikante Unterschiede: Die Kategorien „Naturkatastrophen“, „Ausfälle wichtiger Infrastrukturen (z. B. Strom-, Gas-, Wasser- oder Verkehrsnetzausfälle)“ sowie „Unfälle und Pandemien“ werden von Betrieben der kritischen Infrastrukturen als gravierender wahrgenommen. Kritische Anlagen sind für diese Risikoarten anfälliger und untereinander wechselseitig abhängig. Der Ausfall eines kritischen Sektors kann direkte Auswirkungen auf weitere kritische Sektoren haben (Dominoeffekte). Diese Wechselwirkungen werden durch die zunehmende Digitalisierung zusätzlich verstärkt.

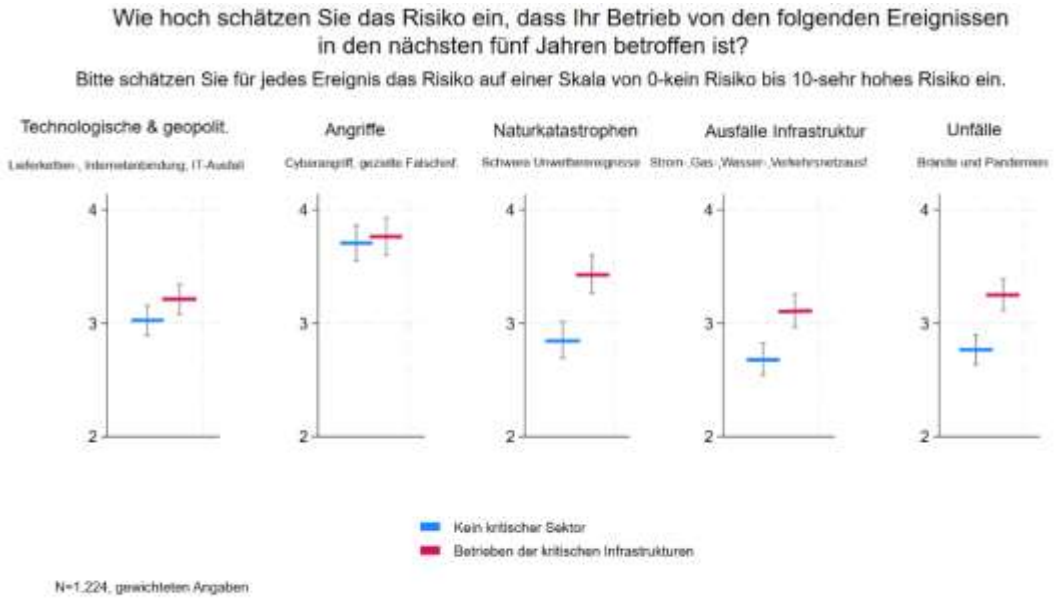


Abbildung 2: Bewertung der fünf Risikodimensionen durch Betriebe der kritischen und nicht kritischen Infrastrukturen (Mittelwerte).

2. Betroffenheit sowie konkrete Anpassungs- bzw. Reaktionsmaßnahmen

In denselben fünf Dimensionskategorien (technologische/geopolitische Disruption, Angriff, Naturkatastrophe, Ausfall wichtiger Infrastrukturen oder Unfall) wurden die Betriebe zudem gefragt, ob sie entsprechende disruptive Ereignisse bereits erlebt haben und ob sie anschließend Maßnahmen ergriffen haben, um sich künftig besser davor zu schützen. Die Abbildungen 3 und 4 zeigen den Anteil der Betriebe (in Prozent), die in den letzten fünf Jahren von diesen fünf Ereignissen betroffen waren und danach konkrete Anpassungs- bzw. Reaktionsmaßnahmen eingeführt haben.

Abbildung 3: Betroffen von disruptiven Ereignissen

Abbildung 4: Konkrete Anpassungs- bzw. Reaktionsmaßnahmen

Ein signifikanter Unterschied in der Betroffenheit und den eingeführten Maßnahmen wurde in der Dimension „Ausfall wichtiger Infrastrukturen“ festgestellt: Betriebe kritischer Infrastrukturen waren um 2,5 Prozentpunkte häufiger von Ausfällen der Strom-, Gas-, Wasser- oder Verkehrsnetze betroffen und haben um 5 Prozentpunkte häufiger konkrete Reaktionsmaßnahmen eingeführt.

In der Dimension „technologische und geopolitische Risiken“ haben beispielsweise 44 % der Betriebe angegeben, in den letzten fünf Jahren von Lieferketten-, Internetanbindungs- oder IT-Ausfällen betroffen gewesen zu sein. 77 % dieser betroffenen Betriebe haben konkrete Anpassungs- und Reaktionsmaßnahmen ergriffen, um in Zukunft besser auf solche Disruptionen vorbereitet zu sein. In der Dimension „Ausfall wichtiger Infrastrukturen“ haben 12,5 % der Betriebe angegeben, in den letzten fünf Jahren von einem Ausfall der Strom-, Gas-, Wasser- oder Verkehrsnetze betroffen gewesen zu sein. 60 % dieser betroffenen Betriebe haben konkrete Maßnahmen ergriffen, um auf solche Ereignisse zukünftig besser reagieren zu können.

Diese Analyse zeigt, dass die Betroffenheit der Betriebe durch verschiedene Szenarien unterschiedlich stark ausgeprägt ist. Über 40 % der Betriebe waren von Ausfällen der IT, des Internets und der Lieferketten betroffen, während weniger als 20 % von gezielten Angriffen, Naturkatastrophen oder Ausfällen kritischer Infrastrukturen betroffen waren. Entsprechend dieser Betroffenheit fallen die Vorsorgemaßnahmen für solche Szenarien geringer aus.

