MHP
A PORSCHE COMPANY

zentrum Nachhaltige Transformation
an der Quadriga Hochschule Berlin

STUDIE

Bedingt abwehrfähig?

Wie gut managt Deutschlands Mittelstand seine Resilienz – eine Bestandsaufnahme

Berlin, Oktober 2026

Eine Studie der MHP Management- und IT-Beratung GmbH und des zNT – zentrum Nachhaltige Transformation an der Quadriga Hochschule Berlin

MHP
A PORSCHE COMPANY

zentrum Nachhaltige Transformation
an der Quadriga Hochschule Berlin

Unternehmen des Mittelstands (bis 5 Mrd. Euro Umsatz) beschäftigen rund 80 Prozent der Arbeitnehmerinnen und Arbeitnehmer in Deutschland und erwirtschaften rund zwei Drittel des BIP. Sie sind damit ein Pfeiler der deutschen Wirtschaft – und in einer besonders heiklen Situation: Viele sehen sich als zu klein, um sich den Aufbau von Management-Ressourcen für die Verteidigungsbereitschaft leisten zu können, sind aber zugleich zu groß und zu stark in Lieferketten eingebunden, um die Folgen von Krisen und Konflikten auszusitzen.

Unser Partner für die Befragung von 1.000 Managerinnen und Managern aus Unternehmen mit 50 Mio. bis 5 Mrd. Euro Umsatz ist das Meinungsforschungsinstitut Civey; die Befragung lief vom 31. Juli bis 17. August 2026.

Executive Summary

Die Sicherheitslage in Deutschland hat sich verschärft: Neben militärischen Risiken prägen hybride Bedrohungen – Spionage, Sabotage, Desinformation und Einflussnahme – die Lage. Für Unternehmen heißt das: Versorgung, Lieferketten, Beschäftigte und der laufende Betrieb können erheblich beeinträchtigt werden, und das gilt auch für Unternehmen, die nicht zur kritischen Infrastruktur gehören. Sie müssen zudem bereit sein, über die Grenzen des eigenen Unternehmens hinaus Verantwortung für Sicherheit und Verteidigung zu übernehmen und sich als Teil einer nationalen Sicherheitsvorsorge zu verstehen.

Der deutsche Mittelstand ist bereit, Verantwortung zu übernehmen:

79%

sehen die Bedeutung von Krisenfestigkeit und Verteidigungsbereitschaft für ihre Branche als gewachsen an.

86%

wären bereit, Kapazitäten für die Landesverteidigung bereitzustellen.

93%

ordnen ihre Branche als relevant für die Versorgungssicherheit ein.

Doch zwischen dieser Einsicht und der Fähigkeit, im Krisen- oder Verteidigungsfall konkrete Beiträge zu leisten, klafft eine deutliche Lücke. Die Herausforderung liegt für diese Unternehmen in der operativen Übersetzung. Es braucht ein systematisches „Defense Management“, das klärt, welche Rolle die Unternehmen im Ernstfall übernehmen, welche Leistungen sie bereitstellen können, wie schnell und wie lange das möglich ist und von welchen Lieferketten, Energie-, Personal- oder IT-Strukturen sie dabei abhängig sind.

Fünf Fähigkeiten der Defense Readiness

Ziel dieses Managementansatzes ist die Defense Readiness. Sie beschreibt die Fähigkeit eines Unternehmens, auch in Krisen handlungsfähig zu bleiben und zugleich einen verlässlichen Beitrag zur Versorgungssicherheit und Landesverteidigung zu leisten. Defense Readiness basiert auf fünf wesentlichen Fähigkeiten:

- dem Verständnis der eigenen Rolle im Sicherheitskontext
- der Klarheit über Risiken
- der Transparenz über die Bedrohung der eigenen Lieferketten
- einem Business Continuity Management, das Alternativen und Notfallpläne entwickelt
- dem Ausbau der Cyberresilienz

Abbildung 1: Fünf Fähigkeiten, ein Management-Kreislauf

Quelle: MHP und zNT; Erfüllungsquoten: zNT-Auswertung der Civey-Rohdaten; n = 1.000 (Operationalisierung siehe Methodik).

I Die Lücke liegt im Management

Wie unsere Untersuchung zeigt, ist die Diskrepanz zwischen der häufig positiven Selbsteinschätzung vieler Unternehmen und den tatsächlich vorhandenen operativen Fähigkeiten frappierend:

3,1 % der befragten Unternehmen zeigt **alle notwendigen** Fähigkeiten der „Defense Readiness"

25 % erfüllt **keine** Voraussetzung

Die zentrale Lücke besteht also nicht im Bewusstsein einer möglichen Bedrohung – sie besteht im Management der Verteidigungsfähigkeit.

Besonders deutlich wird das bei der digitalen und organisatorischen Resilienz, also der Vorbereitung auf Lücken und Ausfälle durch (geübte) Alternativpläne und eine klare Zuordnung von Verantwortung. Im Schnitt fehlen den Unternehmen 5,5 von neun zentralen Maßnahmen zur Cyberresilienz, und 76 Prozent können einen vollständigen Ausfall ihrer IT-Systeme höchstens ein bis drei Tage überbrücken. Physische Kapazitäten allein reichen deshalb nicht aus: Ohne resiliente Steuerungs-, Kommunikations- und Wiederherstellungsprozesse sind sie im Ernstfall nur eingeschränkt nutzbar. Das gilt besonders für Logistik und Transport – Bereiche, die für Versorgung und militärische Mobilität zentral sind.

Was jetzt zu tun ist

1. **VERSTEHEN**
Die Unternehmen müssen ihre Rolle und ihre erfolgskritischen Fähigkeiten klären.

2. **VORBEREITEN**
Verteidigungs- und Bündnisszenarien müssen in die Strategie integriert, Risikomanagement und Business Continuity Management darauf ausgerichtet werden.

3. **VERNETZEN**
Kritische Lieferketten und Abhängigkeiten müssen transparent gemacht werden und klare Schnittstellen zwischen Staat, Zivilschutz und Unternehmen geschaffen werden – mit festen Ansprechpartnern und klaren Regeln.

4. **ERPROBEN**
Die Fähigkeiten müssen regelmäßig und gemeinsam geübt werden.

5. **VERBESSERN**
Übungen und Vorfälle müssen ausgewertet, Pläne und Kennzahlen laufend angepasst werden.

Anders formuliert: Defense Readiness entsteht, wenn dieses Ziel mit klaren Größen geplant und gesteuert wird und die Abläufe so eingeübt sind, dass sie auch unter Belastung funktionieren.

Vom Staat erwarten die Unternehmen – aus unserer Sicht zu Recht – Informationen darüber, was im Ernstfall von ihnen verlangt wird, sowie Koordination und Netzwerke für die Kooperation. Im Gegenzug sind sie selbst zur Zusammenarbeit bereit, etwa bei zentralen Plattformen, über die wichtige Daten wie Klarstände oder Einsatzfähigkeiten geteilt werden: 83 Prozent wären bereit, ihre verfügbaren Kapazitäten über eine bundesweite Plattform zu melden.

Einen zentralen Teil der Defense Readiness müssen die Unternehmen aber selbst herstellen. Die fünf Kernbereiche gehören zu den wichtigsten Aufgaben des Top-Managements – für viele Unternehmen seit Inkrafttreten des NIS-2-Umsetzungsgesetzes auch mit gesetzlich verankerter Verantwortung der Geschäftsleitung. Hier müssen die Geschäftsführungen in den nächsten Monaten erheblich aufholen und sich dieser Management-Herausforderung entschlossen widmen.

Inhalt

Deutschlands Mittelstand ist bereit, Verantwortung zu übernehmen

Unternehmen nehmen die sicherheitspolitische Veränderung nicht mehr als ausschließlich staatliche Angelegenheit wahr. Vier von fünf Entscheiderinnen und Entscheidern berichten, dass die Bedeutung von Krisenfestigkeit und Verteidigungsbereitschaft für ihre Branche in den vergangenen drei Jahren zugenommen hat.

Diese Wahrnehmung ist eine wichtige Voraussetzung für gesamtstaatliche Resilienz: Sie schafft Aufmerksamkeit, legitimiert Investitionen und erhöht die Bereitschaft, vorhandene Kapazitäten in eine gemeinsame Krisenvorsorge einzubringen.

