SIEBER ADVISORS
PARTNER OF SENIOR STRATEGISTS NETWORK

Whitepaper

CORPORATE RISKS

Zehn Risiken, die das Vertrauen in Ihr Unternehmen gefährden – und was Sie dagegen tun können

Von Steffen Fritzsche, Sieber Advisors

1. Einleitung

Ein Cyberangriff, der Kundendaten kompromittiert, ein IT-Ausfall, der die Produktion stoppt, oder ein Sturm, der ganze Lieferketten unterbricht: Die Risiken für Unternehmen in Deutschland werden 2025 immer komplexer und gefährlicher. Laut aktuellem *Allianz Risk Barometer*[1], das die zehn wichtigsten Risiken für in Deutschland tätige Unternehmen im Jahr 2025 untersucht hat, sind Cybervorfälle, Betriebsunterbrechungen und Naturkatastrophen die größten Bedrohungen.

Herausforderung Polykrise

Die Lage ist kritisch: Ein außergewöhnliches Jahr 2024 – geprägt von extremer Wetterlage, geopolitischen Spannungen und einer wachsenden Abhängigkeit von digitalen Technologien – hat die Verwundbarkeit von Unternehmen offengelegt. Besonders auffällig ist die zunehmende Verflechtung unterschiedlicher Risiken in Gestalt der sogenannten Polykrise. Bei ihr treten mehrere Krisen gleichzeitig oder in enger Abfolge auf und beeinflussen oder verstärken sich gegenseitig. Beispiele dafür sind Naturkatastrophen und Cyberangriffe, die oft als Auslöser für Betriebsunterbrechungen wirken, während neue Technologien wie künstliche Intelligenz die Bedrohung durch Cyberkriminalität weiter verschärfen.

Vor diesem Hintergrund bietet dieses Whitepaper nicht nur eine Analyse der relevanten Risiken, sondern zeigt auf, wie Unternehmen mit strategischer Kommunikation und Krisenbewältigungsstrategien ihre Resilienz stärken und Krisen souverän meistern können.

2. Die entscheidende Rolle der Krisenkommunikation

Lackmustest für gutes Management

In einer Krise entscheidet die Kommunikation über Erfolg oder Misserfolg. Effektive Krisenkommunikation ist nicht nur eine Frage der Technik oder Geschwindigkeit, sondern vor allem der Strategie und Empathie. Sie ist der Dreh- und Angelpunkt, an dem sich zeigt, ob ein Unternehmen souverän reagiert und Vertrauen aufbaut – oder ob es durch Fehltritte, Schweigen oder widersprüchliche Aussagen in eine Spirale aus Misstrauen und Reputationsverlust gerät.

[1] Zur Methodik des Allianz Risk Barometers:
Das *Allianz Risk Barometer 2025* bietet eine umfassende Analyse der größten Risiken für Unternehmen weltweit und in Deutschland. Die jährliche Umfrage basiert auf den Antworten von 3.778 Risikomanagement-Experten aus 106 Ländern, darunter 451 aus Deutschland. Die Teilnehmer benannten jeweils die zehn größten

Die Top 10 Risiken für den Standort Deutschland 2025

1. **Cybervorfälle (47%)** – Die Bedrohung durch Ransomware, Datenlecks und IT-Systemausfälle bleibt führend.
2. **Betriebsunterbrechungen (40%)** – Lieferkettenprobleme und Energiekrisen destabilisieren den Betrieb.
3. **Naturkatastrophen (29%)** – Überschwemmungen und Hitzewellen nehmen durch den Klimawandel zu.
4. **Gesetzliche Änderungen und Regulierung (29%) –** Neue Vorschriften, insbesondere im Bereich Nachhaltigkeit und ESG, sowie geopolitische Entwicklungen belasten Unternehmen zunehmend.
5. **Brände/Explosionen (18%) –** Vorfälle mit erheblichen Schäden an Produktionsstätten und Lieferketten.
6. **Politische Risiken und Gewalt (17%) –** Geopolitische Spannungen und potenzielle Handelskriege sorgen für Unsicherheit und können direkte Auswirkungen auf die Geschäftstätigkeit haben.
7. **Klimawandel (17%) –** Neben Naturkatastrophen stellt die langfristige Anpassung an den Klimawandel eine wachsende Herausforderung dar.
8. **Fachkräftemangel (15%) –** Ein weiterhin relevantes Risiko, insbesondere durch wirtschaftliche Abschwächungen und Stellenabbau.
9. **Marktentwicklungen (13%) –** Intensiver Wettbewerb, Marktstagnation und wirtschaftliche Schwankungen machen strategische Anpassungen erforderlich.
10. **Blackouts/Infrastrukturversagen (12%) –** Stromausfälle und das Versagen kritischer Infrastruktur beeinträchtigen sowohl den operativen Betrieb als auch die Lieferketten.