3. Vorsorgemaßnahmen

Die Betriebe wurden gefragt, welche Vorsichtsmaßnahmen sie bereits getroffen haben beziehungsweise in den nächsten fünf Jahren planen, um den Betrieb an mögliche Krisen-, Katastrophen- und Bedrohungslagen anzupassen. Die nachfolgende Grafik zeigt, dass größere Betriebe häufiger Maßnahmen für verschiedene Krisen- und Katastrophenlagen implementiert haben beziehungsweise weitere Maßnahmen planen (Abbildung 5). Die am häufigsten genannte Maßnahme ist die Erhöhung der IT-Sicherheit; sie wurde von 91 % der Betriebe genannt, und 17 % der Betriebe planen weitere Maßnahmen zur IT-Sicherheit. Dieser Befund lässt sich dadurch erklären, dass Cyberangriffe als größte Gefahr wahrgenommen werden (vgl. Abbildungen 2 und 11). Die einzige Maßnahme, die häufiger von kleineren Betrieben genannt wurde, ist die Bildung finanzieller Rücklagen für Krisen- und Katastrophenlagen; dieser Befund ist auf dem 90%-Konfidenzniveau signifikant.

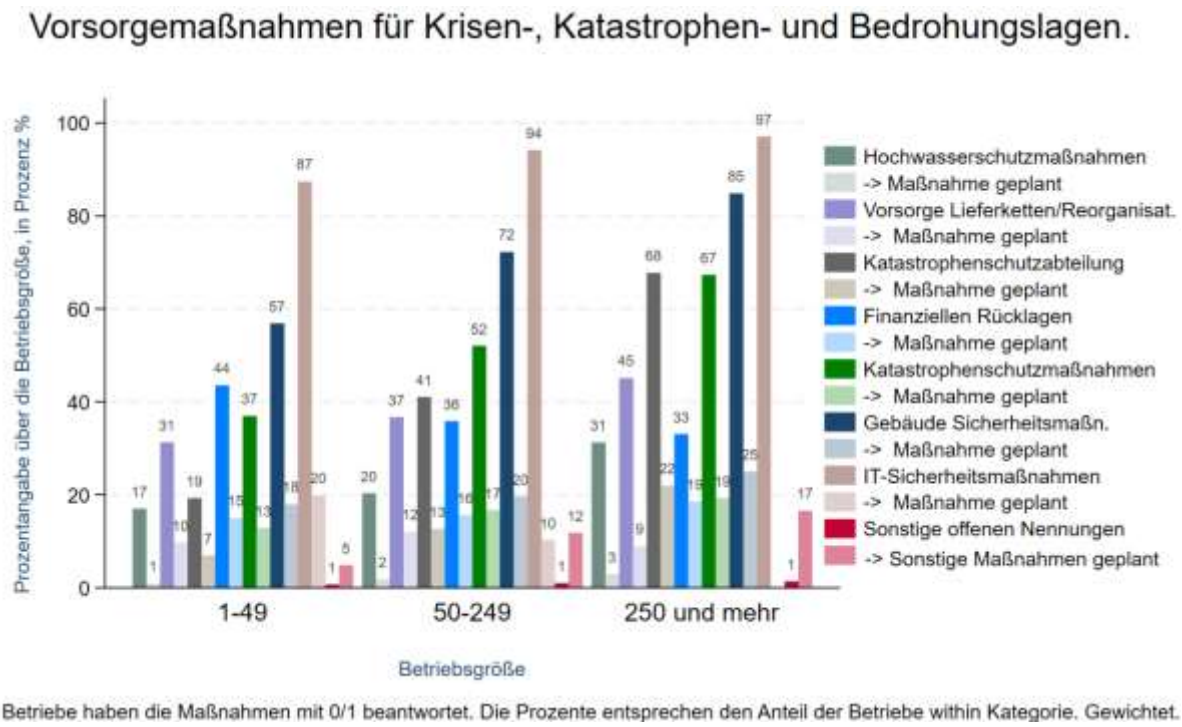


Abbildung 5: Bereits getroffene und geplante Vorsorgemaßnahmen – Prozentangaben nach Betriebsgröße.

Die weiteren Maßnahmen, die von Betrieben unter „Sonstige“ einzeln genannt wurden, lassen sich in folgende Kategorien zusammenfassen:

- Vorsorgemaßnahmen für Treibstoff- oder Wasserknappheit sowie die Bevorratung nicht substituierbarer Produkte, insbesondere Wasser, Treibstoff, Notfalltechnik und Medikamente. Zu den einzelnen Nennungen in der Kategorie Wasserbevorratung zählen unter anderem der Bau von Auffangbecken, Wasserzisternen und Wasserbehältern.
- Vorsorgemaßnahmen mit dem Fokus auf eine autarke Stromversorgung und die Umstellung auf erneuerbare Energien. Zu den einzelnen Nennungen in dieser Kategorie zählen die Installation von Notstromaggregaten, Akkuleuchten, Photovoltaik- bzw. Solaranlagen, BHKW-Anlagen sowie Heizöllager. 35 % der kleinen Betriebe mit bis zu 50 Mitarbeitenden geben an, Notstromaggregate installiert zu haben, im Gegensatz zu 63 % der größten Betriebe mit über 250 Mitarbeitenden. Betriebe des quartären Sektors (IT, neueste Technologien, Entsorgungswirtschaft, Gesundheitssektor) nennen diese Maßnahmen um 4 Prozentpunkte häufiger als Betriebe anderer Sektoren.
- Vorsorgemaßnahmen mit Schwerpunkt auf der Erhöhung der Cybersicherheit sowie auf Vorkehrungen für Ausfälle der IT-Infrastruktur und des Internets. Zu den häufigsten offenen Nennungen in dieser Kategorie zählen die Dezentralisierung und Verteilung von IT-Standorten, redundante Internetverbindungen bzw. Internet-Backups, die Nutzung von Clouddiensten, der Abschluss einer Cyberversicherung sowie der

Ausbau von Hochsicherheitszentren. Die Abhängigkeit von nicht-europäischen digitalen Dienstleistern wurde in dieser Studie nicht erfasst.