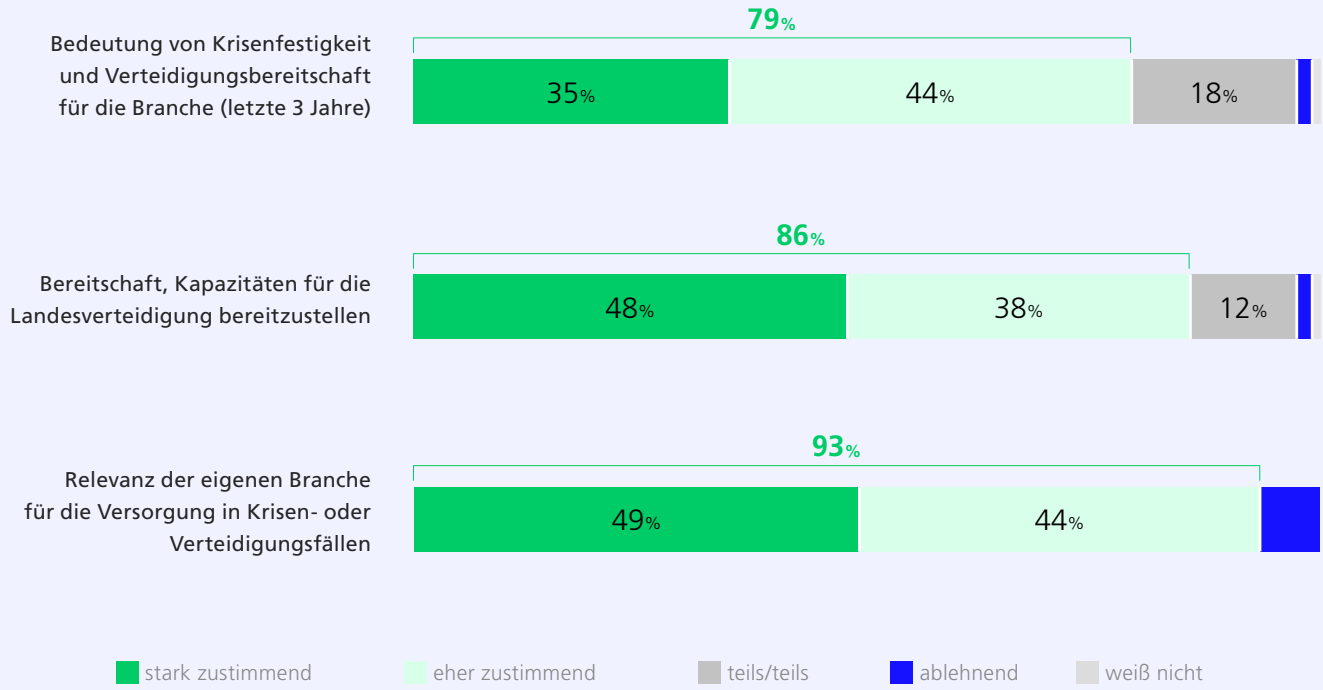


Abbildung 2: Bedeutung, Bereitschaft, Relevanz: hohe Zustimmung auf breiter Front

Quelle: Civey/MHP, Kommstudie Defense, Fragen 1, 2 und 5; n = 1.000.
Stark zustimmend: „eindeutig zugenommen", „ja, auf jeden Fall" bzw. „sehr relevant";

Die Bereitschaft ist dabei nicht auf einzelne Branchen begrenzt. 86 Prozent würden grundsätzlich Kapazitäten bereitstellen, 93 Prozent sehen die eigene Branche als relevant für die Versorgung Deutschlands in Krisen- oder Verteidigungsfällen. Damit ist die gesellschaftliche und wirtschaftliche Anschlussfähigkeit des Themas gegeben. Die Herausforderung liegt im nächsten Schritt: aus allgemeiner Bereitschaft konkrete Leistungsversprechen zu machen.

Die eigene Rolle ist oft ungeklärt

Eine Organisation kann nur dann verlässlich beitragen, wenn sie ihre mögliche Funktion kennt und bewertet hat. Die Befragung zeigt, dass dies keineswegs selbstverständlich ist: Nur 41,7 Prozent der Unternehmen haben ihre Rolle im Verteidigungsfall identifiziert und bewertet. Die Spannweite zwischen den Branchen beträgt 36,7 Prozentpunkte: Das Finanzwesen liegt mit 63,6 Prozent vorn, OEM-Zulieferer bilden mit 26,9 Prozent das Schlusslicht.

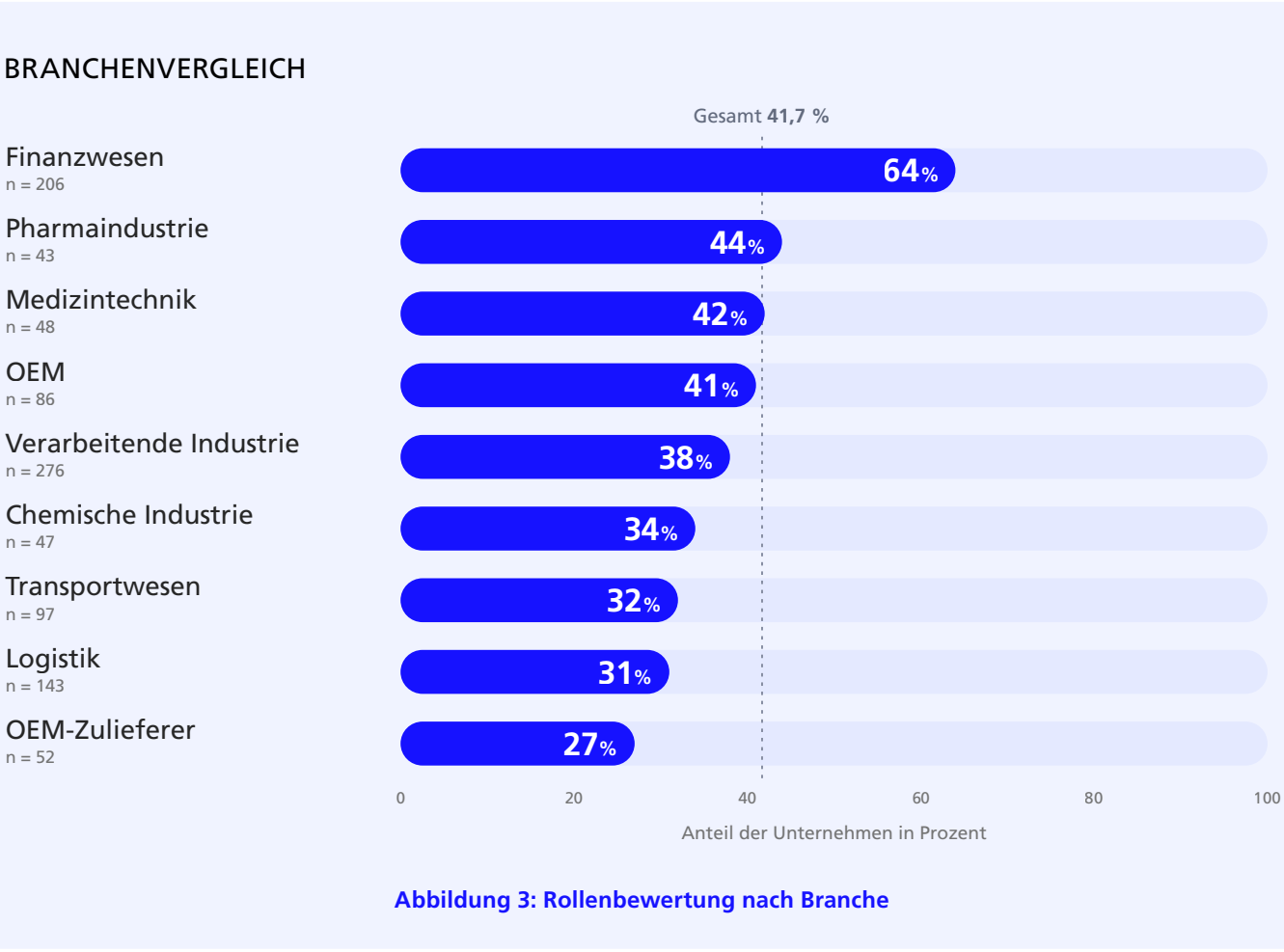


Abbildung 3: Rollenbewertung nach Branche

Quelle: zNT-Auswertung der Civey-Rohdaten (Frage 16); n = 998
(ohne „weiß nicht“ bei der Branche); Anteil „Rolle identifiziert und bewertet“.

Die Unterschiede sind statistisch signifikant, der Zusammenhang mit der Branche ist aber nur mäßig stark.[1] Das spricht gegen eine rein sektorale Erklärung. Entscheidend sind vielmehr konkrete Fähigkeiten, Abhängigkeiten, Kundenstrukturen und staatliche Schnittstellen, die in den Unternehmen unterschiedlich entwickelt sind. Eine Rolle dürfte auch die Regulierung spielen: Das Finanzwesen unterliegt mit der EU-Verordnung DORA seit Januar 2025 umfassenden Vorgaben zur digitalen operationalen Resilienz – und liegt auch bei der Cyberresilienz vorn (siehe Kapitel 2).