Allianz Risk Barometer 2025 Appendix, 8: Figures represent how often a risk was selected as a percentage of all responses for that country. Respondents: 451. Figures don't add up to 100% as up to three risks could be selected.

Leadership in der Krise

Hier zeigt sich wahres Leadership: Unternehmen, die eine klare, faktenbasierte und empathische Kommunikation umsetzen, können die Kontrolle über die Situation behalten und sogar gestärkt daraus hervorgehen. Krisensituationen bieten die Möglichkeit, sich als verantwortungsbewusst und entschlossen zu präsentieren. Ein klug agierendes Management wird dabei nicht nur zum Problemlöser, sondern zum Helden in den Augen von Mitarbeitern, Kunden und der Öffentlichkeit.

Auf der anderen Seite kann schlechte Krisenkommunikation verheerend sein. Verzögerungen, inkonsistente Botschaften oder das Ignorieren der öffentlichen Wahrnehmung führen schnell zu Vertrauensverlust, negativen Schlagzeilen und einem irreparablen Imageschaden. In einigen Fällen haben Krisen, die falsch gemanagt wurden, zum endgültigen Aus für Unternehmen geführt.

Die Fähigkeit, Krisen durch strategische Kommunikation zu entschärfen, ist damit keine Option, sondern eine Überlebensnotwendigkeit. Denn während die Krise vorübergeht, bleiben ihre Auswirkungen auf die Reputation eines Unternehmens oft dauerhaft bestehen. Unternehmen, die in Krisenzeiten den richtigen Ton treffen, legen dagegen den Grundstein für langfristigen Erfolg und Resilienz.

Ganzheitliches Risikomanagement

Die Rangliste auf der vorherigen Seite gibt Aufschluss über die Prioritäten deutscher Unternehmen für 2025 und zeigt die zunehmende Komplexität und Vernetzung der Risiken auf. Das *Allianz Risk Barometer* unterstreicht die Notwendigkeit eines ganzheitlichen Risikomanagements, das sowohl operative als auch kommunikative Maßnahmen umfasst. Ein klarer Handlungsaufruf für Geschäftsführer, ihre Krisenprävention und -kommunikation auf den Prüfstand zu stellen.

3. Im Fokus: Die Top 3 Risiken für Deutschland

3.1. Cybervorfälle

Cyberangriffe sind die größte Bedrohung für deutsche Unternehmen. Neben den unmittelbaren finanziellen Schäden entstehen oft erhebliche Reputationsverluste durch die Verbreitung von Falschinformationen oder schlechte Krisenkommunikation.

Proaktive Informationssteuerung

- Unternehmen müssen klare, schnelle und faktenbasierte Botschaften vorbereiten, um Unsicherheiten zu reduzieren.

Klare, sachliche und angemessene Kommunikation sicherstellen, ohne Unsicherheiten zu verstärken.

- Die Kommunikation sollte faktenbasiert und abgestimmt mit IT-Sicherheits- und Rechtsabteilungen erfolgen.
- Spekulationen und ungesicherte Aussagen müssen vermieden werden, um Verwirrung oder mögliche rechtliche Konsequenzen zu minimieren.

Zielgruppen in den Vordergrund stellen, die trotz Unsicherheiten oder Verpflichtung zur Verschwiegenheit informiert werden müssen.

- Kunden: Sie müssen informiert und über mögliche Auswirkungen der Krise auf die Sicherheit ihrer Daten oder auf die Verfügbarkeit von Dienstleistungen aufgeklärt werden.
- Mitarbeiter: Klare interne Kommunikation ist entscheidend, um Unsicherheiten und Gerüchte zu vermeiden.
- Geschäftspartner: Offene und vertrauensbildende Kommunikation verhindert langfristige Reputationsschäden.
- Behörden und Regulierungsstellen: Eine proaktive Zusammenarbeit zeigt Verantwortungsbewusstsein und minimiert rechtliche Risiken.
- Medien und Öffentlichkeit: Eine angemessene Ansprache hilft, Reputationsschäden durch spekulative oder einseitige Berichterstattung zu reduzieren.

Ermittlungen der Polizei und Verhandlungen mit den Angreifern schützen, ohne die Transparenz zu beeinträchtigen.