- Vorsorgemaßnahmen im Bereich Gebäudeschutz und Warnsysteme. Als einzelne Nennungen wurden in dieser Kategorie Online-Meldesysteme, Alarmanlagen, Brandschutztüren, Videoüberwachung und Sicherheitsdienste genannt.
- Vorsorgemaßnahmen mit den Schwerpunkten Katastrophen- sowie Personalschutz, Notfallpläne und Intensivierung von Krisennetzwerken. Zu den häufigsten Nennungen in dieser Kategorie zählen die Intensivierung der Kooperation mit lokalen Akteuren des Krisen- und Katastrophenschutzes, die Qualifizierung der Beschäftigten im Krisen- und Katastrophenschutz, die Erarbeitung von Notfallplänen, AGAP- und BCP-Plänen, Blackout- und Evakuierungskonzepten sowie Übungen der Werksfeuerwehr und des Krisenstabs sowie weitere Reaktionspläne und Handlungsabläufe.
- Vorsorgemaßnahmen für Lieferketten, strukturellen Wandel, die Reorganisation von Produktionsprozessen und die Ermittlung alternativer Lieferketten. Vorsorgemaßnahmen für den Ausfall von Lieferketten, die Reorganisation und Umstrukturierung von Produktionsprozessen sowie von Entscheidungsketten (einschließlich der Auslagerung bestimmter Tätigkeiten und Prozesse an andere Standorte oder der Verlagerung von Personal in andere Bereiche) werden häufiger von großen Betrieben des sekundären Sektors genannt. Betriebe des sekundären Sektors sowie große Betriebe mit über 250 Mitarbeitenden nennen die Reorganisation von Produktionsprozessen signifikant häufiger als Betriebe des quartären Sektors und häufiger als kleinere Betriebe mit bis zu 50 Mitarbeitenden.
- Maßnahmen der Klimafolgenanpassung, z.B. Investitionen in Flut- und Hochwasserschutz, wurden bei großen Betrieben um 14 Prozentpunkte signifikant häufiger genannt als bei kleinen Betrieben. Weitere offene Nennungen, die der Kategorie Klimaanpassung zugeordnet werden können, sind: bauliche Ertüchtigung von Gebäuden, Installation von Brandschutztüren, Hitze- und Wasserschutz, Qualitätsmanagement, Vergrößerung von Abwasserkanälen, Verbesserung der Wasserführung durch Nivellierung, Bau von Wasserrückhaltebecken, Entsiegelung von Flächen sowie Installation von Wasserpumpen oder Sprinkleranlagen. Zudem wurden allgemeine Maßnahmen genannt, wie die Installation von Warnsystemen und die räumliche Verteilung von Standorten.

Der Zusammenhang zwischen Maßnahmen des Katastrophenschutzes und der Betriebsgröße lässt sich vermutlich über die Verfügbarkeit von Ressourcen erklären. Größere Unternehmen verfügen in der Regel über umfangreichere finanzielle Mittel sowie spezialisierte Abteilungen und implementieren systematischer strukturierte Risikoanalysen und gezielte Personalschulungen. Kleinere und mittlere Unternehmen hingegen weisen häufig weniger formalisierte Strukturen auf, wodurch der Katastrophenschutz in diesen Betrieben weniger umfassend organisiert ist und stärker von individuellen Entscheidungen abhängig bleibt.

4. Zivil- und Katastrophenschutz

Abbildung 6 zeigt die Unterschiede in der Implementierung von Reaktionsplänen für den Zivil- und Katastrophenschutz sowie deren mindestens jährliches Training über die Sektoren hinweg. Diese Unterschiede in der Ausgestaltung der Reaktionspläne spiegeln das Bewusstsein für potenziell disruptive Ereignisse wider.

Ein militärischer Ernstfall ist bei Betrieben des Sekundär- und Tertiärsektors in der Regel nicht Teil der Planungen. Im quartären Sektor – insbesondere in der Energie- und Wasserversorgung, der Telekommunikation sowie im Gesundheitswesen – verfügen nur rund 10 % der Betriebe über spezifische Reaktionspläne für einen militärischen Ernstfall. Diese Bereiche sind für das gesellschaftliche und wirtschaftliche Funktionieren zentral; ein Ausfall kann erhebliche soziale und ökonomische Folgen nach sich ziehen.

Die Analyse zeigt, dass Betriebe des quartären Sektors insgesamt besser auf disruptive Ereignisse vorbereitet sind und entsprechende Trainings signifikant häufiger durchführen als Betriebe des Sekundär- und Tertiärsektors. Vorbereitung und Training für den Verteidigungsfall sind sektorübergreifend jedoch weitgehend nicht vorhanden. Sekundär- und Tertiärsektor wurden in dieser Analyse zusammengefasst, da sich zwischen ihnen keine signifikanten Unterschiede in den betrachteten Maßnahmen zeigen.

Abbildung 6: Reaktionspläne und deren Training in Betrieben.

Die Auswertung zeigt, dass lediglich 10 % der Unternehmen des quartären Sektors über einen Plan für den militärischen Ernstfall verfügen. Vorbereitung und Training für den Verteidigungsfall sind sektorübergreifend als (weitgehend) nicht vorhanden zu bewerten.

Abbildung 7: Anteil von KRITIS-Ausfällen betroffener Betriebe (Bundesländern mit höherer Betroffenheit dunkler eingefärbt).

Regionale Unterschiede des Zivil- und Katastrophenschutzes

Abbildung 7 gibt einen Überblick darüber, in welchen Bundesländern Betriebe häufiger von Infrastrukturausfällen betroffen waren: Ausfälle der Energieversorgung (Strom, Gas, Fernwärme), von Kraftstofflieferungen, der Wasserversorgung oder des Verkehrsnetzes. Die Bundesländer Rheinland-Pfalz, Hessen,

Brandenburg, Hamburg und Berlin weisen im Vergleich zu den übrigen Bundesländern eine erhöhte Frequenz von Störungen infolge von Ausfällen kritischer Infrastrukturen auf. Literaturquellen deuten darauf hin, dass diese Bundesländer in höherem Maße von konventionellen Energiequellen abhängig sind, was auf einen möglichen Zusammenhang mit vermehrten Betriebsstörungen infolge von Ausfällen in der Energieversorgung hindeuten könnte [vgl. 13, S. 4; 14, S. 34–35].

