2026

Globaler Risiko- und Resilienz-Ausblick

Zukunftsfähige Strategien in einer Welt wachsender Risiken

everbridge™

Inhaltsverzeichnis

Vorwort

Bei meinen Gesprächen mit Führungskräften auf der ganzen Welt taucht immer wieder ein Thema auf: Die Natur des Risikos hat sich verändert. Wir sind in eine Ära eingetreten, in der Störungen schneller auftreten, stärker vernetzt sind und sich deutlich schwerer eindämmen lassen. Ein Cybervorfall kann sich innerhalb von Minuten auf Lieferketten, Betriebsabläufe und die Sicherheit auswirken. Risiken warten nicht, bis sie an der Reihe sind – sie kollidieren. Diese expandierende Risikozone definiert neu, was echte Bereitschaft bedeutet.

Deshalb ist der „**Globale Risiko- und Resilienz-Ausblick 2026**“ so relevant. Er unterstützt Führungskräfte dabei zu erkennen, wie konvergierende Risiken die Geschäftskontinuität verändern, und zeigt praxisnahe Wege auf, ihnen einen Schritt voraus zu bleiben. Im Mittelpunkt steht die Zukunftsfähigkeit: der Aufbau von Systemen, Kultur und Vertrauen, um schneller reagieren und sich stärker erholen zu können.

Resilienz ist heute kein statischer Plan, sondern eine Denkweise, die Menschen, Daten und Maßnahmen im gesamten Unternehmen verbindet. Die erfolgreichsten Organisationen vollziehen diesen Wandel bereits, indem sie zweckorientierte KI, Automatisierung und entscheidungsrelevante Informationen nutzen, um vom Reagieren ins Antizipieren zu gelangen. Genau das ist die Grundlage des Dynamischen Krisen- und Notfallmanagement (High Velocity CEM™): Organisationen dabei zu unterstützen, Risiken früher zu erkennen, schneller zu reagieren und sich kontinuierlich zu verbessern.

Das Ziel ist nicht nur, Störungen zu überstehen, sondern aus ihnen gestärkt hervorzugehen. Nutzen Sie diesen Bericht, um Annahmen zu hinterfragen, neue Gespräche anzustoßen und den Weg Ihrer Organisation hin zu echter Resilienz im Jahr 2026 und darüber hinaus zu beschleunigen.

Dave Wagner
Präsident und Geschäftsführer, Everbridge

Zusammenfassung

Die globale Risikolandschaft des Jahres 2026 ist geprägt von zunehmender Komplexität und tief miteinander verflochtenen Bedrohungen, die sich über Branchen und Regionen erstrecken. Diese Realität erfordert eine strategische Weiterentwicklung von der traditionellen Geschäftskontinuität hin zu einer umfassenden organisationalen Resilienz. Organisationen sehen sich mit wachsenden Herausforderungen konfrontiert, die Anpassungsfähigkeit sowie schnelle und entschlossene Reaktionen auf ein sich ständig veränderndes Bedrohungsumfeld verlangen. Resilienz ist in diesem Zusammenhang längst nicht mehr eine reine Compliance-Anforderung, sondern ein integriertes, strategisches Gut, das für nachhaltigen Betrieb und Wettbewerbsvorteile unverzichtbar ist.

Die globalen Bedrohungen von heute treten häufig in systemischen Risikoclustern auf und wirken sich gleichzeitig auf soziale, operative und finanzielle Bereiche aus. Diese Vernetzung schafft neue Schwachstellen und zwingt Organisationen, traditionelle Risikomanagementansätze zu überdenken und echte Zukunftsfähigkeit aufzubauen. Gartner unterstreicht diese Dringlichkeit und prognostiziert, dass bis 2027 sechzig Prozent der Unternehmen, die keine Resilienzprinzipien verankern, weiterhin anfällig für globale technologische Bedrohungen bleiben werden.

Mit zunehmender Komplexität der Geschäftsabläufe steigen auch die Risiken. Wir bezeichnen dies als expandierende Risikozone, in der Häufigkeit und Intensität kritischer Ereignisse die Prioritäten in Vorstandsetagen neu ordnen und die Geschäftskontinuität herausfordern. Unternehmen müssen sich darauf vorbereiten, simultane und miteinander verknüpfte Risiken zu managen. Dies erfordert einen Paradigmenwechsel – weg von reaktiver Vorfallbewältigung hin zu einem proaktiven High-Velocity-Ansatz im Management kritischer Ereignisse.

Die Ergebnisse der Everbridge Global Risk Survey, die im Oktober 2025 durchgeführt wurde, machen erhebliche Schwachstellen in der organisationalen Resilienz deutlich. Besonders besorgniserregend ist, dass die Hälfte der Befragten über keine formale Strategie für das Management kritischer Ereignisse verfügt und fast ein Viertel ihre Kontinuitätspläne nie testet. Weitere Defizite bestehen in unzureichender Mitarbeiterschulung, mangelnden Technologieinvestitionen und einem bemerkenswert geringen Vertrauen in bestehende Krisenkommunikationskanäle. Da Cybersicherheit inzwischen als größte Bedrohung eingestuft wird, verdeutlichen diese Erkenntnisse die dringende Notwendigkeit, proaktive und technologiegestützte Strategien zu entwickeln, um der komplexen Risikolandschaft von heute wirksam begegnen zu können.

Dieser Bericht identifiziert zehn zentrale globale Risiken für das Jahr 2026 und bietet einen strategischen Rahmen, um die organisationale Resilienz zu stärken und die Geschäftskontinuität abzusichern. Er betont die entscheidende Rolle fortschrittlicher Risikomanagementmethoden und gezielter Investitionen im Aufbau zukunftsfähiger Organisationen.

Auswirkungen auf Geschäftskontinuität und Resilienz

Der folgende Abschnitt beschreibt 10 der wichtigsten Risiken, die für 2026 erwartet werden, und analysiert deren direkte Auswirkungen auf die Fähigkeit einer Organisation, operative Resilienz aufrechtzuerhalten und Geschäftskontinuität sicherzustellen.

01

Cyberangriffe und systemisches Cyberrisiko

Während Organisationen die digitale Transformation beschleunigen und ihre Abhängigkeit von vernetzten Technologien weiter wächst, hat die globale Cybersicherheitslandschaft einen kritischen Wendepunkt erreicht. Sie ist geprägt von zunehmender Raffinesse, Häufigkeit und Schwere der Bedrohungen, die gezielt auf das Rückgrat des Geschäftsbetriebs abzielen. In den vergangenen zehn Jahren ist das Cyberrisiko exponentiell gestiegen – angetrieben durch die Ausweitung von IT-Systemen, die Nutzung zahlreicher Drittanbieter und die zunehmende Verteilung der Belegschaft. Diese expandierende Risikozone erhöht nicht nur die Anfälligkeit zentraler Systeme, sondern gefährdet ebenso kritische Lieferketten und Betriebstechnologie.

Moderne Cyberangriffe sind vielschichtig. Organisationen sehen sich heute mit Ransomware konfrontiert, die sich über globale Netzwerke ausbreitet, mit KI-gestützter Malware, die sich in Echtzeit weiterentwickelt, sowie mit Deepfake-basiertem Social Engineering, das gezielt auf Führungskräfte abzielt. Angreifer nutzen Schwachstellen in vernetzten Lieferketten, gemeinsamen digitalen Plattformen und Cloud-Ökosystemen aus und schaffen damit konzentrierte Risiken, die ganze Branchen lahmlegen können. Staatlich geförderte Akteure und organisierte kriminelle Gruppen fokussieren zunehmend auf Sektoren, die als entscheidend für die wirtschaftliche und nationale Sicherheit gelten – insbesondere Energie, Transport, Gesundheitswesen und Finanzdienstleistungen – und setzen dabei fortschrittliche Zero-Day-Exploits, raffinierte Phishing-Kampagnen und persistente Bedrohungen ein.

Die finanziellen und betrieblichen Folgen gehen weit über klassischen Datenverlust hinaus. Ein einzelner schwerwiegender Cybervorfall kann digitale Dienste über Monate lahmlegen, kritische Lieferungen unterbrechen und weitreichende Kaskadeneffekte auslösen, die das Vertrauen der Kunden beeinträchtigen, Einnahmequellen reduzieren und regulatorische Risiken nach sich ziehen. Vor diesem Hintergrund müssen Organisationen ihre Sicherheitskontrollen modernisieren, Überwachung und Cyberhygiene verbessern und Cyber-Resilienz fest in Risikomanagement- und Kontinuitätsstrategien verankern. Erfolg hängt maßgeblich davon ab, eine Kultur der Vorbereitung zu etablieren, die operative Stabilität während eines Angriffs sicherstellt und die Wiederherstellung angesichts zunehmender Bedrohungskomplexität beschleunigt.

Eine Everbridge-Umfrage unter globalen Wirtschaftsführern aus dem Jahr 2025 zeigt, dass Cybersicherheit für 53 Prozent der Organisationen die größte Bedrohung darstellt.

Was passiert:

Cyberbedrohungen entwickeln sich schnell weiter – sowohl in ihrer Häufigkeit als auch in ihrer Komplexität. Angreifer nehmen verstärkt Lieferanten und gemeinsame digitale Plattformen ins Visier und schaffen dadurch konzentrierte Risiken über ganze Systemlandschaften hinweg, die traditionelle Sicherheitsgrenzen infrage stellen.