Die Größenkluft: Kleinere Unternehmen fallen zurück

Deutliche Unterschiede zeigen sich auch nach Unternehmensgröße. Von den Unternehmen mit weniger als 250 Mitarbeitenden hat nur gut ein Viertel (28 Prozent) seine Rolle identifiziert und bewertet; bei Unternehmen mit 1.000 bis 5.000 Mitarbeitenden ist es mehr als die Hälfte (54 Prozent). Die kleineren Unternehmen schätzen sich auch seltener als gut vorbereitet ein (65 gegenüber 80 Prozent) und bewerten die Zusammenarbeit zwischen Staat und Wirtschaft in der Krisenvorsorge deutlich kritischer: Nur 48 Prozent halten sie für gut, gegenüber 67 Prozent bei den Unternehmen mit 1.000 bis 5.000 Mitarbeitenden.[2]

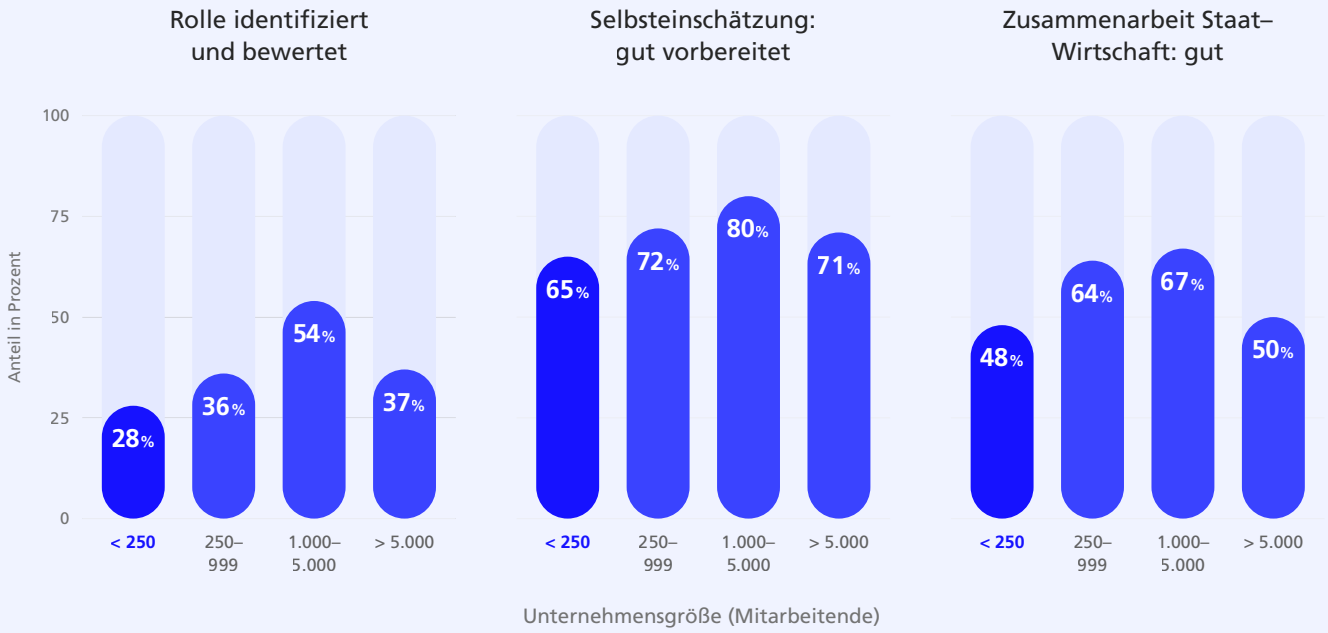


Abbildung 4: Die Größenkluft: Rollenbewertung, Selbsteinschätzung und Bewertung der Zusammenarbeit nach Unternehmensgröße

Quelle: zNT-Auswertung der Civey-Rohdaten (Fragen 13, 15 und 16); n = 1.000; gut = „sehr gut“ oder „eher gut“.

Auffällig ist, dass die sehr großen Unternehmen mit mehr als 5.000 Mitarbeitenden wieder schwächer abschneiden – bei der Rollenbewertung (37 Prozent) ebenso wie bei der Bewertung der Zusammenarbeit zwischen Staat und Wirtschaft (50 Prozent). Readiness wächst also nicht einfach mit der Größe. Am besten schneiden Unternehmen mit 1.000 bis 5.000 Mitarbeitenden ab, am schwächsten die kleineren – genau jene Unternehmen, die sich oft als zu klein für eigene Strukturen sehen, aber zu groß sind, um Krisen auszusitzen.

2. Defense Readiness beginnt im Management

Nach unserer Erfahrung aus Projekten und der Analyse der Daten sehen wir fünf zentrale Herausforderungen – die fünf Grundlagen der Defense Readiness:

- Kenntnis und Bewertung der eigenen Rolle
- Berücksichtigung von Verteidigungs- und Bündnisszenarien im Risikomanagement
- Transparenz über kritische Lieferketten und Abhängigkeiten
- funktionsfähiges Business Continuity Management
- organisatorische und technische Cyberresilienz einschließlich Wiederherstellungsfähigkeit

Entscheidend ist die Kombination dieser Fähigkeiten. Ein Unternehmen kann über Personal, Maschinen und Logistik verfügen und dennoch kurzfristig ausfallen, wenn Energie, IT, Zulieferer oder der Zugang zu Ansprechpartnern nicht abgesichert sind. Readiness beschreibt also die Funktionsfähigkeit des Gesamtsystems und seine Fähigkeit, Schocks und Krisen zu bewältigen.

KI-GESTÜTZTES ENGINEERING

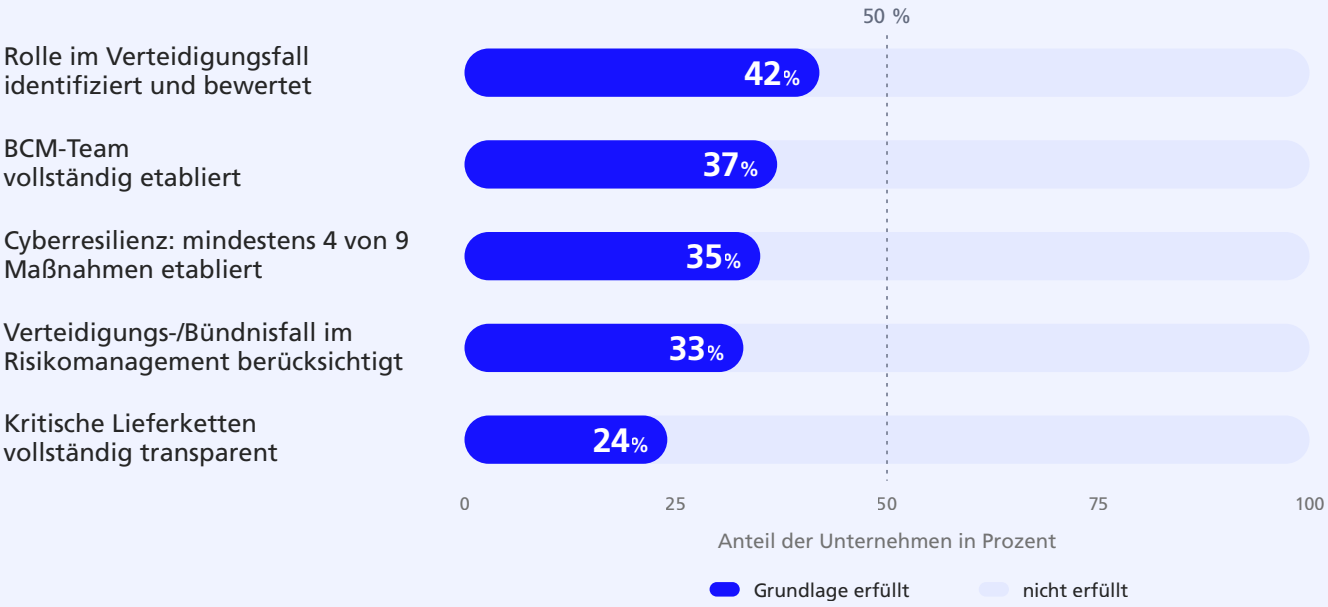


Abbildung 5: Die fünf Grundlagen: Keine erreicht die Hälfte der Unternehmen

Quelle: zNT-Auswertung der Civey-Rohdaten (Fragen 6, 7, 8, 9 und 16); n = 1.000.
Die Anteile beruhen auf unterschiedlichen Fragen und sind nur eingeschränkt vergleichbar; zur Indexbildung siehe Methodik.

Derzeit erfüllen nur 3,1 Prozent der befragten Unternehmen alle fünf Grundlagen. 25,1 Prozent erfüllen keine, 23,3 Prozent eine und weitere 23,3 Prozent zwei. Anders ausgedrückt: 48,4 Prozent der Unternehmen erfüllen keine oder nur eine Grundlage.