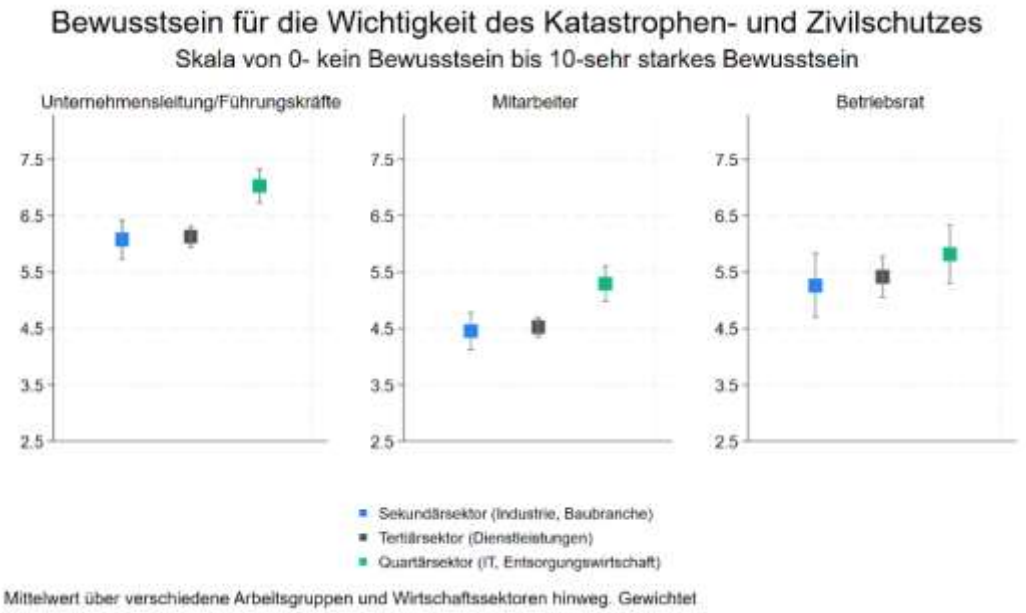
Sensibilisierung für Zivil- und Katastrophenschutz

Im Hinblick auf Stadt-Land-Unterschiede zeigen sich deutliche Differenzen – sowohl beim Bewusstsein für die Bedeutung des Katastrophen- und Zivilschutzes als auch bei der Vorbereitung auf eine Einbindung in Katastrophennetzwerke und der Bereitschaft, im Notfall Unterstützung zu leisten. In ländlichen und dünn besiedelten Regionen ist das Bewusstsein für die Wichtigkeit des Katastrophen- und Zivilschutzes höher ausgeprägt als in städtischen Räumen. Unternehmensleitungen und Führungskräfte messen der Bedeutung des Katastrophenschutzes dabei im Vergleich zu anderen Beschäftigtengruppen signifikant mehr Gewicht bei (Abbildung 8).

Signifikante Unterschiede zeigen sich zudem in den Kontakten zu den Behörden des Katastrophenschutzes sowie in der Bereitschaft, die Bevölkerung im Notfall zu unterstützen (Abbildungen 9 und 10). Diese Ergebnisse legen nahe, dass strukturelle Faktoren – etwa eine stärkere Dezentralisierung, eine geringere Dichte kritischer Infrastrukturen und längere Anfahrtswege in ländlichen und dünn besiedelten Regionen – die Risikowahrnehmung, den Grad der Vorbereitung und die Hilfsbereitschaft in diesen Gebieten beeinflussen.

Darüber hinaus bestehen signifikante Unterschiede in der Einschätzung der Bedeutung des Katastrophenschutzes zwischen Betrieben verschiedener Wirtschaftssektoren sowie zwischen großen und kleineren Unternehmen (Abbildung 8). Leitungs- und Führungskräfte in großen Betrieben des quartären Sektors messen dem Katastrophenschutz eine höhere Bedeutung bei als Leitungs- und Führungskräfte in kleinen und mittleren Betrieben sowie in Unternehmen des sekundären und tertiären Sektors.

Die Ergebnisse deuten darauf hin, dass Leitungs- und Führungskräfte in großen Betrieben des quartären Sektors insgesamt das höchste Bewusstsein für die Bedeutung des Katastrophen- und Zivilschutzes aufweisen. Die Einschätzungen von Betriebsräten und Mitarbeitenden fallen hingegen sektorübergreifend einheitlich niedrig aus Sicht der Befragten aus. Daraus folgt, dass das Bewusstsein für die Relevanz des Katastrophenschutzes in Betriebsräten und unter den Mitarbeitenden – insbesondere in kleinen und mittleren Unternehmen (KMU) – gezielt gestärkt werden sollte.



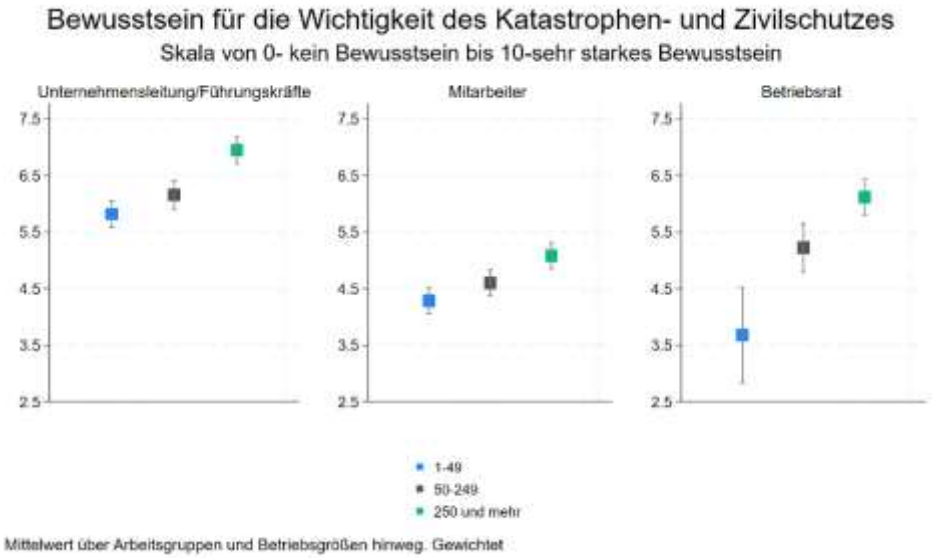


Abbildung 8: Bewusstsein für die Bedeutung des Katastrophenschutzes über Sektoren, Betriebsgrößen und Mitarbeitergruppen