Geschäftliche Auswirkungen:

Ein erfolgreicher Angriff kann erhebliche Betriebsausfälle, Umsatzeinbußen und schwerwiegende rechtliche Konsequenzen nach sich ziehen und wirkt sich unmittelbar auf Wiederherstellungszeitziele aus. Wird die Betriebstechnologie kompromittiert, steigen die Sicherheitsrisiken erheblich, und die Wiederherstellung kann sich über Monate erstrecken. Die durchschnittlichen Kosten einer Datenpanne liegen bei 4,44 Millionen US-Dollar – eine Zahl, die weder Betriebsunterbrechungen noch langfristige Reputationsschäden vollständig abbildet.

Zu beobachtende Signale:

Organisationen sollten verstärkt auf eine Zunahme von Credential-Stuffing-Angriffen sowie Angriffen zielen, die Ermüdungseffekte bei der Multi-Faktor-Authentifizierung ausnutzen. Ebenso kritisch sind ungewöhnliche Aktivitäten in OT-Netzwerken, Sicherheitsvorfälle bei wesentlichen Lieferanten und Deepfakes, die darauf ausgelegt sind, Führungskräfte zu täuschen oder Freigabeprozesse zu manipulieren.

Strategische Maßnahmen für Zukunftsfähigkeit:

Um Geschäftskontinuität zuverlässig zu sichern, ist ein proaktiver Ansatz unerlässlich. Dazu gehören eine durchgehende 24/7-Überwachung, aktives Threat-Hunting und die Stärkung der Identitätssicherheit durch robuste Multi-Faktor-Authentifizierung und Least-Privilege-Zugriffsrechte. Betriebstechnologie sollte segmentiert und isoliert betrieben werden. Ergänzend sind regelmäßige Übungen zu Ransomware- und Deepfake-Szenarien notwendig, um Reaktionsfähigkeit und Entscheidungsfähigkeit unter Druck zu verbessern. Von kritischen Lieferanten sollten Sicherheitszertifizierungen eingefordert werden, während vorbereitete Krisenkommunikationsvorlagen helfen, im Ernstfall schnell und koordiniert zu reagieren.

Sichern Sie Ihre Cyber-Resilienz für die Zukunft

Laden Sie jetzt unser Whitepaper „Cyber Resilience 2026 and Beyond“ herunter, um künftigen Cyberbedrohungen einen Schritt voraus zu sein.

Hier zugreifen

02

Die zwei Perspektiven der KI

Künstliche Intelligenz zählt heute zu den transformativsten Kräften, die Risiko und Resilienz gleichermaßen prägen. Ihre Fortschritte eröffnen Unternehmen beispiellose Möglichkeiten für Innovation, Produktivität und vorausschauende Erkenntnisse und stellen leistungsfähige Werkzeuge zur Antizipation, Erkennung und Bewältigung kritischer Ereignisse bereit. KI-gestützte Plattformen können Entscheidungen beschleunigen, die Krisenkommunikation verbessern und durch Automatisierung die betriebliche Effizienz deutlich steigern.

Gleichzeitig verschärft dieselbe Technologie jedoch auch die Risikolandschaft erheblich. Böswillige Akteure nutzen KI, um Aufklärung zu automatisieren, hochentwickelte Angriffe schnell zu skalieren, täuschend überzeugende Phishing-Schemata zu erstellen oder Ransomware-as-a-Service zu betreiben. Zunehmend kommen KI-generierte Deepfakes zum Einsatz, um Mitarbeitende zu täuschen oder Kontrollen auf Führungsebene zu umgehen. Das Volumen und die Komplexität solcher maschinell gesteuerten Bedrohungen übersteigen bereits heute die Möglichkeiten vieler Organisationen, mit traditionellen Sicherheitsmaßnahmen angemessen zu reagieren.

Das grundlegende Paradoxon besteht darin, dass Unternehmen KI immer schneller einführen, um ihre operative Resilienz zu stärken, gleichzeitig jedoch Schwierigkeiten haben, mit den entstehenden Risiken Schritt zu halten. Dazu zählen mögliche Datenlecks, Modelldrift, schwer interpretierbare oder verzerrte KI-Ergebnisse sowie ein wachsender Druck durch regulatorische Anforderungen. Besonders kritisch ist die schnelle Einführung generativer KI, die oft stattfindet, bevor robuste Governance- und Kontrollrahmen etabliert wurden. Dadurch steigt das Risiko von Compliance-Verstößen und Reputationsschäden erheblich.

Organisationen müssen erkennen, dass die zwei Seiten der KI einen zukunftsfähigen Ansatz erfordern: Sie müssen KI proaktiv zur Stärkung von Geschäftskontinuität und Resilienz nutzen und gleichzeitig kontinuierlich in Aufsicht, Governance, Risikomanagement und Reaktionsmechanismen investieren, um den sich verändernden KI-Bedrohungsprofilen gerecht zu werden.

> „KI-getriebene Bedrohungen entwickeln sich weiter. Führungskräfte müssen sich auf Deepfakes und automatisierte Angriffe vorbereiten und gleichzeitig den Menschen bei kritischen Entscheidungen im Prozess einbinden.“
>
> Pamela Larson, Sicherheitschef, Nordamerika, Everbridge

Was passiert:

KI verstärkt Cyberbedrohungen und verbessert gleichzeitig die Verteidigungsfähigkeit. Angreifer nutzen KI zur automatisierten Aufklärung und für adaptive Malware, während Unternehmen KI häufig schneller einsetzen, als Governance- und Kontrollsysteme aufgebaut werden können.

Geschäftliche Auswirkungen:

Die Häufigkeit und Schwere von Vorfällen nehmen zu und gefährden die Geschäftskontinuität unmittelbar. Die unkontrollierte Nutzung generativer KI kann zu Datenverlusten, verzerrten Ergebnissen oder Compliance-Verstößen führen. Deloitte prognostiziert, dass durch generative KI verursachte Betrugsverluste in den USA bis 2027 auf 40 Milliarden US-Dollar ansteigen könnten.

Zu beobachtende Signale:

Organisationen sollten auf ungewöhnliche Automatisierungsmuster in Zugriffs- und Netzwerkprotokollen achten, Berichte über den Missbrauch generativer KI und Modelldrift beobachten sowie Änderungen durch Drittanbieter-Modelle sorgfältig prüfen. Zudem ist es entscheidend, neue regulatorische Vorgaben für KI in kritischen Funktionen im Blick zu behalten.

Strategische Maßnahmen für Zukunftsfähigkeit:

Unternehmen sollten einen klar definierten KI-Governance-Rahmen mit eindeutigem Risikoappetit implementieren, alle KI-Modelle und Anwendungsfälle inventarisieren und kategorisieren und vor ihrer produktiven Nutzung umfangreiche Red-Teaming-Tests sowie Modellvalidierungen durchführen. Der „Human-in-the-Loop“-Ansatz muss für alle kritischen Entscheidungsprozesse verpflichtend sein. Führungsteams sollten zudem Deepfake-Übungen absolvieren, insbesondere in Bereichen wie Zahlungsfreigaben oder Kommunikationsprozessen, um sich auf hochentwickelte Social-Engineering-Angriffe vorzubereiten.

> Entdecken Sie, wie zweckorientierte KI das Krisenmanagement durch schnellere Entscheidungen, verbesserte Resilienz und präzisere Risikoeinschätzungen stärkt.
>
> Laden Sie Ihr kostenloses Whitepaper herunter: „Die vier Säulen der KI im Krisenmanagement“

03

Naturkatastrophen und klimabedingte Extreme

Die zunehmende Häufigkeit und Intensität extremer Wetterereignisse – von Hurrikanen und Waldbränden über Hitzewellen, Dürren und Überschwemmungen bis hin zu Erdbeben – stellt Organisationen weltweit vor erhebliche Herausforderungen. Unternehmen sind dabei nicht nur von unmittelbaren Störungen betroffen, sondern auch von tiefgreifenden indirekten Auswirkungen, die sich entlang globaler Lieferketten und regionaler Wirtschaftsräume fortsetzen. Aktuelle Daten verdeutlichen die Dringlichkeit: Der Global Assessment Report des UNDRR zeigt, dass Versicherungsleistungen im Zusammenhang mit Naturkatastrophen inzwischen durchschnittlich 1,9 Prozent des jährlichen globalen BIP ausmachen. Ereignisse, die früher als Jahrhundertereignisse galten, treten heute wesentlich häufiger auf und belasten Infrastruktur und Notfallsysteme in einem bislang unbekannten Ausmaß.
Im vergangenen Jahr waren 69 Prozent aller vom Everbridge Risk Intelligence Monitoring Center erfassten Vorfälle klimabedingt – darunter extreme Hitze, Waldbrände, Überschwemmungen, Tornados und Hurrikane. Praxisbeispiele wie der geschätzte Schaden von 131 Milliarden US-Dollar durch einen einzigen Waldbrand in Los Angeles oder die außergewöhnlich intensiven Waldbrandsaisons in Europa verdeutlichen zusätzlich, wie stark klimabedingte Katastrophen in Häufigkeit und Ausmaß zunehmen.

> „Der Klimawandel ist keine ferne Bedrohung mehr – er ist eine gegenwärtige Realität und verändert das Risikoprofil jeder Organisation grundlegend. Wir fühlen uns geehrt, in einer so entscheidenden Phase zunehmender klimatischer Herausforderungen mit dem Büro der Vereinten Nationen für Katastrophenvorsorge zusammenzuarbeiten. Der Aufbau widerstandsfähiger Gemeinschaften und Organisationen ist Kern unserer Mission.“
>
> Dave Wagner, Präsident und Geschäftsführer,, Everbridge

Was passiert:

Extreme Wetterbedingungen sind längst kein seltenes oder isoliertes Phänomen mehr, sondern wirken zunehmend anhaltend und systemisch. Sie beeinträchtigen Transport-, Logistik- und Versorgungsnetze und entfalten sekundäre Auswirkungen wie verschlechterte Luftqualität, Wasserknappheit und Netzinstabilität. Diese Entwicklungen stellen die Fähigkeit von Unternehmen, Menschen, Anlagen und Lieferketten zu schützen, auf eine harte Probe. Da Wiederaufbauprozesse immer länger dauern und Versicherungsbedingungen restriktiver werden, nimmt das chronische Risiko betrieblicher Unterbrechungen weiter zu.

Geschäftliche Auswirkungen:

Unternehmen sehen sich vermehrt mit Standortschließungen, Produktionsstopps und der Verlagerung von Belegschaften aufgrund klimabedingter Gefahren konfrontiert. Versicherungsprämien steigen spürbar, während Deckungsumfänge strenger begrenzt werden. Die Wiederherstellung betroffener Standorte und Prozesse verzögert sich häufig durch sich verändernde Umweltbedingungen. Die finanziellen und betrieblichen Auswirkungen gehen weit über unmittelbare Schäden hinaus, belasten Margen, gefährden Planbarkeit und fordern bestehende Resilienzstrategien auf entscheidende Weise heraus.

Zu beobachtende Signale:

Um zukunftsfähig zu bleiben, müssen Organisationen saisonale Prognosen in allen operativen Regionen aufmerksam verfolgen, Waldbrandrauchindizes, Dürre- und Netzbelastungswarnungen beobachten und regelmäßig aktualisierte Hochwasser- und Gefahrenkarten prüfen. Auch die frühzeitige Erkennung lokaler Notstandserklärungen sowie Anpassungen der Versicherungsrichtlinien ist entscheidend, um rechtzeitig reagieren zu können.

Strategische Maßnahmen für Zukunftsfähigkeit:

Unternehmen sollten ihre Anlagen und Infrastrukturen verstärken und verteidigungsfähige Schutzräume rund um kritische Standorte schaffen. Notstrom- und Wasserversorgung müssen gesichert und die Logistik zur Aufrechterhaltung der Versorgung regelmäßig getestet werden. Zudem sind anlagenbezogene Evakuierungspläne sowie flexible „Work-from-anywhere“-Modelle erforderlich, um die Sicherheit der Mitarbeitenden und die Geschäftskontinuität zu gewährleisten. Eine geografisch diversifizierte Lieferantenbasis und die regelmäßige Überprüfung des Versicherungsschutzes tragen wesentlich zur finanziellen Resilienz bei.

> Das Architektur-, Ingenieur- und Bauunternehmen Burns & McDonnell nutzt Everbridge, um kritische Ereignisse effizient zu bewältigen, indem es Lageinformationen zu betroffenen Zonen erhält, nahtlose Kommunikation ermöglicht und die Sicherheit seiner Mitarbeitenden während wetterbedingter Notfälle sicherstellt.
>
> Hier ansehen

04

Geopolitischer Konflikt

Geopolitische Instabilität und die zunehmende Instrumentalisierung wirtschaftspolitischer Maßnahmen – etwa Zölle auf kritische Mineralien, Exportbeschränkungen, strategische Subventionen und ein intensiverer Einsatz von Sanktionen – gehören heute zu den zentralen Risiken, die Organisationen aktiv managen müssen. Diese Entwicklungen treten nicht isoliert auf. Vielmehr entstehen moderne geopolitische Risiken aus einem komplexen Zusammenspiel geoökonomischer Rivalitäten, globaler Handelsstörungen, soziopolitischer Spannungen und der strategischen Nutzung digitaler Infrastruktur. Gemeinsam verstärken diese Faktoren die Volatilität und gefährden wesentliche Elemente operativer Resilienz.

Die kaskadierenden Effekte geopolitischer Konflikte wirken sich unmittelbar auf Handels- und Warenströme aus. Sie können zentrale Schifffahrtsrouten blockieren, Lieferengpässe entscheidender Vorprodukte verursachen und zu abrupten Preisschwankungen auf Rohstoff- und Energiemärkten führen. Wenn politische Konflikte eskalieren oder sich Handelspolitiken kurzfristig verändern, können essenzielle Materialien plötzlich nicht mehr verfügbar sein oder nur mit erheblichen Verzögerungen geliefert werden. Zugleich erschweren Währungsschwankungen und volatile Versicherungsmärkte die Finanzplanung. Regionale Konflikte können zudem dazu führen, dass Warenströme umgeleitet, Unternehmen neuen regulatorischen Auflagen unterworfen oder Lieferungen wegen Sanktionen blockiert werden. In manchen Fällen führt geopolitischer Druck auch zu fragmentierten Regulierungen, die Markteintritte erschweren oder etablierte Lieferketten neu ausrichten.

Besonders deutlich werden diese Auswirkungen in der Resilienz von Lieferketten. Unternehmen, die sich auf Single-Region-Sourcing oder Just-in-Time-Modelle verlassen, sind bei geopolitischen Schocks besonders verwundbar. Wird ein Lieferant oder ein Transportkorridor plötzlich unterbrochen, fehlen oftmals sofort verfügbare Alternativen – und wenn es sie gibt, sind sie meist begrenzt oder mit deutlich höheren Kosten verbunden. Dies verdeutlicht die Notwendigkeit eines ganzheitlichen Ansatzes für Risikoaufklärung, der berücksichtigt, wie schnell lokale geopolitische Ereignisse globale operative Störungen auslösen können.

Organisationen, die geopolitische Risiken erfolgreich managen, setzen auf proaktive Überwachung, strategische Planung und den gezielten Aufbau von Resilienz. Durch frühzeitige Identifikation von Trends und Risiken können sie Störungen abmildern, Vermögenswerte schützen und die Geschäftskontinuität auch unter unsicheren globalen Bedingungen aufrechterhalten.

Erfahren Sie mehr darüber, wie Organisationen geopolitische Instabilität erfolgreich bewältigen.

Das On-Demand-Webinar „Navigating Global Risk and Geopolitical Instability“ bietet hierzu wertvolle Einblicke

Was passiert:

Eine Kombination aus Zöllen, Exportkontrollen und Sanktionen verändert den globalen Handel grundlegend. Gleichzeitig führen regionale Konflikte zu Störungen an wichtigen Schifffahrtsrouten und beeinträchtigen internationale Versicherungsmärkte. Diese Entwicklungen erzeugen Unvorhersehbarkeit und erschweren die Sicherstellung der Geschäftskontinuität.

Geschäftliche Auswirkungen:

Unternehmen sehen sich mit anhaltender Volatilität bei Transitzeiten und Frachtkosten konfrontiert, während der Marktzugang in manchen Regionen schrumpft oder zusätzlichen regulatorischen Hürden unterliegt. Die Stabilität von Lieferanten wird dadurch zunehmend fragil, und sich wandelnde Vorschriften erhöhen den administrativen Aufwand erheblich. Ein proaktives Lieferkettenmanagement wird damit zur entscheidenden Voraussetzung für Resilienz.

Zu beobachtende Signale:

Für ein belastbares operatives Lagebild sollten maritime Sicherheitswarnungen, Verkehrsdaten von Wasserstraßen und aktuelle Änderungen an internationalen Sanktionslisten sorgfältig beobachtet werden. Schwankungen bei Rohstoffpreisen, Frachtkosten und Kriegsrisikoversicherungen bieten ebenfalls wichtige Hinweise auf aufkommende Risiken.

Strategische Maßnahmen für Zukunftsfähigkeit:

Unternehmen sollten geopolitische Erkenntnisse aktiv in die strategische Planung und ihre Beschaffungsentscheidungen integrieren, um Lieferketten widerstandsfähiger zu gestalten. Vorab definierte Umleitungs- und Transportwechselprotokolle, eine diversifizierte Lieferantenlandschaft über mehrere Regionen hinweg sowie die Prüfung von Near-Shoring-Optionen helfen dabei, Konzentrationsrisiken wirksam zu reduzieren.

Aufbau organisatorischer Resilienz in Zeiten geopolitischer Instabilität

Ein tieferes Verständnis der geopolitischen Landschaft und ihrer sicherheitsrelevanten Auswirkungen ist entscheidend, um Risiken frühzeitig zu erkennen, sich schnell anzupassen und langfristig gestärkt hervorzugehen.

Das Whitepaper „Building Organizational Resilience in Times of Geopolitical Instability“ bietet einen umfassenden Überblick

05

Betriebsunterbrechungen durch Lieferkettenstörungen

Lieferkettenstörungen gehören heute zu den tiefgreifendsten und gleichzeitig allgegenwärtigsten Bedrohungen für die Stabilität und Resilienz von Organisationen. Es handelt sich dabei längst nicht mehr um isolierte Herausforderungen, sondern um systemische Schocks, die die Geschäftskontinuität ganzer Branchen und Regionen beeinträchtigen können. Moderne Lieferketten sind weltweit verzahnt, hochkomplex und in hohem Maß voneinander abhängig. Dadurch kann eine einzige Störung schnell weitreichende Auswirkungen entfalten, Produktion unterbrechen, Vertriebskanäle lahmlegen und kostspielige Verzögerungen in großem Umfang verursachen.

Die Ursachen solcher Störungen sind vielfältig. Hafenüberlastungen, Arbeitskräftemangel, Engpässe im Transportwesen und die Nichtverfügbarkeit kritischer Rohstoffe können selbst robuste Lieferketten destabilisieren. Zunehmend rücken zudem digitale Schwachstellen in den Mittelpunkt: Viele Unternehmen verlassen sich für zentrale Betriebsprozesse auf Drittanbieter-IT-Dienstleister, wodurch digitale Ausfälle oder Cybervorfälle zu einem systemischen Risikofaktor werden. Ein einziger Ausfall kann einen „digitalen Dominoeffekt“ auslösen, der sich rasch über mehrere Ebenen hinweg ausbreitet, betriebliches Chaos verursacht und die Geschäftskontinuität für zahlreiche Organisationen gleichzeitig gefährdet.

Die betriebswirtschaftlichen und operativen Folgen solcher Schocks sind erheblich. Die Produktion kann zum Erliegen kommen, Vorlaufzeiten verlängern sich, vertragliche Verpflichtungen können nicht eingehalten werden, und sowohl der Cashflow als auch das langfristige Vertrauen von Kunden und Partnern leiden. Besonders kritisch wirken sich diese Effekte in Branchen aus, die auf Just-in-Time-Bestände oder schlanke Betriebsmodelle setzen. In solchen Fällen verstärkt bereits ein einziges Ereignis die Verwundbarkeit und macht deutlich, wie abhängig viele Organisationen von Störungen sind, die weit außerhalb ihres direkten Einflussbereichs liegen.

> „Es ist entscheidend, ein klares Bild Ihrer gesamten Lieferkette zu haben – wo Rohstoffe herkommen, welche Standorte und Partner sie durchlaufen und wohin die fertigen Waren transportiert werden.“
>
> Tracy Reinhold, Globaler Sicherheitschef, Everbridge

Was passiert:

Physische Knotenpunkte wie Häfen und Logistikzentren, aber auch digitale Infrastrukturpartner verzeichnen immer häufiger Störungen. Eine ausgeprägte Abhängigkeit von wenigen Zulieferern oder Dienstleistern führt schnell zu einzelnen Fehlerquellen, die Organisationen anfällig für weitreichende operative Unterbrechungen und längere Ausfallzeiten machen.

Geschäftliche Auswirkungen:

Unterbrechungen können Produktionslinien zum Stillstand bringen, die Einhaltung von Service-Level-Agreements gefährden, erhebliche Umsatzverluste verursachen und die Fähigkeit einer Organisation auf die Probe stellen, sich zügig und koordiniert zu erholen. Die zunehmende Zahl digitaler Schwachstellen verstärkt diese Risiken, da Ausfälle bei IT-Drittanbietern unmittelbare Auswirkungen auf große Teile der Lieferkette haben können.

Zu beobachtende Signale:

Unternehmen sollten steigende Vorlaufzeiten, Zuteilungsmitteilungen für kritische Komponenten, Änderungen globaler Logistikrouten aufgrund geopolitischer Entwicklungen sowie Berichte über Ausfälle digitaler Serviceanbieter aufmerksam verfolgen. Auch die finanzielle und operative Stabilität zentraler Lieferanten muss kontinuierlich bewertet werden, um Frühwarnsignale nicht zu übersehen.

Strategische Maßnahmen für Zukunftsfähigkeit:

Organisationen sollten Dual- oder Multi-Sourcing-Strategien für kritische Materialien einführen, um Redundanz zu schaffen, und Pufferbestände für essenzielle Produkte aufbauen. Zusätzlich empfiehlt sich die frühzeitige Verhandlung alternativer Transportwege und -modalitäten, um im Störungsfall flexibel reagieren zu können. Diese Maßnahmen tragen dazu bei, Ausfallzeiten zu minimieren und die Geschäftskontinuität selbst bei weitreichenden Lieferkettenunterbrechungen sicherzustellen.

06

Fehlinformation und Desinformation

Die Verbreitung von Fehlinformationen und Desinformation zählt zu den am schnellsten wachsenden und bedeutendsten Risiken für die organisationale Resilienz im Jahr 2026. Falsche Narrative, Deepfake-Inhalte und die bewusste Manipulation von Informationsökosystemen werden zunehmend eingesetzt, um sowohl private als auch öffentliche Organisationen zu attackieren. Diese Bedrohungen reichen weit über Reputationseinbußen hinaus. Irreführende oder böswillig erzeugte Inhalte können die Krisenkommunikation massiv beeinträchtigen, ein wirksames Krisenmanagement destabilisieren und konkrete operative Zwischenfälle auslösen. Verzerrte Informationslagen schwächen die interne Abstimmung, untergraben das Vertrauen in Führungsentscheidungen und stiften Verwirrung bei Mitarbeitenden, Partnern, Kunden und der Öffentlichkeit.

Angetrieben durch den rasanten Fortschritt von KI-gestützten Werkzeugen – insbesondere generativer KI – wird die Erstellung hochgradig überzeugender Fehlinformationen immer einfacher, schneller und kostengünstiger. Das Volumen und die Wirkung erfundener oder manipulierten Inhalte steigen weiter an. Zielgerichtete Kampagnen können Kundenabwanderung auslösen, Lieferketten stören oder regulatorische Untersuchungen anstoßen. Besonders problematisch ist der Vertrauensverlust während kritischer Ereignisse: Er verlangsamt Reaktionen, fördert interne Konflikte und gefährdet langfristige Beziehungen zu Kunden und Partnern.

Der Global Risks Report des Weltwirtschaftsforums hat „Fehlinformation und Desinformation“ kürzlich als das schwerwiegendste globale Risiko der kommenden zwei Jahre eingestuft. Dies verdeutlicht die enorme Sprengkraft solcher Inhalte und ihre Fähigkeit, Entscheidungen zu untergraben und Märkte weltweit zu destabilisieren. Operative Folgen lassen sich bereits beobachten: So erreichte ein Deepfake-Livestream, der den CEO von Nvidia imitierte, mehr als 100.000 Zuschauerinnen und Zuschauer, bevor er gestoppt wurde – ein Beispiel für die Geschwindigkeit, mit der solche Angriffe eskalieren, und für ihr Potenzial, erheblichen Marken- und finanziellen Schaden zu verursachen.

> „Transparenz schafft Resilienz. Vertrauenswürdige Organisationen verdienen eine stärkere Kundenbindung, ein höheres Mitarbeiterengagement und ein robusteres Anlegervertrauen – selbst in volatilen Märkten.“
>
> Jeremy Capell, Vertrauenschef, Everbridge

Was passiert:

Falsche Narrative und Deepfakes untergraben zunehmend das Vertrauen in Marken und Führungspersonen. Angriffe zielen verstärkt darauf ab, Krisenreaktionen zu stören und Märkte zu manipulieren, weshalb verifizierte und eindeutig identifizierbare Kommunikation zu einem zentralen Bestandteil organisationaler Resilienz wird.

Geschäftliche Auswirkungen:

Verunsicherte Stakeholder – insbesondere Investoren und Kunden – reagieren zunehmend sensibel auf Fehlinformationen. Das führt zu verzögerter Entscheidungsfindung, steigenden Betrugsverlusten, Reputationsschäden und einer spürbaren Destabilisierung operativer Abläufe. Für viele Organisationen entwickelt sich dies zu einer kritischen Bedrohung ihrer Markenintegrität und ihrer betrieblichen Stabilität.

Zu beobachtende Signale:

Frühindikatoren sind vermehrte Imitationen von Führungskräften, Versuche von Zahlungsumleitungen, unerwartete Spitzen in der eingehenden Kommunikation sowie plötzlich viral gehende markenbezogene Gerüchte. Auch koordinierte Narrative-Kampagnen können Hinweise auf gezielte Angriffe liefern.

Strategische Maßnahmen für Zukunftsfähigkeit:

Organisationen müssen sämtliche Führungskommunikation über etablierte, abgesicherte Kanäle authentifizieren, um Manipulationen vorzubeugen. Eine schnell reagierende Kommunikationseinheit hilft, Informationsflüsse während einer Krise zu steuern. Mitarbeitende sollten darin geschult werden, Deepfakes und Bot-Aktivitäten zu erkennen. Darüber hinaus müssen Medien- und Social-Media-Monitoring fester Bestandteil der Vorfallreaktionspläne sein, um Angriffe früh zu identifizieren und rasch koordinierte Gegenmaßnahmen einzuleiten.

> Entdecken Sie die strategische Kraft von Offenheit und Verantwortlichkeit, um stärkere Teams aufzubauen, Kundenbindung zu fördern und langfristigen Erfolg zu sichern.
>
> Mehr dazu im Everbridge-Blog

07

Regulatorische Fragmentierung, Zölle und Handelsbeschränkungen

Das zunehmende Tempo regulatorischer Veränderungen prägt die globale Risikolandschaft heute in einem Ausmaß, das weitreichende operative Auswirkungen hat. Organisationen sehen sich mit einem dynamischen, immer stärker fragmentierten Geflecht aus Vorschriften, Zöllen und Handelsbeschränkungen konfrontiert, das betriebliche Unsicherheit schafft und das Compliance-Risiko zu einem zentralen Thema auf Vorstandsebene macht. Während Compliance in früheren Jahren vergleichsweise stabil und vorhersehbar war, ist das heutige regulatorische Umfeld durch divergierende Anforderungen unterschiedlicher Rechtsräume gekennzeichnet – insbesondere in Bereichen wie Sorgfaltspflichten in der Lieferkette, operative Resilienz, Cybersicherheit, Datenschutz und Umweltstandards.

Sanktionsregime, Exportkontrollen und Lokalisierungsauflagen werden immer kurzfristiger und häufiger angepasst. Dadurch entsteht ein permanenter Anpassungsdruck, der das Risiko unbeabsichtigter Regelverstöße erhöht. Für global agierende Unternehmen kann die wachsende regulatorische Volatilität grenzüberschreitende Geschäftsabläufe beeinträchtigen, zu erheblichen Lieferverzögerungen führen und den für digitale Services wesentlichen internationalen Datenfluss einschränken. Parallel steigen die Kosten für Compliance sowie die dafür erforderlichen Ressourcen – insbesondere in den Bereichen Beschaffung, Recht und Risikomanagement. Zudem nimmt die Wahrscheinlichkeit behördlicher Prüfungen und Durchsetzungsmaßnahmen zu, was das Risiko von Reputationsschäden erhöht, wenn Organisationen nicht über ausreichende Kontrollmechanismen verfügen.

Operativ gesehen ist diese Entwicklung hochrelevant: Fehlende Agilität im Umgang mit regulatorischen Änderungen kann den Marktzugang einschränken, Lieferketten unterbrechen oder die Fähigkeit gefährden, vertragliche Verpflichtungen rechtzeitig und vollständig zu erfüllen. Dadurch wird die organisationale Resilienz geschwächt. Erfolgreich sind jene Organisationen, denen es gelingt, Compliance, Handel, Beschaffung und Risiko zu einer einheitlichen operativen Sicht zusammenzuführen. Nur so können regulatorische Veränderungen frühzeitig antizipiert und abgefedert werden, bevor sie zu ernsthaften Störungen der Geschäftskontinuität führen.

> „Um die Komplexität des Compliance-Risikoumfelds zu bewältigen, konzentrieren Sie sich auf die Koordination über Risikomanagementfunktionen hinweg. Machen Sie den Aufbau wichtiger Fähigkeiten zu einer Priorität – so ermöglichen Sie schnellere, fundiertere Entscheidungen und ein wirksameres Risikomanagement.“
>
> Gartner

Was passiert:

Die regulatorischen Rahmenbedingungen driften weltweit auseinander, insbesondere im Hinblick auf Sorgfaltspflichten, operative Resilienz und Cybersicherheit. Sanktionen und Exportkontrollen werden häufig aktualisiert und machen Compliance zu einem beweglichen Ziel, das ständig neu bewertet werden muss.

Geschäftliche Auswirkungen

Die Folge sind steigende Compliance-Kosten, höhere Komplexität entlang der Lieferketten und eingeschränkte Datenflüsse. Zudem steigt das Risiko behördlicher Prüfungen und Durchsetzungsmaßnahmen erheblich, was den operativen Betrieb zusätzlich erschweren kann.

Zu beobachtende Signale:

Unternehmen sollten neue Vorschriften in wichtigen Ziel- und Produktionsmärkten aufmerksam verfolgen, behördliche Leitlinien regelmäßig prüfen und Warnmeldungen relevanter Branchenverbände berücksichtigen, um frühzeitig auf mögliche Veränderungen reagieren zu können.

Strategische Maßnahmen für Zukunftsfähigkeit:

Eine einheitliche operative Sicht, die Compliance-, Handels-, Beschaffungs- und Risikomanagementfunktionen verknüpft, ist essenziell. Ein proaktiver Kalender mit erwarteten regulatorischen Änderungen schafft Vorhersehbarkeit. Szenarioplanungen helfen dabei, mögliche Engpässe bei Materialien und Datenflüssen zu erkennen. Die Standardisierung von Lieferantendokumentationen unterstützt Organisationen darin, sich entwickelnde Sorgfaltspflichtanforderungen zuverlässig zu erfüllen und die Geschäftskontinuität abzusichern.

> „Regulatorische Anforderungen werden komplexer und zunehmend vernetzter. Bei Resilienz geht es nicht darum, ein Kästchen abzuhaken, sondern darum, die Fähigkeit zu entwickeln, sich anzupassen, wenn sich die Regeln ändern.“
>
> **Dave Wagner, Präsident und Geschäftsführer, Everbridge**

Lesen Sie den vollständigen Blogbeitrag hier

08

Makroökonomische und finanzielle Instabilität

Makroökonomische und finanzielle Instabilität ist heute ein zentrales Anliegen für Organisationen, die ihre Geschäftskontinuität und operative Resilienz sicherstellen wollen. Das globale Geschäftsumfeld wird zunehmend volatiler und ist geprägt von anhaltender Inflation, schwankenden Zins- und Wechselkursen sowie schnellen Veränderungen in der Steuer- und Handelspolitik. Diese Faktoren sind längst keine Hintergrundvariablen mehr, sondern entwickeln sich zu maßgeblichen Risiken, die unmittelbare Auswirkungen auf Betriebskapital, Finanzierungskosten, Beschaffungszyklen und Einnahmequellen haben.

Organisationen geraten zunehmend unter Druck, da die Inflation die reale Nachfrage schwächt und Margen reduziert, während Zinsänderungen Finanzierungskosten nach oben treiben und Planungsunsicherheit verursachen. Politische Eingriffe – beispielsweise neue Zölle oder Subventionsprogramme – können Handelsströme abrupt verändern und die Vorhersehbarkeit grenzüberschreitender Prozesse stark beeinträchtigen. Hinzu kommen verschärfte Liquiditätsbedingungen, eine höhere Anfälligkeit für Lieferantenausfälle, schwankende Nachfrage sowie verkürzte Projektzeitpläne entlang der gesamten Wertschöpfungskette.

Selbst wirtschaftlich solide Unternehmen sehen sich in diesem Umfeld mit plötzlichem Cashflow-Druck, steigenden Kosten und gleichzeitigen Schocks auf Angebots- und Nachfrageseite konfrontiert. In den vergangenen Jahren mussten zahlreiche Unternehmen ihre Gewinnprognosen und strategischen Projektpläne aufgrund ungünstiger Währungseffekte oder Handelsbeschränkungen überarbeiten – ein deutliches Zeichen für die weitreichenden Auswirkungen makroökonomischer Volatilität auf langfristige Geschäftsstrategien und Resilienz.

> „Ausfallzeiten sind teurer denn je. Ein Gartner-Bericht ergab, dass die durchschnittlichen Kosten für IT-Ausfallzeiten 5.600 US-Dollar pro Minute betragen. In Branchen wie E-Commerce, Finanzdienstleistungen oder SaaS liegen diese Werte sogar noch deutlich höher.“
>
> David Alexander, Marketingchef und Geschäftsführer für digitale Operationen, Everbridge

Was passiert:

Inflation und volatile Wechselkurse lösen Welleneffekte über gesamte Lieferantennetzwerke hinweg aus und beeinträchtigen sowohl Warenkosten als auch Projektplanungen. Parallel steigt das Risiko geopolitisch bedingter Handelsstörungen.

Geschäftliche Auswirkungen:

Unternehmen müssen mit enger werdender Liquidität, drohenden Lieferantenausfällen und Verzögerungen in Projekten rechnen. Das Risiko zeitgleicher Angebots- und Nachfrageschocks nimmt zu und stellt die finanzielle Resilienz entlang der gesamten Wertschöpfungskette auf eine harte Probe.

Zu beobachtende Signale:

Frühindikatoren sind Trends im Einkaufsmanagerindex (PMI), Veränderungen bei Kreditspreads und Hinweise auf finanzielle Instabilität zentraler Lieferanten. Auch neue Zollankündigungen, Fremdwährungsklauseln in Verträgen und Anfragen von Partnern zur Verlängerung von Zahlungszielen sollten aufmerksam verfolgt werden.

Strategische Maßnahmen für Zukunftsfähigkeit:

Unternehmen sollten Cashflow-Stresstests durchführen und Maßnahmen für kurzfristige Kostensenkungen vorbereiten. Eine diversifizierte Finanzierung, ausreichende Liquiditätspuffer und flexible Preisgestaltungsmodelle stärken die operative Stabilität. Währungsrisiken sollten aktiv abgesichert werden. Zusätzlich helfen Frühwarn-Dashboards und klare Reaktionsprozesse dabei, Störungen zu mindern und die Geschäftskontinuität zuverlässig aufrechtzuerhalten.

Weitere Einblicke dazu, wie Organisationen ihre Resilienz stärken und

Geschäftskontinuität sicherstellen können, finden Sie im kostenlosen eBook „8 Schritte zu einem effektiven Geschäftskontinuitätsplan“

Hier zugreifen

09

Fachkräftemangel und Qualifikationsdefizite

Technologische Umwälzungen, demografische Veränderungen und wirtschaftliche Übergänge führen weltweit zu einem kritischen Fachkräftemangel. Dabei geht es längst nicht mehr nur um fehlendes Personal, sondern vor allem um das Fehlen spezifischer Schlüsselkompetenzen, die für die Durchführung zentraler Geschäftsprozesse erforderlich sind. Bleiben entscheidende Rollen unbesetzt oder verfügen Mitarbeitende nicht über die notwendigen Fähigkeiten, entstehen Single Points of Failure, Reaktionszeiten im Incident-Management verlängern sich und wertvolles institutionelles Wissen geht verloren. Die Folgen sind längere Wiederherstellungszeiten, verfehlte Wiederanlaufziele und stagnierende Modernisierungsprogramme – alles Faktoren, die die Geschäftskontinuität und die organisationale Resilienz nachhaltig untergraben.

Bis 2030 wird Schätzungen zufolge jeder sechste Mensch weltweit über 60 Jahre alt sein, was die Alterung der Belegschaft weiter beschleunigt. Gleichzeitig wachsen die Qualifikationsdefizite in vielen Organisationen. Das Weltwirtschaftsforum stellt fest, dass Führungskräfte einerseits von einer Überkapazität an Arbeitskräften sprechen, gleichzeitig aber einen akuten Mangel in kritischen Bereichen wie künstlicher Intelligenz wahrnehmen. Eine weitere Studie zeigt, dass 44 Prozent der Führungskräfte den Mangel an internem Fachwissen als zentrales Hindernis bei der Einführung von KI identifizieren. Diese Kompetenzen sind längst nicht mehr ein HR-Thema, sondern eine strategische Voraussetzung für Kontinuität und damit für Resilienz.

Um Geschäftskontinuität sicherzustellen, müssen Unternehmen Kompetenzen systematisch kritischen Prozessen zuordnen, Wissen in standardisierten Handbüchern dokumentieren, Automatisierung gezielt einsetzen und Teams funktionsübergreifend schulen, um Lastspitzen abzufedern. Ein integrierter Ansatz aus Neueinstellungen, Umschulungen und der Nutzung von Managed Services kann kurzfristige Lücken schließen und gleichzeitig langfristige Resilienz stärken. Es ist essenziell, Talentverfügbarkeit als zentralen operativen Risikoindikator zu begreifen und aktiv zu managen.

> „Bei Everbridge sprechen wir häufig darüber, dass Resilienz eine geteilte Verantwortung ist. Sie ist nicht die Aufgabe einer einzelnen Abteilung. HR spielt dabei eine große Rolle, denn wie Sie Ihr Team in schwierigen Momenten unterstützen, sagt viel darüber aus, wer Sie als Unternehmen sind.“
>
> Cara Antonacci, Personalchef, Everbridge

Was passiert:

Die Kombination aus alternden Belegschaften und rasantem technologischem Wandel führt zu erheblichen Kompetenzlücken in resilienzrelevanten Rollen wie Betriebstechnologie-Sicherheit, Zuverlässigkeitstechnik oder Datenmanagement. Fluktuation und lückenhafte Übergaben – insbesondere in Remote-Arbeitsumgebungen – verschärfen den Verlust institutionellen Wissens zusätzlich.

Geschäftliche Auswirkungen:

Längere Wiederherstellungszeiten, das Verfehlen definierter Wiederanlaufziele und Verzögerungen bei Modernisierungsinitiativen sind direkte Konsequenzen. Zusätzlich steigt der Arbeitsdruck in kritischen Teams, was das Risiko von Burnout erhöht und die Stabilität weiter beeinträchtigt.

Zu beobachtende Signale:

Frühwarnzeichen für Kompetenz- oder Kapazitätsrisiken sind lang andauernde Vakanzen in kritischen Rollen, steigende Überstunden und permanente Rufbereitschaften. Ebenso weisen Schulungsrückstände, fehlende Zertifizierungen oder Mitarbeitende, die als einzige Wissensträger bestimmter Systeme fungieren, auf strukturelle Risiken hin.

Strategische Maßnahmen für Zukunftsfähigkeit:

Unternehmen sollten Kompetenzen gezielt mit kritischen Anlagen und Prozessen abgleichen, standardisierte Runbooks etablieren und Teams funktionsübergreifend schulen. Eine Kombination aus Neueinstellungen, Weiterqualifizierung und Managed Services schafft zusätzliche Kapazitäten und Resilienz. Darüber hinaus sind regelmäßige Bewertungen der Personalstärke und Nachfolgepläne notwendig. Rückblickende Analysen (After-Action-Reviews) helfen dabei, Runbooks zu aktualisieren und Schulungsprogramme kontinuierlich zu verbessern.

29 Prozent der befragten Organisationen nennen unzureichende Mitarbeiterschulung und Sensibilisierung als größte Schwäche ihrer Strategien für das Management kritischer Ereignisse

(Everbridge Global Risk Survey, 2025)

10

Polykrisen: Überlappende Risiken, exponentielle Auswirkungen

Polykrisen entstehen, wenn mehrere Risiken gleichzeitig eintreten und sich in ihrer Wirkung gegenseitig verstärken. Dadurch entstehen komplexe, voneinander abhängige Störungen, die weit über den Umfang eines einzelnen Vorfalls hinausgehen. Anders als isolierte Ereignisse basieren Polykrisen auf der Konvergenz globaler Bedrohungen, die sich gegenseitig potenzieren. Dieses Phänomen tritt zunehmend häufiger auf, da unsere Welt immer stärker vernetzt ist. Die Wahrscheinlichkeit gleichzeitiger, sektorübergreifender Störungen nimmt zu – getrieben von globalen Lieferketten, gemeinsamen digitalen Plattformen und kritischen Infrastrukturen, die über geographische und organisatorische Grenzen hinweg verbunden sind.

Die Auswirkungen von Polykrisen sind nichtlinear und häufig exponentiell. So kann ein bewaffneter Konflikt Lieferketten unterbrechen und Inflation auslösen, während gleichzeitig extreme Wetterereignisse wichtige Produktionsstandorte treffen und Cyberbedrohungen verteilte Belegschaften attackieren. Diese Konvergenz belastet die organisatorische Belastbarkeit erheblich, überfordert etablierte Krisenmanagementprotokolle und führt zu einer „Entscheidungsmüdigkeit“ in den Führungsteams. In solchen Situationen sind isolierte oder sequenzielle Reaktionstaktiken schnell überholt, da Organisationen mehrere, sich rasch entwickelnde Herausforderungen gleichzeitig bewältigen müssen.

Die vergangenen Jahre haben gezeigt, dass kaskadierende Risiken ganze Branchen lahmlegen, Wiederherstellungszeiten drastisch verlängern und das Vertrauen von Stakeholdern selbst bei gut vorbereiteten Organisationen nachhaltig beeinträchtigen können. Führungskräfte sehen sich mit langwierigen Vorfällen, erheblichen Ausfallzeiten und steigenden finanziellen Verlusten über mehrere Geschäftsbereiche hinweg konfrontiert – eine direkte Bedrohung sowohl für die organisationale Resilienz als auch für die langfristige Stabilität.

Der Global Risks Report des Weltwirtschaftsforums hebt hervor, dass 85 Prozent der befragten Experten gleichzeitige Risikoereignisse als eine der bestimmenden Herausforderungen des kommenden Jahrzehnts ansehen.

Was passiert:

Miteinander verbundene globale Risiken kollidieren zunehmend. Konflikte können beispielsweise zu Lieferengpässen führen, die anschließend inflationäre Effekte verstärken. Zugleich erhöhen gemeinsame digitale Ökosysteme die Wahrscheinlichkeit, dass sich mehrere Vorfälle parallel über Ländergrenzen hinweg ausbreiten.

Geschäftliche Auswirkungen:

Wenn mehrere Vorfälle gleichzeitig eintreten, stößt traditionelle manuelle Koordination schnell an ihre Grenzen. Die Wiederherstellung verlangsamt sich, Ressourcen geraten in Konkurrenzsituationen, und Entscheidungsmüdigkeit beeinträchtigt die Führungsfähigkeit. Diese Entwicklungen können das Vertrauen von Stakeholdern untergraben und die organisationale Resilienz erheblich schwächen.

Zu beobachtende Signale:

Organisationen sollten multiregionale Warnungen zu Wetter, Cyberbedrohungen und Logistik aufmerksam verfolgen, parallele Vorfälle in kritischer Infrastruktur sowie Lieferketten überwachen und eskalierende Reise- und Sicherheitswarnungen im Blick behalten, die Auswirkungen auf verteilte Belegschaften haben können.

Strategische Maßnahmen für Zukunftsfähigkeit:

Eine einzige, gemeinsame Sicht auf alle Vorfälle – ein sogenanntes Common Operating Picture – ist entscheidend, um koordinierte Entscheidungen zu ermöglichen. Unternehmen sollten funktionsübergreifende Kommandozentren mit klarer Entscheidungsbefugnis etablieren und Notfallteams im Voraus definieren. Regelmäßige, realitätsnahe Übungen, die gleichzeitige, grenzüberschreitende Szenarien simulieren, helfen dabei, die organisationale Resilienz zu testen und zu stärken.

Ergebnisse aus der Everbridge-Umfrage

Aufdeckung kritischer Lücken in der organisationalen Resilienz

Der Aufbau echter Zukunftsfähigkeit beginnt mit einem klaren Verständnis des aktuellen Reifegrads einer Organisation. Um die globale Vorbereitung auf kritische Ereignisse zu bewerten, führte Everbridge eine umfassende Online-Umfrage unter Führungskräften weltweit durch. Die Everbridge Global Risk Survey, die Ende 2025 abgeschlossen wurde, bietet zentrale Erkenntnisse zu Geschäftskontinuität und operativer Resilienz.

Die Ergebnisse zeigen deutliche strategische Lücken.

Die Hälfte der Befragten (50 Prozent) gab an, nur begrenzte oder gar keine formellen Strategien für das Management kritischer Ereignisse zu besitzen und erst zu reagieren, wenn eine Störung bereits eingetreten ist. **Darüber hinaus testen 24 Prozent der Organisationen ihre Business-Continuity- oder Krisenmanagementpläne nie, was bei unerwarteten Störungen ein erhebliches Risiko darstellt.** Lediglich 31 Prozent der globalen Führungskräfte äußerten großes Vertrauen in die Fähigkeit ihrer Organisation, kritische Ereignisse effektiv zu bewältigen. Dieses Defizit zeigt deutlich, dass viele Unternehmen unzureichend vorbereitet sind, um die zunehmende Komplexität der expandierenden Risikozone zu beherrschen.

Auch in den Bereichen Schulung und Technologie bestehen große Lücken.

Unzureichende Mitarbeiterschulung und mangelnde Sensibilisierung wurden von 29 Prozent der Befragten als größte Schwäche genannt. 26 Prozent gaben an, zu wenig in moderne Tools und Technologien zu investieren. Besonders bemerkenswert ist, dass 61 Prozent der Unternehmen weder KI noch prädiktive Analytik einsetzen – ein klarer Hinweis auf Defizite bei der Nutzung moderner Resilienztechnologien.

Hinzu kommen Herausforderungen bei Kommunikation und Verantwortlichkeit.

Nur 37 Prozent der Befragten vertrauten uneingeschränkt den Kommunikationskanälen ihrer Organisation während einer Krise. Fehlende klare Kommunikationsprotokolle (16 Prozent) sowie unzureichende Budgetzuweisungen (64 Prozent der Unternehmen investieren weniger als fünf Prozent ihres Jahresbudgets oder sind hinsichtlich des Budgets unsicher) verstärken diese Schwachstellen.

Wichtigste Bedrohungen

Als wichtigste Bedrohungen für 2026 nannten die Befragten Cyberangriffe (53 Prozent), gefolgt von wirtschaftlichen Abschwüngen, Naturkatastrophen, Fachkräftemangel und geopolitischen Konflikten.

Die Ergebnisse unterstreichen die Notwendigkeit, rein compliance-getriebene Ansätze hinter sich zu lassen und hochdynamische Strategien für Geschäftskontinuität und Resilienz zu implementieren. Nur Organisationen, die gezielt in Schulung, Technologie und systematische Planung investieren, können ihre Zukunftsfähigkeit stärken und besser auf komplexe, sich schnell wandelnde Risiken reagieren.

Fünfstufige Resilienzstrategie

Wie man eine resiliente, zukunftsfähige Organisation aufbaut

Um echte Zukunftsfähigkeit zu erreichen, benötigen Resilienzverantwortliche einen integrierten und proaktiven Ansatz, der ihnen ermöglicht, Risiken früher zu erkennen, schneller zu reagieren und sich kontinuierlich weiterzuentwickeln. Ziel ist es, Menschen und Vermögenswerte zu schützen und gleichzeitig den reibungslosen Betrieb der Organisation sicherzustellen. Dies erfordert einen strategischen Wandel – weg von isolierten Business-Continuity- und Disaster-Recovery-Maßnahmen hin zu einer holistischen Resilienzstrategie, die durch ein hochdynamisches Management kritischer Ereignisse getragen wird.

01 Die erste Phase konzentriert sich auf die Planung.

Organisationen müssen über statische Risikoberichte hinausgehen und Szenarioplanung sowie anlagenbezogene Informationen nutzen, um potenzielle Auswirkungen präzise einzuschätzen. Eine solche proaktive Haltung erlaubt es, Risiken frühzeitig zu identifizieren, Ressourcen zielgerichtet zu priorisieren und die Grundlage für belastbare Geschäftskontinuität zu schaffen.

02 In der zweiten Phase geht es um die kontinuierliche Überwachung.

Unternehmen müssen jederzeit wissen, welche Mitarbeitenden, Standorte, Technologien oder Lieferketten potenziell gefährdet sind. KI-gestützte Risikoaufklärung und kontextbezogene Daten helfen dabei, Bedrohungen früh zu erkennen – von extremen Wetterereignissen bis hin zu geopolitischen Entwicklungen – und ermöglichen fundierte, schnelle Entscheidungen.

03 Die dritte Phase ist die Alarmierung.

Wenn jede Minute zählt, sind klare, gezielte und multimodale Benachrichtigungen unerlässlich. Ein hochdynamischer CEM-Ansatz beschleunigt Erkennung, Bewertung und Kontaktaufnahme, sodass Organisationen Reaktionszeiten drastisch verkürzen und ihre Sorgfaltspflichten gegenüber Mitarbeitenden zuverlässig erfüllen können – unabhängig davon, ob diese an einem Standort arbeiten oder auf Reisen sind.

04 In der vierten Phase steht die koordinierte Reaktion im Mittelpunkt.

Fragmentierte Systeme und isolierte Prozesse verlangsamen Entscheidungen. Ein gemeinsames Lagebild, das sicherheitsrelevante, operative und technologische Informationen integriert, sorgt dafür, dass die richtigen Personen zur richtigen Zeit die richtigen Maßnahmen ergreifen können. Über eine Plattform wie Everbridge High Velocity CEM™ lassen sich Entscheidungsprozesse und Ressourceneinsätze zentralisieren – mit erheblichen Vorteilen für Effizienz und Wirksamkeit.

05 Die fünfte Phase betrifft die kontinuierliche Verbesserung.

Organisationen müssen aus jedem Vorfall lernen, Nachanalysen durchführen und gewonnene Erkenntnisse in Prozesse und Systeme integrieren. Nur durch eine konsequente Weiterentwicklung von Business-Continuity-Plänen, Runbooks und Schulungsprogrammen entsteht langfristige Resilienz.

Durch die konsequente Umsetzung dieser fünfstufigen Strategie vollziehen Unternehmen den Wandel von einem reaktiven Risikomanagement hin zu echter Zukunftsfähigkeit. Sie schaffen die Voraussetzungen, um Mitarbeitende und Vermögenswerte zu schützen und den Geschäftsbetrieb auch unter den Bedingungen eines komplexen und dynamischen Risikoumfelds im Jahr 2026 und darüber hinaus zuverlässig aufrechtzuerhalten.

Fazit

Zukunftssichere organisatorische Resilienz ist entscheidend

Die sich wandelnde globale Risikolandschaft erfordert von Organisationen ein grundlegendes Umdenken in Bezug auf Geschäftskontinuität und operative Resilienz. Wie in diesem Bericht dargestellt, sind die Bedrohungen, denen Unternehmen im Jahr 2026 ausgesetzt sind, komplexer, stärker vernetzt und weniger vorhersehbar als je zuvor. Von Cyberangriffen und KI-gesteuerten Störungen bis hin zu extremen Wetterereignissen, regulatorischer Volatilität und Herausforderungen innerhalb der Belegschaft – jedes dieser Risikofelder bringt eigene sowie kombinierte Auswirkungen für Organisationen mit sich, die ihre Mitarbeitenden, Vermögenswerte und geschäftskritischen Werte schützen müssen.

Ein zentrales Thema kristallisiert sich klar heraus: Resilienz ist kein statischer Zustand, sondern eine fortlaufende Fähigkeit. Sie erfordert modernes Risikomanagement, kontinuierliche Investitionen in Kompetenzen, organisationales Lernen und die Einführung eines hochdynamischen Managements kritischer Ereignisse. Die Notwendigkeit, Zukunftsfähigkeit in sämtliche Betriebsprozesse zu integrieren, wird weiter steigen, da sich Risiken vervielfachen, verstärken und Grenzen zwischen isolierten Vorfällen und systemischen Bedrohungen zunehmend verschwimmen. Ein proaktiver, datengetriebener und integrierter Ansatz befähigt Organisationen, Störungen frühzeitig zu erkennen, zu überstehen, sich davon zu erholen und sich dauerhaft anzupassen.

Das Dynamische Krisen- und Notfallmanagement **(Everbridge High Velocity CEM™),** unterstützt durch zweckorientierte KI, steht an vorderster Front dieser neuen Resilienzgeneration. Seine intelligente Automatisierung, die Echtzeit-Risikointelligenz und die einheitliche Plattformarchitektur ermöglichen es Organisationen, Informationsrauschen zu durchdringen, Reaktionszeiten deutlich zu verkürzen und Kontinuität zuverlässig sicherzustellen – unabhängig von Art, Umfang oder Komplexität eines Ereignisses. Mit mehr als 6.500 Kunden weltweit hat Everbridge gezeigt, dass skalierbare, unternehmensgerechte Lösungen entscheidend sind, um den Anforderungen der expandierenden Risikozone gerecht zu werden.

Mit Blick auf die Zukunft wird die Herausforderung darin bestehen, Wachsamkeit zu bewahren und gleichzeitig eine Kultur der kontinuierlichen Verbesserung sowie funktionsübergreifenden Zusammenarbeit zu fördern. Organisationen, die mutig handeln, zukunftsorientierte Strategien konsequent operationalisieren und fortschrittliche Lösungen nutzen, werden nicht nur Unsicherheiten überstehen, sondern daraus gestärkt hervorgehen – und Widrigkeiten in nachhaltige Stärke und neue Chancen verwandeln.

Erleben Sie die Möglichkeiten live

Bereit, das Management kritischer Ereignisse zu transformieren und die Resilienz Ihrer Organisation nachhaltig zu stärken? Fordern Sie Ihre personalisierte Demo an und erleben Sie das Dynamische Krisen- und Notfallmanagement (Everbridge High Velocity CEM™) in Aktion.

Vereinbaren Sie Ihre Demo unter everbridge.com/de/demo

Demo vereinbaren

Zusätzliche Ressourcen

High Velocity CEM Webinar-Reihe

Erhalten Sie Expertenrat, praxisnahe Einblicke und bewährte Lösungen, um sowohl physische als auch digitale Bedrohungen wirksam zu bewältigen.

Unsere laufende Webinar-Reihe unterstützt Ihr Team dabei, Geschäftskontinuität und Resilienz in einer zunehmend komplexen und dynamischen Risikolandschaft sicherzustellen.

Hier registrieren →

Einblicke in Thought Leadership

Entdecken Sie inspirierende Artikel und Videos führender Branchenexpertinnen und -experten.

Resilienz bedeutet nicht nur, auf Krisen zu reagieren – sie entsteht durch vorausschauendes Denken, Anpassungsfähigkeit und die Fähigkeit, selbst in Zeiten tiefgreifender Störungen erfolgreich zu bleiben. Gewinnen Sie wertvolle Perspektiven von Stimmen, die die Zukunft resilienter Organisationen aktiv mitgestalten.

Hier ansehen →

Machen Sie eine virtuelle Tour

Erfahren Sie, wie Everbridge Ihre Organisation mit einer individuell zugeschnittenen Demo transformieren kann.

Wählen Sie Ihre Interessensbereiche – wir erstellen ein personalisiertes Video, das genau die Lösungen zeigt, die für Sie am wichtigsten sind.

Hier besuchen →

Rapid Resilience videos

Bleiben Sie über kritische globale Ereignisse informiert – mit aktuellen Updates und fundierten Analysen unserer Everbridge-Expertinnen und -Experten.

Die Rapid Resilience Videos vermitteln umsetzbare Strategien, die auf realen Entwicklungen basieren und nahezu in Echtzeit bereitgestellt werden.

Hier ansehen →

Entdecken Sie die Everbridge-Produktpalette

Lernen Sie das Dynamische Krisen- und Notfallmanagement (Everbridge High Velocity CEM™) kennen – die branchenweit fortschrittlichste Plattform für das Management kritischer Ereignisse.

Sie kombiniert Automatisierung, Risiko-Intelligenz und zweckorientierte KI und ermöglicht Resilienz im großen Maßstab. Erkunden Sie unsere vollständige Produktsuite, die Ihre Organisation in jedem Schritt ihrer Resilienzreise unterstützt.

Hier mehr erfahren →

Online-Ressourcen

Greifen Sie auf eine umfassende Wissensbasis zu – darunter Whitepapers, Analystenberichte, Online-Schulungen und Präsenzveranstaltungen.

Unser Ressourcen-Hub stellt Ihnen alle Werkzeuge bereit, die Sie benötigen, um modernes Krisenmanagement zu meistern, Geschäftskontinuität sicherzustellen und die heutige komplexe Risikolandschaft effektiv zu navigieren.

Hier erkunden →

Anhang

Entscheidende Zukunftsfragen

Zukunftssicherung erfordert vorausschauende Planung und die Bereitschaft, auf Vorstandsebene schwierige, aber entscheidende Fragen zu stellen. Die folgenden Leitfragen helfen Führungskräften dabei, Resilienz in den Bereichen Betrieb, Technologie und aufkommende Risiken wirksam zu verankern:

- **Wo liegen unsere Single Points of Failure –** bei Mitarbeitenden, Standorten, Technologien oder Lieferanten – und welche Notfallpläne greifen, wenn einer davon ausfällt?
- **Wie schnell können wir unsere fünf größten Risiken erkennen, bewerten, benachrichtigen und mobilisieren?** Sind unsere Playbooks aktuell und regelmäßig getestet?
- **Welcher Anteil unseres Umsatzes und Betriebs ist durch getestete Kontinuitätsmaßnahmen geschützt?** Wo bestehen noch Lücken?
- **Wie steuern wir den Einsatz von KI und schützen uns vor KI-gestützten Bedrohungen** wie Deepfakes oder automatisierten Angriffen?
- **Welche geopolitischen, regulatorischen oder klimatischen Risiken nehmen zu,** und welche Diversifikationsoptionen sind sofort einsatzbereit?
- **Verfügen wir über einen umfassenden Krisenkommunikationsplan,** der regelmäßig aktualisiert und in unterschiedlichen Szenarien getestet wird?
- **Welche Auswirkungen hätte ein groß angelegter Cyberangriff auf unsere Kernoperationen,** und wie verlässlich sind unsere Wiederherstellungsziele?
- **Wo gibt es Schwachstellen in unserer Lieferkette,** und welche alternativen Lieferanten, Routen oder Transportmodi sind bereits vorab genehmigt?
- **Ist unsere Organisation wirklich resilient und zukunftssicher?**

everbridge

Empowering Resilience

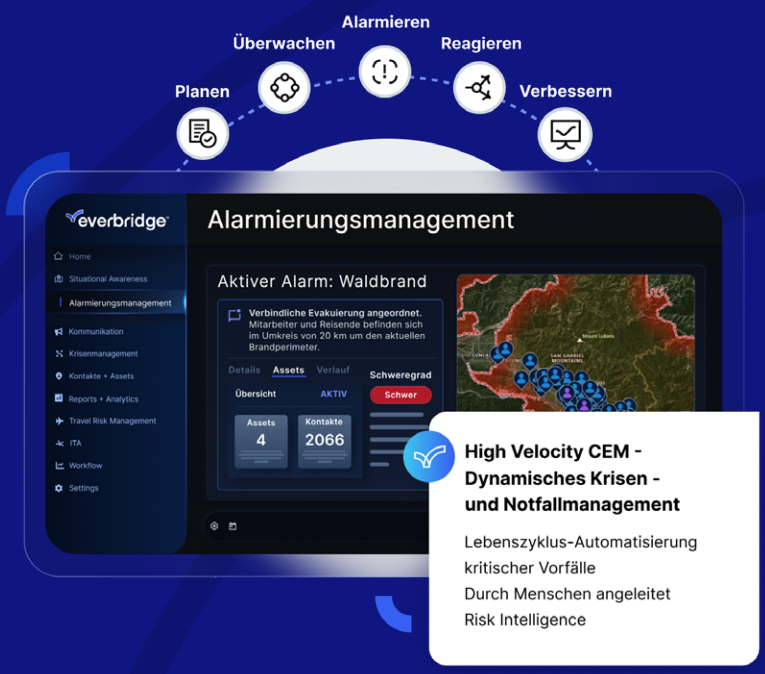
Über Everbridge

Everbridge ist der weltweit führende Anbieter im Bereich des Managements kritischer Ereignisse (CEM) und unterstützt Organisationen dabei, einen echten Vorteil in ihrer Geschäftsresilienz zu erzielen. Mit dem Dynamischen Krisen- und Notfallmanagement (Everbridge High Velocity CEM™) beschleunigen unsere Kunden ihre Reaktionszeiten, minimieren Störungen und behalten die operative Kontrolle – selbst angesichts der komplexesten Bedrohungen von heute.

Durch zweckorientierte KI, entscheidungsreife Risiko-Intelligenz und eine vollständige Lebenszyklus-Automatisierung ermöglicht Everbridge Organisationen, früher informiert zu sein, schneller zu reagieren und sich kontinuierlich und mit Zuversicht weiterzuentwickeln.

Everbridge — Keeping people safe and organizations running

- Besuchen Sie Everbridge.com
- Lesen Sie unseren Unternehmensblog
- Folgen Sie uns auf LinkedIn
- Folgen Sie uns auf X



Everbridge verschafft Organisationen einen klaren Vorteil in ihrer Geschäftsresilienz – mit dem Dynamischen Krisen- und Notfallmanagement (Everbridge High Velocity CEM™), unterstützt durch zweckorientierte KI und entscheidungsreife Risiko-Intelligenz. So lassen sich Reaktionszeiten verkürzen, Ausfallzeiten reduzieren und das schützen, was am wichtigsten ist. Fordern Sie eine Demo an unter everbridge.com/demo

WP-German-GlobalRiskAndResilienceOutlook2026 _12.03.25