ERFÜLLTE GRUNDLAGEN DER VERTEIDIGUNGSFÄHIGKEIT

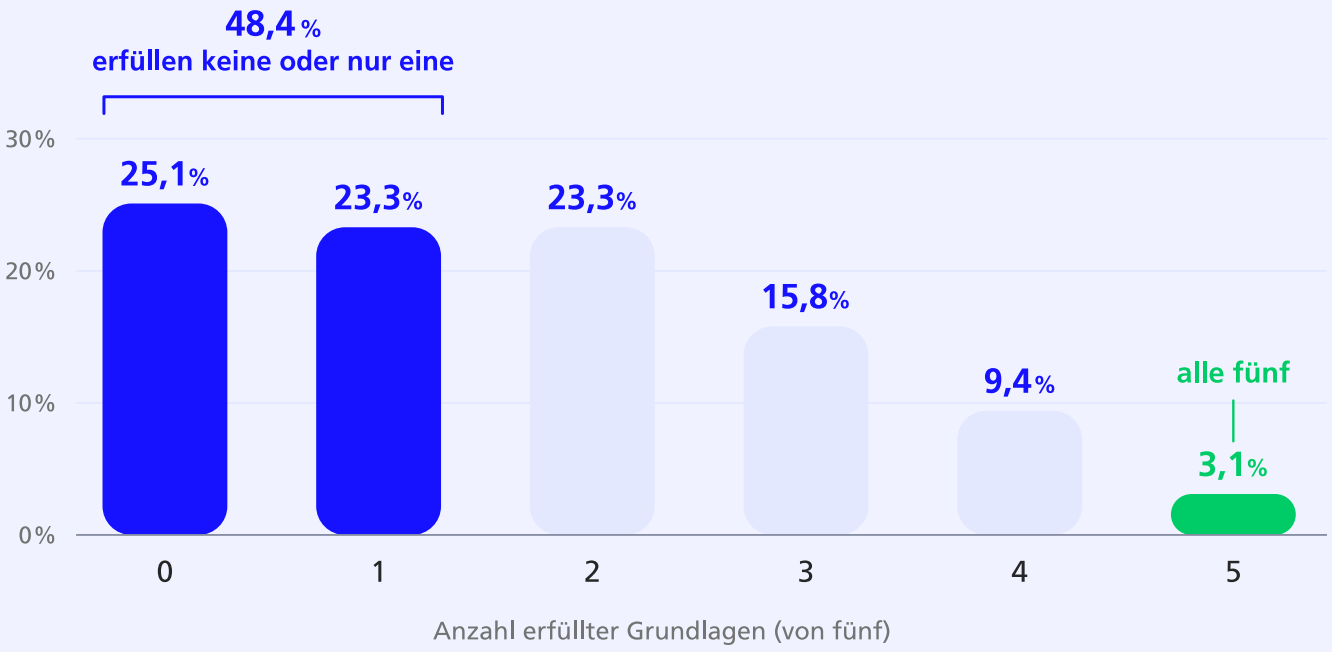


Abbildung 6: Defense Readiness im Überblick: Wie viele Grundlagen die Unternehmen erfüllen

Quelle: zNT-Auswertung der Civey-Rohdaten; n = 1.000; explorativer Index von 0 bis 5 erfüllten Grundlagen.

Diese Verteilung macht deutlich, warum eine einzelne positive Kennzahl – etwa eine hohe Produktionskapazität oder eine hohe Bereitschaft – kein ausreichender Readiness-Nachweis ist.

Die Ergebnisse sind als explorative Selbstauskunft zu interpretieren, nicht als objektives Audit.

Gerade darin liegt aber ihre Relevanz: Selbstbild und operative Vorbereitung entwickeln sich nicht synchron. Unternehmen können sich subjektiv gut aufgestellt fühlen, während das praktische Management der zentralen Bausteine noch nicht etabliert ist.

Das positive Selbstbild überdeckt operative Lücken

Der Zusammenhang zwischen dem eigenen Vorbereitungsurteil und der Zahl erfüllter Grundlagen ist eindeutig – aber nicht beruhigend. Von den Unternehmen, die keine oder nur eine Grundlage geschaffen haben, beurteilen sich dennoch 55,2 Prozent als sehr gut oder eher gut vorbereitet; selbst ohne eine einzige erfüllte Grundlage sind es 46,2 Prozent. Die Befunde deuten dort, wo operative Grundlagen fehlen, auf eine systematische Selbstüberschätzung hin.

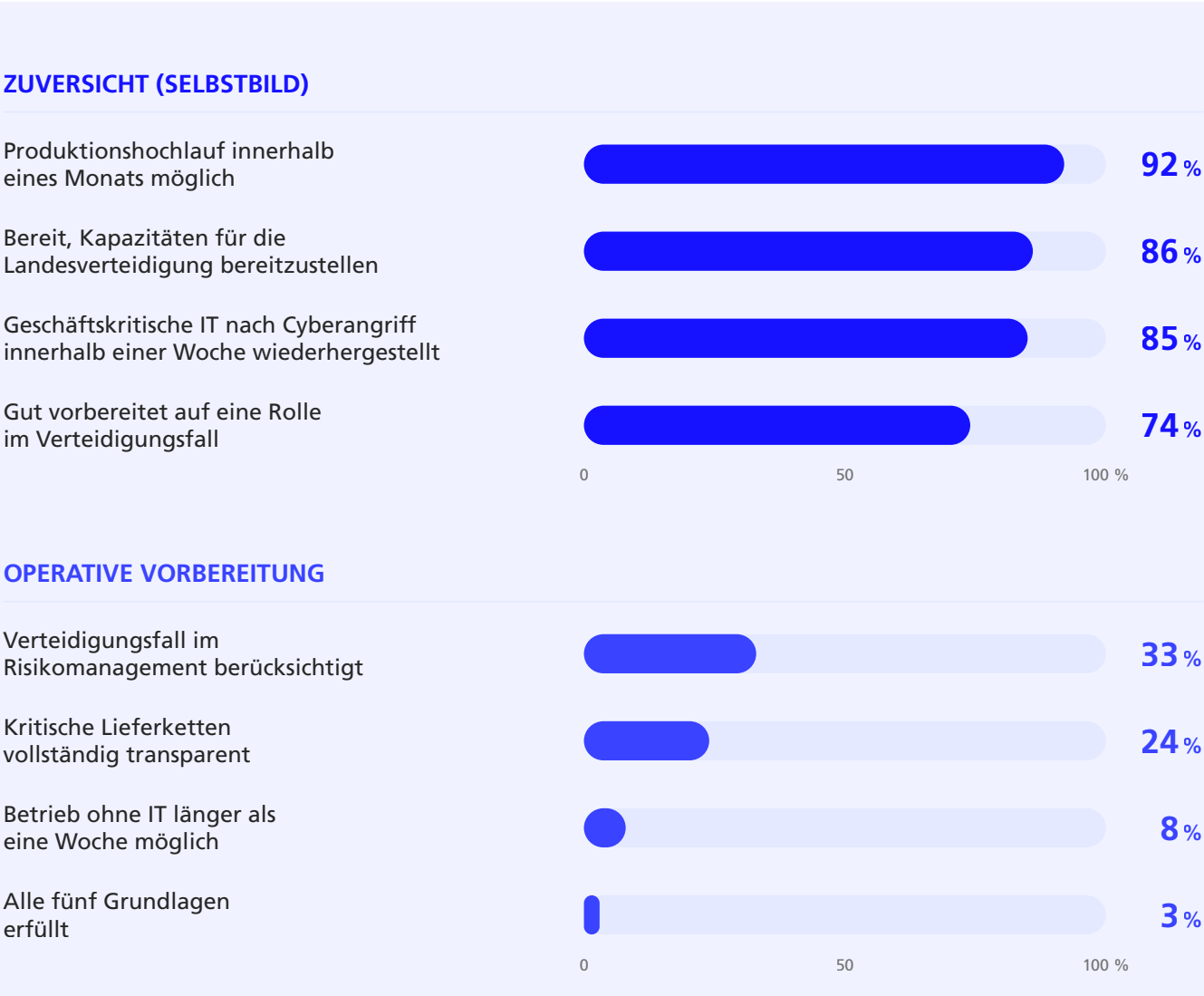


Abbildung 7: Zuversicht und operative Vorbereitung im Vergleich

Quelle: zNT-Auswertung der Civey-Rohdaten (Fragen 3, 5–11, 15 und 16); n = 1.000.

Für das Management folgt daraus eine praktische Konsequenz, die aus anderen Bereichen der Unternehmensführung bekannt ist: Readiness muss messbar sein und durch Szenarien und Tests validiert werden. Selbsteinschätzungen sind ein wichtiger Startpunkt, ersetzen aber weder Notfallübungen noch Wiederanlaufproben, Lieferkettenanalysen oder die Klärung staatlicher Ansprechpartner.

Regulatorischer Rückenwind: NIS-2 macht Resilienz zur Chefsache

Seit dem 6. Dezember 2025 gilt in Deutschland das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. Ob ein Unternehmen erfasst ist, hängt von der konkreten Einrichtungsart nach den Anlagen 1 und 2 des BSIG und – in der Regel – von Beschäftigtenzahl, Jahresumsatz und Jahresbilanzsumme ab. Für viele Einrichtungsarten liegt die Schwelle bei mindestens 50 Beschäftigten oder bei mehr als 10 Mio. Euro Jahresumsatz und zugleich mehr als 10 Mio. Euro Jahresbilanzsumme; für einzelne Einrichtungsarten gelten abweichende Regeln. Damit können unter anderem Unternehmen aus Transport und Logistik, Chemie, Pharma, Medizintechnik und Fahrzeugbau betroffen sein, nicht jedoch pauschal alle Unternehmen dieser Branchen. Das BSI rechnet mit rund 29.500 betroffenen Einrichtungen; bis Ende Juni 2026 hatten sich knapp 18.000 registriert.