Katastrophenschutznetzwerk

Die Vernetzung zwischen Betrieben, die Zusammenarbeit mit Hilfsorganisationen (Abbildung 9) und die Unterstützungsbereitschaft sind in ländlichen Regionen im Vergleich zu städtischen Gebieten signifikant stärker ausgeprägt. Betriebe in Städten müssen daher stärker dafür sensibilisiert werden, wie wichtig es ist, Mitarbeitende zur Beteiligung an Hilfsorganisationen zu ermutigen und dieses Engagement organisatorisch zu unterstützen.

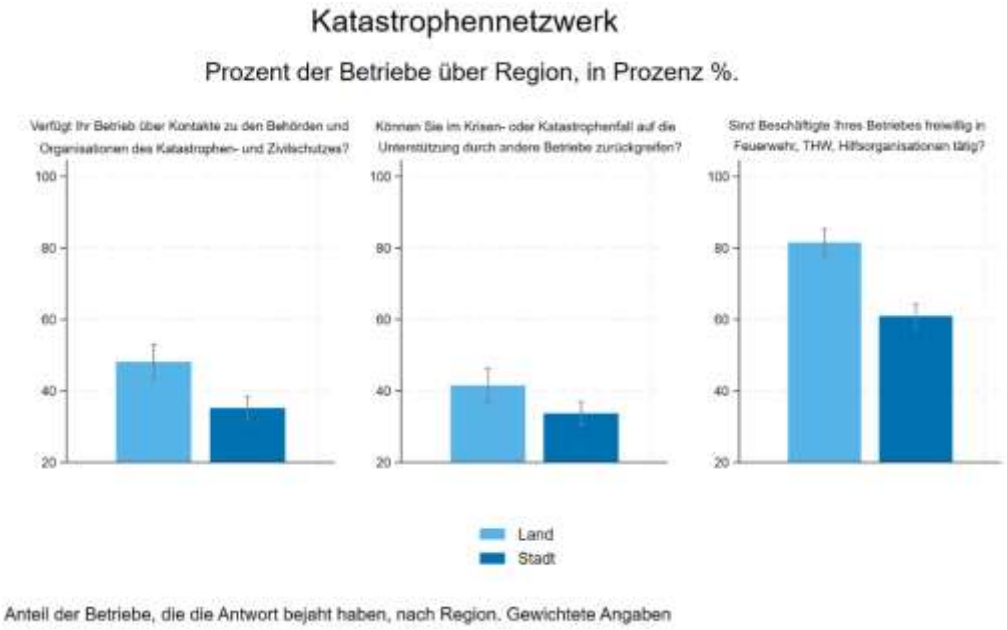


Abbildung 9: Katastrophennetzwerk

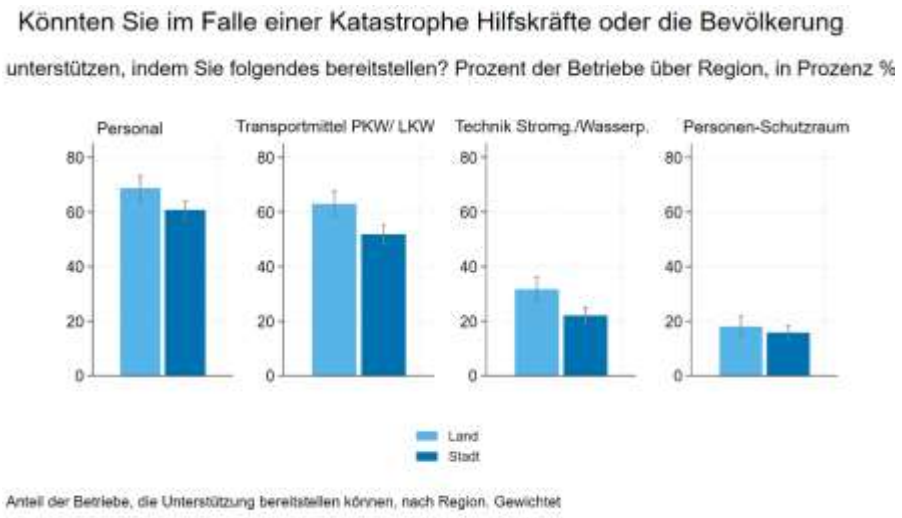


Abbildung 10: Engagement und Bereitschaft der Betriebe im Katastrophenfall

Sektorale Unterschiede oder Unterschiede nach Betriebsgröße – weder in der Vernetzung der Betriebe untereinander und mit Hilfsorganisationen noch in der Bereitschaft zur Hilfeleistung im Katastrophen- bzw. militärischen Ernstfall – konnten nicht festgestellt werden. Rund 55 % der Betriebe gaben an, im Notfall Personal und Transportmittel bereitstellen zu können.

Städtische Regionen sind weniger eng mit Hilfsorganisationen vernetzt und verfügen im Katastrophenfall über geringere Unterstützungskapazitäten in den Bereichen Technik, Transport und Personal (Abbildung 10). Daher sollten sowohl die Vernetzung städtischer Betriebe mit Katastrophenschutzbehörden und Hilfsorganisationen als auch die Schulung und Qualifizierung der Beschäftigten im Katastrophenschutz in städtischen Regionen gezielt ausgebaut werden.