- Im Zweifelsfall die Linie des abgestimmten Holding-Statements halten.
- Alle Kommunikationsmaßnahmen müssen eng mit den Ermittlungsbehörden und eventuell eingebundenen Cybersecurity-Experten abgestimmt sein.
- Interne Abstimmungen und die Freigabe von Informationen sollten klar geregelt werden, um keine sensiblen Details öffentlich werden zu lassen, die den Angreifern nutzen könnten.
- Die Balance zwischen Transparenz, Vertrauensaufbau und Schutz sensibler Informationen ist entscheidend, um die Krise effektiv zu managen und langfristigen Schaden zu vermeiden.

Für eine Verbesserung der Crisis Readiness haben sich **Incident-Response-Simulationen** bestens bewährt: Sieber Advisors nutzt die immersive Software *Conducttr*, um vor allem Cyberkrisen realistisch nachzubilden. Mit **KI-gestützter Automatisierung** können Szenarien wie Datenlecks oder IT-Ausfälle in **Echtzeit** simuliert werden, inklusive inklusive realitätsnaher Crisis Responsiveness und Social-Media-Dynamik.

3.2. Betriebsunterbrechungen

Betriebsunterbrechungen durch Lieferengpässe, Energiekrisen oder IT-Störungen gefährden Geschäftskontinuität und Kundenbeziehungen.

- **Stakeholder-Management:** Frühzeitige und transparente Kommunikation mit Lieferanten und Kunden sichert das Vertrauen.
- **Narrativbildung:** Positive Botschaften darüber, wie das Unternehmen Probleme aktiv löst, stärken die Außenwahrnehmung.
- **Simulation von Eskalationen:** In unseren Krisensimulationen können Unternehmen Lieferkettenunterbrechungen antizipieren und die interne sowie externe Kommunikation in Echtzeit testen.

3.3. Naturkatastrophen

Naturkatastrophen wie Überschwemmungen und Hitzewellen nehmen auch in Deutschland zu und haben nicht nur wirtschaftliche, sondern auch gesellschaftliche Folgen.

- **Multi-Stakeholder-Kommunikation:** Schnelle Einbindung derwichtigsten Stakeholder und Notfall-Pressekonferenzen mit Behördenvertretern schaffen Vertrauen und helfen, Verantwortlichkeiten zu klären.
- **Empathische Krisenansprache:** In Katastrophensituationen ist eine sensible Kommunikation entscheidend, um das Vertrauen der Öffentlichkeit zu sichern.
- **Krisen erfahrbar machen:** Im Rahmen unserer Krisensimulationen lassen sich Katastrophenszenarien vollständig durchspielen – von Notfall-Evakuierungen bis hin zu Presse-Statements.

4. Fazit

2025 wird erneut geprägt sein von dynamischen und miteinander verknüpften Risiken. Cyberangriffe bleiben die größte Bedrohung für Unternehmen in Deutschland, verstärkt durch die rasante Entwicklung der künstlichen Intelligenz. Betriebsunterbrechungen, die oft als Folge anderer Risiken auftreten, und Naturkatastrophen, deren Intensität durch den Klimawandel zunimmt, erfordern ein strategisches Umdenken in der Unternehmensführung.

Stärkung der Resilienz als strategisches Ziel

Wie das *Allianz Risk Barometer* zeigt, ist Resilienz nicht nur ein operatives Ziel, sondern eine strategische Notwendigkeit. Durch Krisenbewältigungsstrategien können Unternehmen diese stärken und

Krisen souverän meistern. Vanessa Maxwell, Leiterin Risikoprüfung bei Allianz, bringt es auf den Punkt: „Unternehmen müssen Resilienz ganz oben auf ihre Agenda setzen und sich konsequent um die Verbesserung ihres Risikomanagements und ihrer Widerstandsfähigkeit bemühen“.[2]

Die Frage ist nicht, ob eine Krise eintritt, sondern wann. Unternehmen, die vorbereitet sind, können nicht nur Schäden begrenzen, sondern durch gezielte und faktenbasierte Kommunikation Vertrauen und Glaubwürdigkeit aufbauen – selbst in den schwierigsten Zeiten.

5. Kontakt

Möchten Sie mehr über realitätsnahe Krisensbewältigungsstrategien erfahren, die Ihre Organisation auf den Ernstfall vorbereiten und Ihre Teams fit für die Krise machen?

Kontaktieren Sie uns für eine unverbindliche Beratung.

Steffen Fritzsche
Mobil: + 49 160 534 2032
Mail: steffen.fritzsche@sieber-advisors.de

[2] Pressemitteilung Allianz Risk Barometer 2025, 15. Januar 2025