Pflichten: Soweit das BSIG anwendbar ist, verlangt § 30 Risikomanagementmaßnahmen, die eng mit den in dieser Studie abgefragten Fähigkeiten zusammenhängen – unter anderem Business Continuity Management mit Backup- und Wiederherstellungskonzepten, die Bewältigung von Sicherheitsvorfällen, die Sicherheit der Lieferkette und Multi-Faktor-Authentifizierung. Für von DORA erfasste Finanzunternehmen haben die dortigen Vorgaben zum Cybersicherheitsrisikomanagement und zur Meldung erheblicher Sicherheitsvorfälle Vorrang, soweit sie mindestens gleichwertig sind.

Verantwortung: Für besonders wichtige und wichtige Einrichtungen verpflichtet § 38 BSIG die Geschäftsleitung, die nach § 30 zu ergreifenden Maßnahmen umzusetzen und zu überwachen. Sie muss regelmäßig an Schulungen teilnehmen und haftet gegenüber dem Unternehmen für schuldhaft verursachte Schäden. Vollständig an CIO oder CISO delegieren lässt sich diese Verantwortung nicht. Bei Finanzunternehmen unter DORA ist im Einzelfall zu prüfen, welche BSIG-Pflichten neben den vorrangigen DORA-Regelungen verbleiben.

Für einen Teil der befragten Unternehmen sind die hier gemessenen Lücken damit nicht nur ein strategisches, sondern auch ein regulatorisches Risiko. Zugleich bietet die Regulierung einen Hebel: Wer NIS-2- oder DORA-Pflichten ohnehin umsetzt, kann Verteidigungs- und Bündnisszenarien in dieselben Steuerungs-, Melde- und Übungsprozesse integrieren. Ergänzend verpflichtet das 2026 verabschiedete KRITIS-Dachgesetz die Betreiber kritischer Anlagen zu Maßnahmen der physischen Resilienz.

GESETZLICHE CYBERSICHERHEITSPFLICHTEN

Rund

29.500

Einrichtungen in Deutschland fallen unter NIS-2.

Verbindliche Anforderungen an die Cybersicherheit.

Cyberresilienz ist der sichtbarste Engpass

Keine der abgefragten Maßnahmen ist in der Mehrheit der Unternehmen etabliert. Multi-Faktor-Authentifizierung und 24/7-Monitoring erreichen jeweils 46 Prozent, ein Incident-Response-Team gibt es nur bei 27 Prozent.

Im Schnitt haben die Unternehmen 3,5 von neun Maßnahmen umgesetzt. Besonders problematisch ist die Kombination aus hoher Abhängigkeit von digitalen Systemen und unzureichender Wiederherstellungsorganisation.

CYBERRESILIENZ: UMGESETZTE MASSNAHMEN

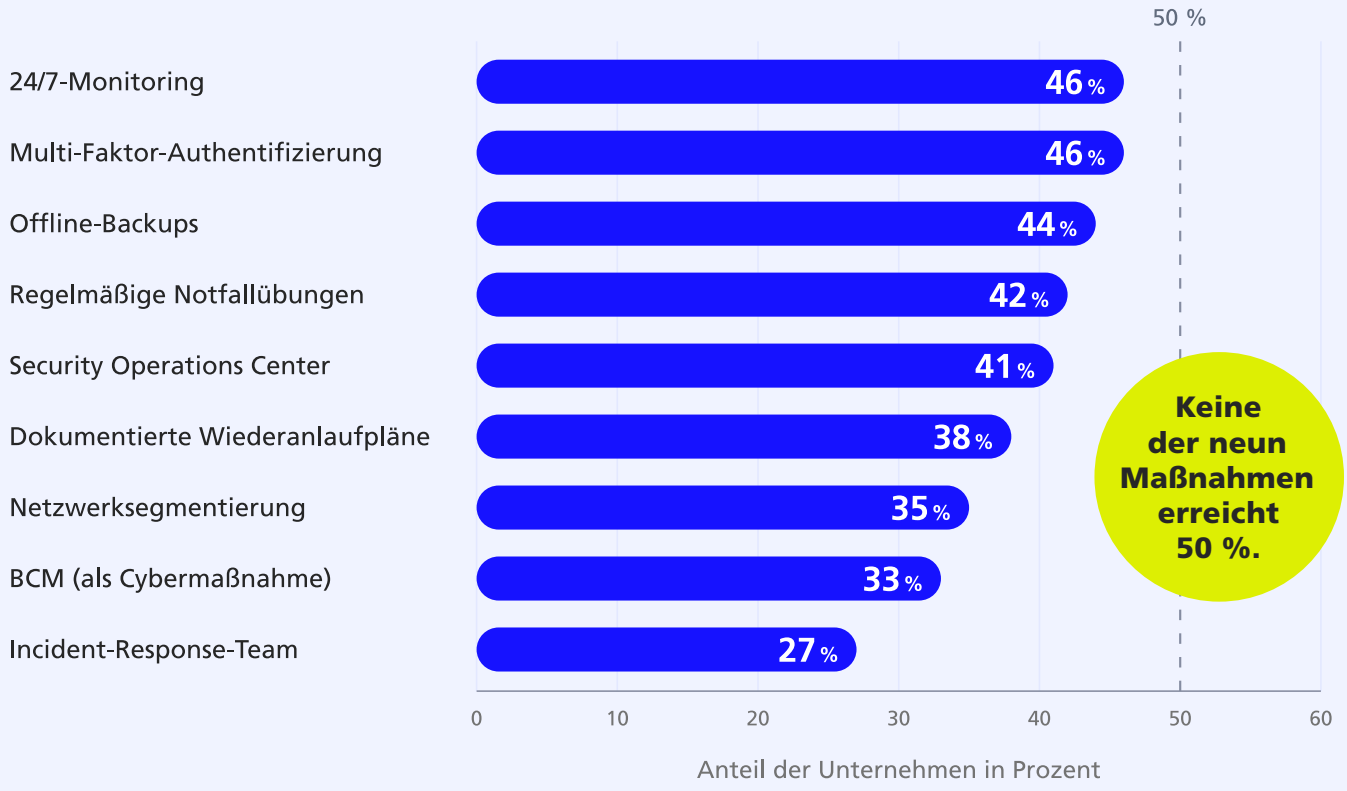
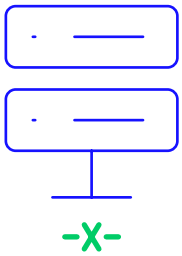


Abbildung 8: Cyberresilienz: Keine Maßnahme erreicht die Mehrheit

Quelle: Civey/MHP, Kommstudie Defense, Frage 9 (Mehrfachnennung); n = 1.000.

Das Muster ist in Logistik und Transport besonders ausgeprägt: Unternehmen dieser Branchen haben im Schnitt nur 2,7 beziehungsweise 2,8 der neun Maßnahmen etabliert, das Finanzwesen dagegen 4,2. Gerade Logistik und Transport sind für Versorgung und militärische Mobilität zentral. Ein physisch verfügbarer Fuhrpark oder eine Lagerkapazität hilft nur begrenzt, wenn Disposition, Kommunikation, Telematik oder Abrechnung nach einem Cyberangriff nicht verfügbar sind.

Durchhalten und Wiederherstellen sind zwei unterschiedliche Fähigkeiten



76 Prozent der Unternehmen können den Betrieb bei vollständigem Ausfall zentraler IT-Systeme höchstens ein bis drei Tage aufrechterhalten, 46 Prozent sogar höchstens 24 Stunden. Das beschreibt die Durchhaltefähigkeit.

BETRIEBSFÄHIGKEIT BEI IT-AUSFALL

Wie lange kann der Betrieb bei vollständigem IT-Ausfall aufrechterhalten werden?

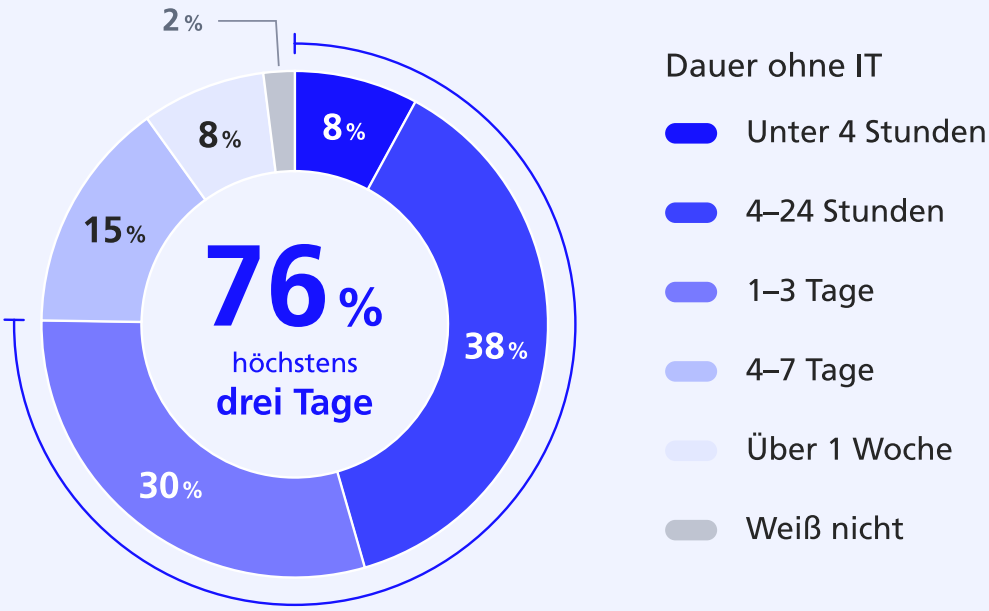


Abbildung 9: Belastbarkeit bei vollständigem IT-Ausfall

Quelle: Civey/MHP, Kommstudie Defense, Frage 10; n = 1.000.

Schneller Hochlauf, kurze IT-Ausfalltoleranz

Wie weit Selbstbild und Substanz auseinanderliegen, zeigt eine Kreuzauswertung: Von den Unternehmen, die ihre Produktion im Verteidigungsfall innerhalb einer Woche hochfahren könnten (69 Prozent aller Befragten), kann rund die Hälfte (51 Prozent) einen vollständigen IT-Ausfall höchstens 24 Stunden überbrücken. Bei denjenigen, die sich sogar einen Hochlauf binnen 24 Stunden zutrauen, sind es 61 Prozent – deutlich mehr als im Durchschnitt (46 Prozent). Ausgerechnet die zuversichtlichsten Unternehmen sind also besonders abhängig von funktionierender IT.

SCHNELLER HOCHLAUF, KURZER IT-PUFFER

Anteil der Unternehmen, die einen vollständigen IT-Ausfall höchstens 24 Stunden überbrücken können

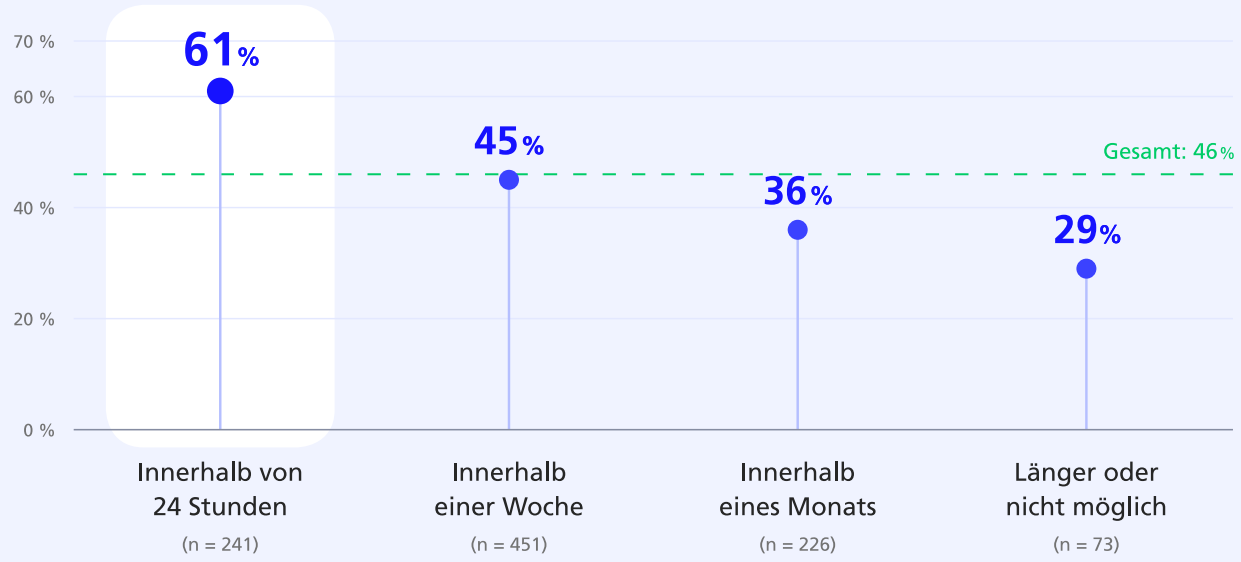


Abbildung 10: Schneller Hochlauf, kurze IT-Ausfalltoleranz

Quelle: zNT-Auswertung der Civey-Rohdaten (Fragen 3 und 10); n = 991 (ohne „weiß nicht" bei Frage 3).

Von der Durchhaltefähigkeit ist die Wiederherstellungsfähigkeit zu unterscheiden: In der zNT-Kreuzauswertung trauen es sich 92 Prozent der Unternehmen mit einer Ausfalltoleranz von bis zu drei Tagen zu, geschäftskritische IT-Systeme nach einem großflächigen Cyberangriff innerhalb einer Woche wiederherzustellen; bei Unternehmen mit mindestens vier Tagen Ausfalltoleranz sind es nur 68 Prozent.[3]

Eine längere Ausfalltoleranz ist damit nicht automatisch ein Zeichen besserer Readiness. Sie kann auch bedeuten, dass Wiederanlaufprozesse weniger dringlich entwickelt wurden.
Eine kausale Erklärung lässt sich aus dem Zusammenhang nicht ableiten; denkbar sind unterschiedliche technische Architekturen, dezentrale Systeme, analoge Fallback-Prozesse oder bewusst eingeplante Puffer. Der Befund zeigt jedoch: Unternehmen sollten Durchhalte- und Wiederherstellungsfähigkeit getrennt planen und testen.

3. Von der Bereitschaft zur Defense Readiness

Die Ergebnisse zeigen: Die Bereitschaft der Unternehmen ist hoch. Für die Defense Readiness kommt es darauf an, welche Leistungen sie im Ernstfall tatsächlich bereitstellen können – in welcher Menge, mit welcher Vorlaufzeit und über welchen Zeitraum. Dafür müssen Unternehmen ihre Rolle und ihre Fähigkeiten kennen, kritische Abhängigkeiten transparent machen, Szenarien vorbereiten, Wiederanlauf und Versorgung testen und die Schnittstellen zu staatlichen Stellen klären. Die folgenden Handlungsfelder orientieren sich am Management-Kreislauf.

Verstehen: Rolle und Leistungsfähigkeit kennen

Am Anfang steht die Bewertung der eigenen Rolle. Daraus sollte ein belastbares Leistungsprofil folgen: Welche Leistung kann in welcher Menge, mit welcher Vorlaufzeit, über welche Dauer, in welcher Qualität und unter welchen Abhängigkeiten bereitgestellt werden? Die größten Engpässe für zusätzliche Kapazitäten sehen die Unternehmen heute beim Personal (46 Prozent), bei der Materialverfügbarkeit (38 Prozent) und bei langen Genehmigungsprozessen (34 Prozent).

Die wichtigsten Aufgaben:

- kritische Leistungen beschreiben und dokumentieren
- Kapazitäten sowie Personal-, Energie- und IT-Abhängigkeiten quantifizieren
- Ansprechpartner ermitteln, Eskalationswege festlegen
- rechtliche und vertragliche Voraussetzungen prüfen

Der Staat kann Orientierung, Szenarien, Prioritäten und Ansprechpartner bereitstellen. Die Unternehmen müssen ihre eigene Leistungsfähigkeit jedoch selbst kennen und regelmäßig aktualisieren.

Vorbereiten: Szenarien in Risikomanagement und BCM integrieren

Nur 33 Prozent der Befragten haben einen Verteidigungs- oder Bündnisfall im Risikomanagement bereits berücksichtigt; bei knapp zwei Dritteln (65 Prozent) ist er bestenfalls in Planung. Ein Business-Continuity-Management-Team, das kritische Abläufe absichert, ist nur bei 37 Prozent vollständig etabliert. Damit fehlt vielerorts der Übergang von der allgemeinen Krisenvorsorge zu konkreten Verteidigungsszenarien. Wichtig ist, diese Szenarien in die Risiko-, Krisen- und Business-Continuity-Prozesse zu übersetzen, sofern es sie schon gibt. Für kritische Leistungen sind Mindestbetriebsniveaus, Wiederanlaufzeiten, alternative Ressourcen und klare Verantwortlichkeiten festzulegen.

Dazu sind vier Schritte nötig:

1. Verteidigungsszenarien in die Risikosteuerung aufnehmen
2. Geschäftsprozesse priorisieren, Mindestbetriebsniveaus definieren
3. Wiederanlaufpläne für IT, Energie, Personal und Logistik dokumentieren
4. Regelmäßige Übungen mit realistischen Annahmen durchführen

Die Kernfrage lautet nicht, ob ein Plan existiert, sondern ob er unter Zeitdruck funktioniert. Übungen sollten deshalb auch Informationsmangel, Ausfälle von Dienstleistern und widersprüchliche Lagebilder simulieren.

Vernetzen: Lieferketten und Kapazitäten sichtbar machen

Bei drei Vierteln der Unternehmen sind die kritischen Lieferketten über mehrere Zuliefererstufen hinweg für Außenstehende nicht vollständig transparent; nur 24 Prozent bezeichnen sie als vollständig transparent. Wer seine Lieferketten nicht offenlegen kann, kann sie auch nur eingeschränkt in ein gemeinsames Lagebild einbringen. Befragte aus Großstädten berichten dabei etwas häufiger von zumindest überwiegend transparenten Lieferketten als Befragte aus dem ländlichen Raum (74 gegenüber 63 Prozent). Da die Befragung den Wohnort der Entscheiderinnen und Entscheider erfasst, nicht den Unternehmensstandort, ist das allerdings nur ein Indiz für regionale Unterschiede.[4]

Die wichtigsten Schritte:

- kritische Lieferketten und Single Points of Failure erfassen
- alternative Bezugsquellen und regionale Engpässe bewerten
- verfügbare Kapazitäten mit Vorlaufzeit und Durchhaltehorizont melden
- Datenqualität, Aktualisierungszyklen und Zugriffsrechte festlegen

Gleichzeitig wären 83 Prozent bereit, an einer bundesweiten Plattform zur Meldung verfügbarer Kapazitäten teilzunehmen. Darin liegt ein konkreter Ansatzpunkt: Bereitschaft kann in einen aktuellen, strukturierten Lage- und Kapazitätsdatensatz übersetzt werden. Kritische Kapazitäten und Abhängigkeiten müssen dafür nicht nur transparent, sondern in einer Form verfügbar sein, die operative Steuerung ermöglicht. Dazu gehören neben verfügbaren Mengen insbesondere Vorlaufzeiten, Durchhaltefähigkeit, Abhängigkeiten, Alternativen und der aktuelle Status.

Eine Plattform ersetzt keine Entscheidung. Sie kann aber die Voraussetzung dafür schaffen, dass Staat und Wirtschaft im Ernstfall mit demselben Lagebild arbeiten. Dafür braucht es nicht zwingend ein neues zentrales Datensilo: Bestehende Systeme und Datenquellen können interoperabel verbunden werden, sodass ein gemeinsames Lagebild über Kapazitäten, Engpässe und Alternativen entsteht. Der Mehrwert liegt in der Fähigkeit, auf dieser Datengrundlage zu priorisieren, umzusteuern und auf Ausfälle zu reagieren.

Erproben: Schnittstellen und Zusammenarbeit testen

Von staatlicher Seite wünschen sich die Unternehmen vor allem regelmäßigen Informationsaustausch (43 Prozent), klare rechtliche Rahmenbedingungen (40 Prozent), finanzielle Anreize (39 Prozent) und standardisierte Prozesse (38 Prozent); feste Ansprechpartner nennt ein Drittel (33 Prozent). Diese Prioritäten verweisen auf ein Koordinationsproblem: Die Bereitschaft ist vorhanden, doch die Wege, auf denen sie aktiviert werden kann, sind nicht ausreichend standardisiert. Auffällig ist, dass gemeinsame Übungen mit 26 Prozent am seltensten genannt werden – obwohl sich gerade dort zeigt, ob Absprachen im Ernstfall tragen.

INFORMATIONSAUSTAUSCH LIEGT VOR

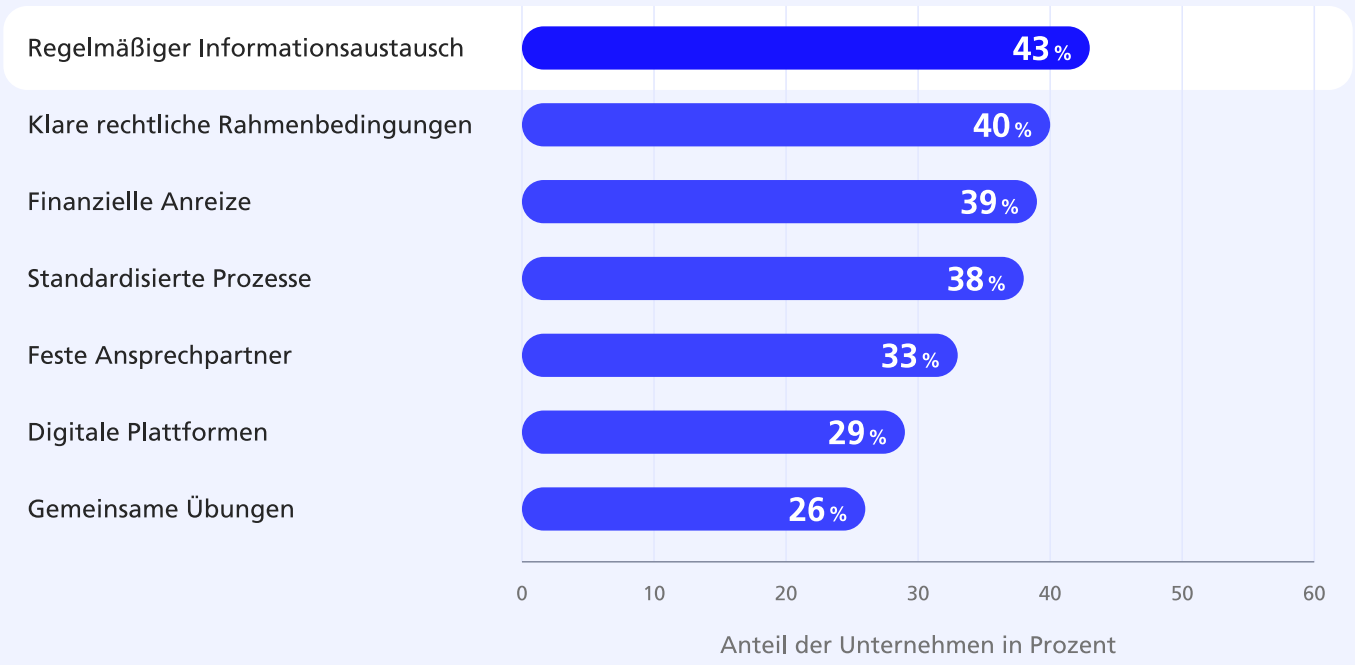


Abbildung 11: Was die Mitwirkung im Krisenfall am stärksten erleichtern würde

Quelle: Civey/MHP, Kommstudie Defense, Frage 12 (staatliche Unterstützungsangebote, Mehrfachnennung); n = 1.000.

Dafür braucht es:

- gemeinsame Übungen von Staat, Unternehmen und kritischen Dienstleistern
- feste Ansprechpartner mit Stellvertretungen und Eskalationsregeln
- Klärung von Haftung, Vergütung, Priorisierung und Informationsschutz
- Auswertung jeder Übung mit verbindlichen Verbesserungsmaßnahmen

Belastbare Kooperation zeigt sich daran, ob Absprachen auch unter Zeitdruck funktionieren.

Verbessern: Readiness messen und nachsteuern

Defense Readiness muss regelmäßig überprüft und angepasst werden. Jede Übung, jeder Vorfall und jede Veränderung der Lage zeigt, wo Pläne, Kapazitätsangaben oder Schnittstellen nicht tragen. Unternehmen sollten deshalb wenige, klare Kennzahlen definieren – etwa den Anteil kritischer Leistungen mit dokumentiertem Leistungsprofil, getestete Wiederanlaufzeiten oder die Aktualität gemeldeter Kapazitäten – und sie regelmäßig in der Geschäftsleitung nachhalten. Wo NIS-2 greift, lassen sich diese Kennzahlen mit den ohnehin geforderten Überwachungs- und Berichtspflichten verbinden.

Staat und Wirtschaft brauchen einen gemeinsamen Handlungsrahmen

Die Befunde sprechen für eine arbeitsteilige Verantwortung. Unternehmen sind für die Kenntnis ihrer Fähigkeiten, ihre interne Resilienz und die Aktualität ihrer Daten verantwortlich. Der Staat ist gefordert, Szenarien, Prioritäten, Ansprechpartner, rechtliche Rahmenbedingungen und sichere Austauschformate bereitzustellen. Wie viel hier noch zu tun ist, zeigt die Bewertung der bisherigen Zusammenarbeit in der Krisenvorsorge: Nur 62 Prozent der Unternehmen halten sie für gut, 17 Prozent für schlecht. Im Transportwesen (53 Prozent) und in der Logistik (54 Prozent) fällt das Urteil deutlich zurückhaltender aus als im Finanzwesen (78 Prozent), ebenso bei kleineren Unternehmen (48 Prozent).

Wer was leisten muss

Unternehmen

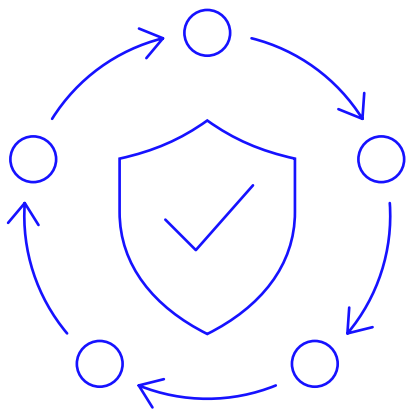
- eigene kritische Leistungen und Kapazitäten kennen
- Szenarien und Wiederanlauf vorbereiten
- Daten und Leistungsprofile aktuell halten
- Fähigkeiten regelmäßig testen

Staat

- Szenarien, Anforderungen und Prioritäten definieren
- Ansprechpartner und Aktivierungswege benennen
- rechtliche Rahmenbedingungen schaffen
- sichere Informations- und Austauschwege ermöglichen
- Koordination und übergreifendes Lagebild organisieren

Gemeinsam

- Kapazitäten erfassen und Abhängigkeiten sichtbar machen
- Lagebild herstellen, Leistungen aktivieren, Engpässe steuern
- Übungen durchführen, Schnittstellen verbessern und die Zusammenarbeit regelmäßig erproben



Das Ziel ist ein Defense-Readiness-Management, das aus fünf wiederkehrenden Tätigkeiten besteht: verstehen, vorbereiten, vernetzen, erproben und verbessern. So wird aus einer Absicht eine nachweisbare Fähigkeit.

4. Fazit: Von der Bereitschaft zur Verteidigungsfähigkeit

Die deutsche Wirtschaft ist in hohem Maße bereit, im Krisen- und Verteidigungsfall Verantwortung zu übernehmen. Die Studie zeigt jedoch eine klare Lücke zwischen Bereitschaft, Selbstbild und operativer Vorbereitung.

Die Lücke lässt sich nicht durch eine einzelne Investition schließen. Sie betrifft Rollenverständnis, Risikomanagement, Lieferketten, BCM, Cyberresilienz und die Zusammenarbeit mit staatlichen Stellen. Besonders kritisch ist, dass Logistik und Transport – zentrale Bereiche der Versorgung und militärischen Mobilität – überdurchschnittlich große Lücken bei der Cyberresilienz aufweisen und kleinere Unternehmen bei der Klärung ihrer Rolle deutlich zurückliegen.

Defense Readiness ist deshalb kein einmal erreichter Zustand, sondern ein kontinuierlicher Managementprozess. Unternehmen müssen ihre Fähigkeiten kennen, Szenarien durchspielen, Daten aktuell halten und Wiederanlaufprozesse testen. Staatliche Stellen müssen dafür klare Rahmenbedingungen, Ansprechpartner und sichere Austauschwege schaffen. Erst das Zusammenspiel beider Seiten macht wirtschaftliche Leistungsfähigkeit im Ernstfall nutzbar.

Defense Readiness heißt, Rolle, verfügbare Leistung, Abhängigkeiten und Durchhaltefähigkeit zu kennen und regelmäßig zu überprüfen. Am Ende steht eine einfache Frage: **Was kann ein Unternehmen im Ernstfall tatsächlich leisten – in welcher Menge, mit welcher Vorlaufzeit, über welchen Zeitraum und unter welchen Bedingungen?** Erst wenn diese Leistungsfähigkeit bekannt, planbar und im Bedarfsfall aktivierbar ist, wird aus Bereitschaft belastbare Verteidigungsfähigkeit.

Methodik und Einordnung

Datengrundlage

Die Studie basiert auf einer Befragung von 1.000 privatwirtschaftlichen Entscheiderinnen und Entscheidern in Deutschland, durchgeführt von Civey im Zeitraum vom 31. Juli bis 17. August 2026. Befragt wurden Personen ab Teamlead-Ebene aus verschiedenen Branchen in Unternehmen mit einem Jahresumsatz von mindestens 50 Mio. und höchstens 5 Mrd. Euro. Die Stichprobe umfasst die verarbeitende Industrie (28 Prozent), das Finanzwesen (21 Prozent), Logistik (14 Prozent), Transportwesen (10 Prozent), OEM (9 Prozent), OEM-Zulieferer (5 Prozent) sowie Medizintechnik, chemische und pharmazeutische Industrie (je 4 bis 5 Prozent). Der ausgewiesene statistische Fehler des Gesamtergebnisses beträgt 3,1 Prozentpunkte.

Auswertung

Die Auswertung stützt sich auf die Ergebnisberichte von Civey sowie auf eigene Auswertungen der Rohdaten durch das zNT (Kreuztabellen, Signifikanztests, Index). Alle Werte in dieser Studie wurden aus den Rohdaten berechnet und gerundet; gegenüber den Civey-Ergebnisberichten, die gerundete Einzelwerte addieren, kann es daher zu Abweichungen von einem Prozentpunkt kommen. Summen können von 100 Prozent abweichen.

Der Readiness-Index orientiert sich an fünf Grundlagen. Eine Grundlage gilt als erfüllt, wenn das jeweilige Kriterium zutrifft; die Summe ergibt einen explorativen Index von 0 bis 5. Er dient der Strukturierung und ersetzt kein objektives Audit.

Grundlage	Frage	Kriterium „erfüllt“	Anteil
Rollenbewertung	16	„Rolle identifiziert und bewertet“	41,7%
Risikomanagement	6	Verteidigungs- oder Bündnisszenarien „bereits berücksichtigt“	33,0%
Lieferkettentransparenz	7	kritische Lieferketten für Außenstehende „vollständig transparent“	23,7%
Business Continuity Management	8	BCM-Team „vollständig etabliert“	36,8%
Cyberresilienz	9	mindestens 4 von 9 abgefragten Maßnahmen etabliert	35,2%

Quelle: zNT-Auswertung der Civey-Rohdaten; n = 1.000

Grenzen der Aussagekraft

Die Ergebnisse beruhen auf Selbstauskünften. Sie messen Wahrnehmungen, den angegebenen Stand von Maßnahmen und explorative Zusammenhänge, nicht die technische oder organisatorische Wirksamkeit im Einzelfall. Branchen- und Größenvergleiche sind bei kleinen Teilgruppen vorsichtig zu interpretieren; sehr kleine Gruppen werden nicht gesondert ausgewiesen. Regionale Auswertungen beziehen sich auf den Wohnort der Befragten, nicht auf den Unternehmensstandort. Korrelationen werden nicht als Kausalnachweise verstanden.

Quellenverzeichnis

Civey/MHP: Kommstudie Defense, Befragung vom 31.07. bis 17.08.2026, n = 1.000.

zNT – zentrum Nachhaltige Transformation: eigene Auswertungen der Civey-Rohdaten.

Bundesamt für Sicherheit in der Informationstechnik (BSI): NIS-2-Pflichten; NIS-2 in Zahlen (Stand: 30.06.2026), www.bsi.bund.de.

NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz (NIS2UmsuCG), in Kraft seit 6. Dezember 2025; §§ 30, 38 BSIG.

KRITIS-Dachgesetz (KRITISDachG), BGBl. 2026 I Nr. 66.

Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA), anwendbar seit 17. Januar 2025.

Anmerkungen

[1] Der Zusammenhang zwischen Branche und vollständiger Rollenbewertung ist statistisch signifikant ($\chi^2(8) = 57{,}7$; $p < 0{,}001$), bleibt in seiner Stärke aber begrenzt (Cramérs V = 0,24).

[2] Gruppengrößen: unter 250 Mitarbeitende: n = 141; 250 bis 999: n = 384; 1.000 bis 5.000: n = 391; über 5.000: n = 84. Die Unterschiede sind jeweils statistisch signifikant (Rollenbewertung: $\chi^2(3) = 41{,}2$; $p < 0{,}001$; Selbsteinschätzung: $\chi^2(3) = 13{,}2$; $p = 0{,}004$; Zusammenarbeit: $\chi^2(3) = 21{,}1$; $p < 0{,}001$). Die Gruppe unter 50 Mitarbeitenden wird wegen der geringen Fallzahl (n = 28) nicht gesondert ausgewiesen.

[3] Basis: Unternehmen mit gültiger Angabe zur Wiederherstellungsdauer (Frage 11).

[4] Anteil „vollständig“ oder „überwiegend transparent“: großstädtisch 74,1 Prozent (n = 421), klein-/mittelstädtisch 65,8 Prozent (n = 404), ländlicher Raum 63,4 Prozent (n = 175); $\chi^2(2) = 9{,}5$; $p = 0{,}008$; Cramérs V = 0,10.

Layout & Design: www.freiland-design.de

Kontakt

MHP Management- und IT-Beratung GmbH

John Eisenhauer
Partner Public & Defense
john.eisenhauer@mhp.com

zNT – zentrum Nachhaltige Transformation an der Quadriga Hochschule Berlin

Prof. Dr. Torsten Oltmanns
Managing Partner
torsten.oltmanns@znt-berlin.com

MHP Management- und IT-Beratung GmbH
Film- und Medienzentrum
Königsallee 53
D-71638 Ludwigsburg
E-Mail info@mhp.com