Fazit: Unternehmen stehen vor einer Resilienz-Lücke – aber Lösungen sind machbar

Die Ergebnisse der Studie zeichnen ein klares Bild: Die Betroffenheit deutscher Unternehmen durch Krisen ist sehr unterschiedlich ausgeprägt. Während technologische und geopolitische Risiken wie Cyberangriffe oder Lieferkettenstörungen knapp die Hälfte der Betriebe treffen, sind andere Bedrohungen – etwa Naturkatastrophen oder Ausfälle kritischer Infrastrukturen – bislang seltener. Genau darin liegt jedoch ein zentrales Problem: Da weniger als 20 % der Unternehmen von diesen extremen Szenarien betroffen waren, bleibt die Vorsorge dafür häufig unzureichend. Zugleich wird deutlich, dass selbst seltene, aber schwerwiegende Ereignisse wie Stromausfälle oder militärische Krisen existenzbedrohende Folgen haben können – insbesondere für Betreiber kritischer Infrastrukturen.

Besonders ins Auge fällt der Mangel an Vorbereitung auf den Verteidigungsfall: Sektorübergreifend fehlen weitgehend entsprechende Notfallpläne und Trainings. Gerade für Betriebe im quartären Sektor – etwa in den Bereichen Energie, Gesundheitswesen oder IT – ist dies eine gravierende Lücke, da ihr Ausfall unmittelbare Auswirkungen auf die gesamte Gesellschaft hätte. Hinzu kommen deutliche Defizite bei kleinen und mittleren Unternehmen (KMU): Sie verfügen seltener über strukturierte Risikoanalysen, unterhalten weniger systematische Vorsorgemaßnahmen und sind im Katastrophenschutz weniger engagiert als Großbetriebe. Ressourcenknappheit und weniger formalisierte Abläufe erhöhen hier die Anfälligkeit.

Ein weiterer zentraler Befund betrifft regionale und sektorale Unterschiede: Ländliche Regionen weisen ein höheres Bewusstsein für Katastrophenschutz auf und sind stärker mit lokalen Hilfsorganisationen vernetzt, während städtische Gebiete deutlich zurückliegen. Gerade in Metropolen mit hoher Bevölkerungsdichte sind Risikobewusstsein, Zusammenarbeit mit Behörden und Bereitschaft zur Unterstützung im Ernstfall weniger ausgeprägt – obwohl Städte besonders anfällig für großflächige Infrastrukturausfälle, etwa im Strom- oder Verkehrsnetz, sind. Gleichzeitig zeigt die Studie, dass große Betriebe des quartären Sektors – etwa aus der IT- oder Gesundheitsbranche – deutlich resilienter aufgestellt sind als andere Branchen. Systematische Risikoanalysen, regelmäßige Notfallübungen und bessere finanzielle Ressourcen ermöglichen dort eine gezieltere Vorsorge.

Was jetzt zu tun ist: Vier Handlungsfelder für mehr Resilienz

Die Ergebnisse verdeutlichen, dass Unternehmen ihre Krisenvorsorge dringend ausbauen müssen – und zwar auf mehreren Ebenen:

(1) Risikobewusstsein schärfen: Viele Betriebe unterschätzen seltene, aber folgenschwere Szenarien wie Blackouts, Pandemien oder militärische Konflikte. Erforderlich sind realistische Bedrohungsanalysen und entsprechende Vorsorgemaßnahmen – unabhängig davon, ob ein Unternehmen bislang betroffen war oder nicht.

(2) KMU gezielt unterstützen: Kleine und mittlere Unternehmen benötigen Zugang zu praxistauglichen Instrumenten – etwa standardisierte Checklisten für Notfallpläne, Förderprogramme für Cybersicherheit oder Kooperationen mit lokalen Behörden und Hilfsorganisationen.

(3) Städtische Regionen nachrüsten: In Ballungsräumen sollten die Vernetzung mit Hilfsorganisationen und Behörden intensiviert, die Belegschaften für Katastrophenschutz sensibilisiert und klare Alarm- und Kommunikationswege etabliert werden.

(4) Lücken beim Verteidigungsfall schließen: Für Betreiber kritischer Infrastrukturen sollte die Entwicklung von Notfallplänen für militärische oder hybride Bedrohungen zur verbindlichen Praxis werden. Auch andere Branchen sollten prüfen, wie sie auf extreme Szenarien wie Sabotage, Desinformationskampagnen oder großflächige IT-Ausfälle reagieren können.

Resilienz ist kein Luxus, sondern eine Überlebensstrategie

Krisenvorbereitung ist kein „Nice-to-have“, sondern eine Frage der Existenzsicherung. Unternehmen, die heute in Notfallpläne, IT-Sicherheit, finanzielle Puffer und tragfähige Netzwerke investieren, sind morgen widerstandsfähiger – nicht nur im Ernstfall, sondern auch im Wettbewerb. Die positive Botschaft: Viele Maßnahmen lassen sich mit überschaubarem Aufwand umsetzen. Der entscheidende erste Schritt besteht darin, eigene Schwachstellen zu identifizieren und diese systematisch anzugehen. Denn eines ist sicher: Die nächste Krise kommt – die Frage ist, wie gut Unternehmen darauf vorbereitet sind.

Anhang

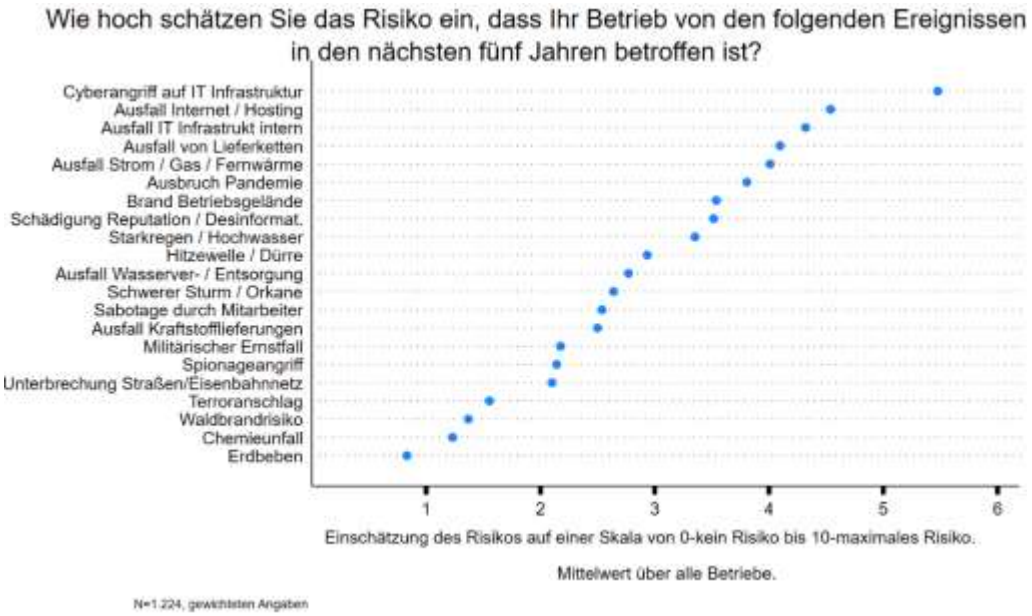


Abbildung 11: Durchschnittliche Angabe für 21 abgefragte Risiken aller an der Befragung teilnehmenden Betriebe. Die Antwortmöglichkeiten im Fragebogen reichten von 0 (kein Risiko) bis 10 (maximales Risiko); dargestellt ist hier der Mittelwert über alle Betriebe.

Quellen

[1] Bundesministerium des Innern. (29.08.2025). *Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen*. Retrieved from https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/reg-kritis-dachgesetz.pdf?__blob=publicationFile&v=1

[2] Seyghalani Talab, F., Ahadinezhad, B., Khosravizadeh, O., & Amerzadeh, M. (2024). A model of the organizational resilience of hospitals in emergencies and disasters. BMC Emerg Med, 24(1), 105. https://doi.org/10.1186/s12873-024-01026-6

[3] Meissner, J. O., Heike, M., & Sigrist, D. (2023). Organisationale Resilienz und Hochzuverlässigkeit. In J. O. Meissner, M. Heike, & D. Sigrist (Eds.), Organisationsdesign in einer komplexen und instabilen Welt: Einführung in Modelle und Konzepte sowie deren Anwendung (pp. 163-192). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-42339-1_9

[4] Miceli, A., Hagen, B., Riccardi, M. P., Sotti, F., & Settembre-Blundo, D. (2021). Thriving, Not Just Surviving in Changing Times: How Sustainability, Agility and Digitalization Intertwine with Organizational Resilience. Sustainability, 13(4), 2052.

[5] Bunde, N. (2023). BRANCHEN UND SEKTOREN: IFO BRANCHEN-DIALOG 2022. Wege zu mehr Resilienz in globalen Lieferketten. ifo Schnelldienst 76(1), 1-6. https://www.ifo.de/DocDL/sd-2023-01-bunde-industrieforum.pdf

[6] Prognos AG (Ed.). (2025). *Industrielle Resilienz und strategische Souveränität Deutschlands. Studie im Auftrag des Netzwerk Zukunft der Industrie e.V.* DCM Digitaldruck. https://buendnis-zukunft-der-industrie.de/wp-content/uploads/2025/05/PROGNOS_Industrielle-Resilienz-und-strategische-Souveraenitaet-Deutschlands-1.pdf

[7] World Economic Forum. (2026). The Global Risks Report 2026. 21st Edition. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

[8] Bundesagentur für Arbeit. (2026). Glossar: Ausländer. https://statistik.arbeitsagentur.de/DE/Navigation/Grundlagen/Definitionen/Glossar/Glossar-Nav.html?lv2=2018290&lv3=2059500

[9] Simonson, J., Kelle, N., Kausmann, C., Karnick, N., Arriagada, C., Hagen, C., Hameister, N., Huxhold, O., & Tesch-Römer, C. (2021). Volunteering in Germany: key findings of the Fifth German Survey on Volunteering (FWS 2019). Berlin: Bundesministerium für Familie, Senioren, Frauen und Jugend. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-74767-6

[10] Umweltbundesamt (UBA). (2011). HOCHWASSER VERSTEHEN, ERKENNEN, HANDELN! https://www.umweltbundesamt.de/system/files/medien/378/publikationen/uba_hochwasser_barrierefrei_new.pdf

[11] Bundesagentur für Arbeit. (2024). Aggregat "Kritische Infrastruktur". Auf Basis der Klassifikation der Wirtschaftszweige von 2008 (WZ 2008). https://statistik.arbeitsagentur.de/DE/Navigation/Grundlagen/Methodik-Qualitaet/Methodische-Hinweise/Uebergreifend/Methodische-Hinweise-Uebergreifend-Nav.html#:~:text=Aggregat%20%22Kritische%20Infrastruktur,2008

[12] Simonson, J., Vogel, C., & Tesch-Römer, C. (Eds.). (2017). Freiwilliges Engagement in Deutschland. Der Deutsche Freiwilligensurvey 2014. Springer VS Wiesbaden. https://doi.org/https://doi.org/10.1007/978-3-658-12644-5.

[13] Agentur für Erneuerbare Energien. (2022). Renews Kompakt. Energiemix und Energieeffizienz in den Bundesländern. Ausgabe 56. Agentur für Erneuerbare Energien e.V. https://www.unendlich-viel-energie.de/media/file/4851.AEE_RenewsKompakt_Energiemix_Effizienz_sep22.pdf

[14] Ministerium für Umwelt Klima und Energiewirtschaft Baden-Württemberg. (2024). Erneuerbare Energien in Baden-Württemberg 2023. Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg. Referat 64. https://um.baden-wuerttemberg.de/fileadmin/redaktion/m-um/intern/Dateien/Dokumente/2_Presse_und_Service/Publikationen/Energie/Eneuerbare-Energien-2023.pdf

[15] Ebnet, M. (2016). Institutionelle Veränderungen und ihre Wirkung auf Branchen. ifo Schnelldienst, 69(03), 41-44. https://www.econstor.eu/bitstream/10419/165706/1/ifosd-v69-2016-i03-p41-44.pdf

[16] Czernich, N., & Neumeier, J. (2022). BRANCHEN UND SEKTOREN: IFO BRANCHEN-DIALOG 2021. ifo Schnelldienst, 75(1). https://www.ifo.de/DocDL/sd-2022-01-einleitung-branchen-dialog.pdf

[17] BMUKN. (2026). Kommunalrichtlinie. Machen Sie Ihre Kommune lebenswerter – mit Klimaschutz, der sich lohnt. Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit. Zugriff 16.03.2026. https://www.klimaschutz.de/de/foerderung-der-nki/foerderprogramme/kommunalrichtlinie

[18] BMWE. (2026). Förderdatenbank. Bundesministerium für Wirtschaft und Energie. Zugriff 16.03.2026. https://www.foerderdatenbank.de/FDB/Content/DE/Foerdergeber/B/bmftr-bm_fuer_forschung_technologie_raumfahrt.html

[19] Möller, H. W. (2017). Im Regelkreis der Wirtschaft – Wirtschaftskreislauf und Wirtschaftsrechnung (VGR). In H. W. Möller (Ed.), Versuch und Irrtum: Wie Markt und Staat die Volkswirtschaft lenken (pp. 215-235). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-02312-6_13

[20] Bundesministerium der Justiz und für Verbraucherschutz. (2026). Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG). Bundesgesetzblatt, 2026(66), 1-22. https://www.recht.bund.de/bgbl/1/2026/66/VO

[21] IHK München und Oberbayern. (2025). Krisen, Konflikte, Katastrophen. Wie Sie Ihr Unternehmen in unsicheren Zeiten schützen. https://www.ihk-muenchen.de/Neu/Verteidigungsindustrie/Krisenvorsorgeplan_KMU_IHK_Muc_neu.pdf

Working Papers des Forschungsclusters OPAL der Helmut-Schmidt-Universität:

01. **Hintze, Astrid 2018:** Entwicklung und Implementierung einer Cluster-Dachmarke - Konzeptualisierung auf strukturationstheoretischer Basis am Beispiel des Luftfahrtclusters Metropolregion Hamburg

02. **Collien, Isabel 2018:** Functions of boundary spanning in context: A postcolonial, power-sensitive perspective

03. **Pötschke, Ivonne 2019:** The Ties That Bind: Exploring relationship-oriented values in family firms from employees' perspective

04. **Meister-Scheytt, Claudia 2019:** Governance von Universitäten: Das Beispiel österreichischer Universitätsräte

05. **Heller, Manja Annegret 2020:** Ist der Mehrwert auch mehr wert? – Eine qualitative Untersuchung von CSV in Clustern am Beispiel der Hamburg Aviation WoMen Group

06. **Spieß, Julia 2021**: Führung und Machtspiele in Veränderungsprozessen in kommunalen Krankenhäusern

07. **Holtmann, Doris & Matiaske, Wenzel 2021:** Betriebliche Arbeitszeitpolitiken, Exploration in ausgewählten Frauen- und Männerbranchen Ost- und Westdeutschlands

08. **Weingärtner, Simon & Köhler, Christoph 2021:** Sociological Labour Market Theories. A German Perspective on an International Debate

09. **Maas, Martina 2022:** Die Bedeutung der Kapitalmarktkommunikation für börsennotierte Unternehmen

10. **Hartong, Sigrid; Loft-Akhoondi, Anja; Brandau, Nina; Junne, Barbara; Czarnojan, Izabela; Tobias Scheytt 2023:** Auf dem Weg zur Digitalität in Schule, Zwischenbericht über Interventionen und Explorationen im Rahmen des Projekts „SMASCH - Smarte Schulen"

11. **Maas, Martina 2023:** Investor Relations als Beruf – Eine Untersuchung zur Professionalisierung der Kapitalmarktkommunikation von Unternehmen

12. **Maas, Martina & Matiaske, Wenzel 2023:** Regionale Personalarbeit – Eine Fallstudie aus Nordstadt

13. **Roggan, Michael 2024:** Der Einfluss der Rechtsform auf die Mitarbeiterbeteiligung - Eine kritische Betrachtung der Grenzen der Mitarbeiterkapitalbeteiligung

14. **Dario Azzellini 2024:** Crowdwork: Kontext und Kompetenzentwicklung in den Ländern Italien, den Niederlanden, Schweden und dem Vereinigten Königreich

15. **Tanja Klenk & Sabine Kuhlmann 2025:** Digitalisierung als Herausforderung und Chance für die Migrations- und Integrationsverwaltung – Expertise im Auftrag des Sachverständigenrat Integration & Migration

16. **Marleen J. Wohlert 2025:** Exzellenz in der hochschulischen Gründungsunterstützung – Eine Exploration der Erfolgsfaktoren exzellenter gründungsunterstützender Hochschulen in Deutschland

17. **Hans J. Pongratz 2025:** Individualisierte Beruflichkeit: Erosion von Berufsstrukturen und Kompensationsstrategien im Crowdworking – Eine Literaturstudie

18. **Marcus Eckelt 2025:** Auszubildende in Deutschland – Lebenssituation und digitale Praktiken

19. **Evita Milana 2025:** Navigating the Path to Market: an Empirical Analysis of University Inventions

Working Papers des Forschungsclusters OPAL der Helmut-Schmidt-Universität:

20. **Michael Lust 2026:** Das Phänomen „akademischer Widerstand“ an deutschen Hochschulen: Eine Untersuchung am Beispiel der Einführung von Qualitätsmanagement

21. **Tamara Böhm, Stefan Liebig & Wenzel Matiaske 2026:** Krisenresilienz deutscher Unternehmen

OPAL

WORKING PAPERS

ORGANISATION
PERSONAL
ARBEIT
LEADERSHIP

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg