Securitas

Risk Intelligence Center

Annual Intelligence Estimate

Ausgabe 2026

Januar 2026

intelligence@securitas.com

Inhalt

Einführung

Mike Evans

Director, Risk Intelligence Center

SCHÖNE NEUE WELT: WO ES RISIKEN GIBT, GIBT ES AUCH CHANCEN

Noch nie zuvor ist es vorgekommen, dass sowohl Sicherheit als auch Risiko zum Schutz von Unternehmen notwendig waren, um weiter und schneller vorwärts zu kommen und für die Zukunft gerüstet zu sein. Sicherheit ist dabei keine Kostenstelle, sondern ein strategisches Mittel zur Geschäftsführung – und Risiko ist kein Mittel zur Verwaltung dieser Kosten, sondern zur Entscheidungsfindung. Sicherheit und Risiko verschaffen Unternehmen als Teil einer informationsgestützten Strategie den Vorteil und das Vertrauen, Risiken zu beherrschen und Chancen zu nutzen.

Die Ereignisse in den letzten Tagen des Jahres 2025 – und den ersten Tagen des Jahres 2026 – geben den Ton für die Risiko- und Sicherheitslage im kommenden Jahr an:

- **Unwahrscheinlich bedeutet nicht unmöglich:** Die (erneute) Bewertung von Risiken mit geringer Wahrscheinlichkeit, aber großen Auswirkungen unter dem Aspekt, wann sie eintreten und nicht, ob sie eintreten, sowie die Vorbereitung auf Worst-Case-Szenarien tragen dazu bei, die bestmöglichen Ergebnisse zu erzielen.
- **Divergenz treibt Konvergenz voran:** Die Welt ändert sich ständig. Unternehmen sind direkt (und indirekt) von globalen und lokalen Ereignissen betroffen – physisch und digital, ob sie sich dessen bewusst sind oder nicht – und Situationsbewusstsein und Verständnis sind der Schlüssel zu einem erfolgreichen Umgang mit diesen Ereignissen.
- **Sicherheit als strategischer Wegbereiter:** Wo es Risiken gibt, gibt es auch Chancen. Angesichts der Öffnung (und Schließung) neuer Märkte, der sich ändernden Verbraucherwünsche und der öffentlichen Meinung sind Sicherheit und Risiko von entscheidender Bedeutung, um Unternehmen zu schützen und ihnen zu ermöglichen, ihre Ziele zu erreichen.

Aus der Sicht der Entscheidungsträger ist das derzeitige Klima in der Regel geprägt vom Konzept „Hohes Risiko/Hohe Belohnung“. Eine andere Sichtweise ist jedoch „Beherrschtes Risiko/Maximale Belohnung“. Dies ist ein wichtiges Thema für Unternehmen in der heutigen unsicheren globalen Risikolandschaft, das auch im Mittelpunkt des Annual Intelligence Estimate 2026 des Securitas Risk Intelligence Center (RIC) steht.

WAS IST DER ANNUAL INTELLIGENCE ESTIMATE DES SECURITAS RIC?

Der Annual Intelligence Estimate des Securitas Risk Intelligence Center (RIC) ist ein Bericht, der Fachleuten für Unternehmenssicherheit und Sicherheitsrisiken verwertbare Informationen für das kommende Jahr – und darüber hinaus – bietet.
Der Annual Intelligence Estimate umfasst:

- **Strategische Sicherheits- und Risikofaktorenanalyse** zur Ermittlung von Schlüsselthemen, Trends, Mustern und neuen Signalen, die die Sicherheits- und Risikolandschaft im Jahr 2026 prägen.
- **Bewertung der Unternehmenssicherheit anhand von Daten** für Unternehmen aller Branchen und Standorte, einschließlich der Analyse von Bedrohungs- und Sicherheitsdaten.
- **Weltweite Risikodatenbewertungen,** die globale, regionale und lokale Daten abdecken, einschließlich geopolitischer Bedrohungs- und Risikoanalysen.
- **Wildcard-Szenario-Analyse,** die verschiedene Szenarien mit hoher Auswirkung und geringer Wahrscheinlichkeit, aber weitreichenden Folgen für Unternehmen untersucht.
- **Eckdaten 2026** zur Hervorhebung von Brennpunkten mit erhöhter Bedrohung und Risiken im Zusammenhang mit geplanten Ereignissen, einschließlich geopolitischer, politischer und sozialer Ereignisse.

Der Bericht ist als handlungsorientierte Alternative zu anderen thematischen Bewertungen gedacht und richtet sich insbesondere an Entscheidungsträger im Sicherheitsbereich. Der Annual Intelligence Estimate schließt die Lücke zwischen strategischen Risikobewertungen für Führungskräfte und taktischen Analysen für den Einsatz im Tagesgeschäft. Damit möchte er diejenigen unterstützen, die für den Schutz von Menschen, Eigentum und anderen schützenswerten Dingen verantwortlich sind.

Der Annual Intelligence Estimate vermittelt Unternehmen aller Branchen und Sektoren ein Situationsbewusstsein und ein Verständnis für die Situation. Als solcher ist er ein leicht verständlicher Abriss mit praktischen Überlegungen für ein breites Publikum.
Das RIC erstellt auf Anfrage jedoch auch unternehmensspezifische, branchenrelevante und geografisch zugeschnittene Bewertungen.

Haben Sie Fragen zu diesem Bericht oder möchten Sie Ihren konkreten Informationsbedarf besprechen, wenden Sie sich bitte an das RIC.

Unser Intelligence Toolkit

Bewusstseinsbildung

Regelmäßige geplante und fallbezogene Berichterstattung über die globale Sicherheits- und Bedrohungslage. Dies schließt Informationsberichte und Lageberichte ein.

- Tägliche globale Informationsberichte
- Wöchentliche globale Informationsausblicke
- Monatliche Bedrohungsprognosen
- Monatliche Informations-zusammenfassungen
- Lageberichte und Informationsberichte zu wichtigen Entwicklungen

Warnmeldungen

Standortspezifische E-Mail-Warnungen zu Sicherheits- und Bedrohungsereignissen in der Nähe. Diese können auf Grundlage von Schweregrad, Nähe und Häufigkeit nach Vorfallsarten angepasst werden:

- Kriminalität
- Zivile Unruhen
- Terrorismus
- Wetterereignisse
- Reisen und Beförderung

Handlungs-empfehlungen

Eine **umfassende** Schutz-, Bedrohungs- und Risikoanalyse für Ihr Unternehmen, Ihr Geschäft und Ihre Marke. Dies umfasst:

- Überwachung für Ihre konkreten Anforderungen
- Zusammenfassungen der täglichen Überwachungs-berichte
- Unverzügliche Informationen zu Warnmeldungen
- Lösung für Bedrohungs-, Schutz- und Risikoinformationen
- Zugriff auf die fallbezogene Berichterstattung

Analyst

Eigens erstellte Informationsressourcen, die auf das Fachwissen der Global Intelligence Community von Securitas zurückgreifen.

Ausgestattet mit allen Tools und Schulungen zur Deckung Ihres Informationsbedarfs, um Ihr Unternehmen zu schützen.

Fallbezogene Informationen

Fachwissen und Beratung für alle dynamischen, konkreten Informationsanforderungen Gängige Berichtstypen sind unter anderem:

- Reise- und Sicherheitsbericht für Reisende: Tiefgreifende Analyse von Gefahren für die Reisesicherheit.
- Personenschutz und Abwehrinformationen: Bewertung von Schwachstellen einer Zielperson anhand von Informationen (z. B. Führungskraft).
- Sicherheitsprüfung und -überwachung von Veranstaltungen: Sorgfältige Prüfung und Live-Überwachung.

Unser Team


ALEX JOHNSON


ALMA ABRAHAM


ANASTASIA JOBARD


BEN GIDDINGS


CIAN LYNCH


FREDDIE VENABLES


JOHN COUDRIET


JOSHUA MENDELSON


JUANITA JOHNSON


KIMBERLEY DEAN


LAURA STEVENS


LOUISE MARTIN


LUCY DICKENS


MATT PHILLIPS


NATHAN SKEET


NICK FULLICK


OLIVER BACCHUS


SOPHIE CAIRNEY


CHARMIAN TAYLOR


PIERS REGISTER


MIKE EVANS

Unser Ansatz

Das RIC bezieht Informationen und Daten aus allen möglichen Quellen und nutzt alle verfügbaren und geeigneten Informationsquellen anhand der Datenanforderungen.

Der Ansatz kombiniert das Fachwissen unserer internen Analysten, das globale Netzwerk von Securitas, Dritten und Partnern sowie modernste Technologie für Open-Source-Intelligence, um Informationen höchster Qualität zusammenzutragen. Die Aufnahme in den Annual Intelligence Estimate bedeutet nicht, dass eines dieser Szenarien eintreten wird. Es besteht jedoch die Möglichkeit, dass die Bedrohung auftreten kann, sodass sie bei der Durchführung von Sicherheitsüberprüfungen und Risikobewertungen berücksichtigt werden sollte.

Bedrohungsstufen

In diesem Bericht werden die Bedrohungsstufen des RIC verwendet, um Bedrohungen auf einer Skala von 1 bis 5 zu bewerten. Diese Bewertung beruht auf der Einschätzung der Eintrittswahrscheinlichkeit und des Schweregrads bzw. der Absicht und Möglichkeit.

5 – EXTREM	Sehr hohe/extreme Bedrohung. Prüfen und wenn nötig reagieren.
4 – HOCH	Hohe/große Bedrohung. Geeignete Maßnahmen in Erwägung ziehen.
3 – MODERAT	Moderate Bedrohung. Bewusstseinsbildung aufrechterhalten, Vorsichtsmaßnahmen in Betracht ziehen.
2 – GERING	Geringe/eingeschränkte Bedrohung. Beratung in Anspruch nehmen.
1 – SEHR GERING	Sehr geringe/vernachlässigbare Bedrohung. Zur Bewusstseinsbildung.

Terminologie der Eintrittswahrscheinlichkeit

Dieser Bericht stützt sich auf die Terminologie der Eintrittswahrscheinlichkeit des RIC, um die Eintrittswahrscheinlichkeit einer Bedrohung auf Grundlage der Wahrscheinlichkeit unter Verwendung von Prozentsätzen, Anteilen oder Verhältnissen einzuschätzen. Dies schafft Kontext und Klarheit und ein einheitliches Verständnis der Bewertung und der verwendeten Terminologie.

Begriff	Wahrscheinlichkeit
Fernliegend	0–5 %
Sehr unwahrscheinlich	10–20 %
Unwahrscheinlich	25–35 %
Realistische Möglichkeit	40–50 %
Wahrscheinlich	55–75 %
Sehr wahrscheinlich	80–90 %
Nahezu sicher	95–99 %

Stichtag für Informationseingang	**00:00 UTC, 5. Januar 2026**

Trends, Muster und Einflussfaktoren

Die Annual Intelligence Estimates des RIC der Jahre 2023, 2024 und 2025 zeigen eine Vielzahl von Trends und Mustern innerhalb der globalen Sicherheitsbedrohungslandschaft auf, die direkte Auswirkungen auf Unternehmen – darunter auf die Sicherheit, den Betrieb, die Marke und den Ruf – hatten und haben. Einige der Bedrohungen haben sich in den letzten Jahren überschnitten und weiterentwickelt und umfassen nun neue Bedrohungsakteure, Taktiken und Ziele. Daneben sind völlig neue Bedrohungsszenarien und strategische Faktoren in den Vordergrund gerückt. Unternehmen sehen sich zunehmend größeren Bedrohungen und Risiken ausgesetzt, die sich aus der veränderlichen globalen Bedrohungslage ergeben. Das bedeutet, dass die proaktive Bereitstellung von Informationen immer wichtiger wird, um Unternehmen über die vorrangigsten Bedrohungen zu informieren.

Die Bedrohungs- und Risikoszenarien für die Unternehmenssicherheit in den Annual Intelligence Estimates des RIC der Jahre 2023, 2024, 2025 und 2026 sollen Unternehmen einen Entscheidungsvorteil verschaffen, um die potenziellen Auswirkungen der globalen Sicherheitsbedrohungen zu begrenzen. Die Hauptthemen sind nachfolgend aufgeführt:

2023

- ESG-Initiativen führen zu Gegenreaktionen und Sicherheitsbedrohungen
- Chronische Belastungen durch den Klimawandel und akute Schocks durch Naturkatastrophen
- Abwägung zwischen Gesundheitssicherheit und Überempfindlichkeit
- Cyberbedrohungslandschaft verändert sich ständig
- Störungen bei der Informationsversorgung und zunehmende Bedrohung durch „Fake News“ in der realen Welt
- Aktivistenlage weitet sich aus
- Umbruch und Entwicklung bei Terrorismus und Extremismus
- Spionage in Unternehmen und deren Ressourcen
- Widerstandsfähigkeit und Sicherheit in der Energieversorgung
- Bedrohung der Widerstandsfähigkeit und Sicherheit der globalen Lieferketten

2024

- Annäherung der geopolitischen und gesellschaftspolitischen Motivationen von Bedrohungsakteuren
- Störung der Lieferketten durch Engpässe und Machtkämpfe
- Superwahljahr 2024
- Wettrüsten mit künstlicher Intelligenz
- Klima- und Umweltrisiken stoßen an neue Grenzen
- Starker Anstieg bei der Cyberkriminalität
- Globale Auswirkungen des wirtschaftlichen Abschwungs in China
- ESG-Gegenreaktionen gehen von Drohungen zu Taten über
- Kritische Infrastrukturen bleiben eine entscheidende Schwachstelle
- Zunehmende Unternehmensspionage verlagert Fokus auf Spionageabwehr

2025

- Wandel der auf Regeln basierenden Ordnung verstärkt Besorgnis über möglichen Zusammenbruch
- Verstärkte Kriegsführung und Sabotage in der Grauzone bedrohen die Sicherheit von Unternehmen
- Unternehmen bereiten sich verstärkt auf Kriegsszenarien vor
- Führungskräfte und Politiker im Fadenkreuz von Bedrohungsakteuren
- KI steht vor einem Wendepunkt
- Ideologische Insider bedrohen zunehmend die Sicherheit von Unternehmen
- Verstärkte Überschneidung der Motivationen von Bedrohungsakteuren
- Ausnutzung von Drohnen für feindliche Zwecke
- Nutzung sozialer Medien schürt Störungen bei der Informationsversorgung
- Auswirkungen von Vorfällen im Bereich Gesundheitssicherheit wirken sich auf die gesamte Lieferkette aus

2026

- Bedrohungsakteure zielen für maximale Wirkung auf kritische nationale Infrastrukturen ab
- Rückschritte der Unternehmen bei ESG-Herausforderungen treiben Aktivismus voran
- Massenentlassungen aufgrund von KI verstärken unternehmensfeindliche Stimmung und erhöhen Insiderrisiken
- Zunehmend protektionistische Maßnahmen zur Sicherung der Unabhängigkeit von Ländern
- Bedrohungsakteure nutzen anfällige öffentliche und private Veranstaltungen aus
- Nachhaltigkeits-bedenken behindern ressourcenintensive Infrastrukturprojekte
- Reaktion der Behörden auf Drohnengefahr fördert weitere Instrumentalisierung
- Risiken für Unternehmen durch zunehmende Abhängigkeit von Cloud-Umgebungen
- Bedrohung der Informationslandschaft durch aufkommende GenAI
- Zunehmende Instru-mentalisierung der sozialen Medien zur Erleichterung von Massen-Doxxing-Kampagnen

Strategische Risikofaktoren

P Politisch

STRATEGISCHE RISIKOFAKTOREN 2025

- Der Machtwechsel in den USA führte zu einer Verlagerung hin zu „geopolitischem Transaktionismus“ und belastete traditionelle Bündnisse.
- Die (größtenteils durch Konflikte geschürte) nationale/regionale Instabilität zog dabei internationale Mächte in Mitleidenschaft und beeinflusste die Innenpolitik und Sicherheit in nicht betroffenen Ländern.
- Die Verschärfung des Konkurrenzkampfes zwischen den Großmächten, insbesondere zwischen China und den USA sowie zwischen Russland und dem Westen, führte zu einer Neuausrichtung der Außenpolitik in allen Regionen und zu verstärkten Aktivitäten bei der Kriegsführung im Grauzonenbereich.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Demokratische Rückschritte und Probleme bei der Staatsführung (einschließlich Korruption und Aushöhlung der Rechtsstaatlichkeit) dürften die Wahrscheinlichkeit von Unruhen erhöhen.
- Radikale Politik wird im Westen immer mehr zum Mainstream und führt zu raschen Gesetzesänderungen, Unruhen und einem polarisierenden Diskurs, der Unternehmen und hochrangige Persönlichkeiten ins Visier nimmt.
- Der zunehmend diktatorische Führungsstil, mit dem vor allem unilaterale Maßnahmen einhergehen, verstärkt die Dynamik von „Macht geht vor Recht“ weiter und erhöht das Risiko von Eskalationen, Fehlkalkulationen und Konflikten.

E Wirtschaftlich

STRATEGISCHE RISIKOFAKTOREN 2025

- Protektionistische Handelsmaßnahmen führten zu erheblichen Störungen der Lieferkette, erhöhten die Kosten und schwächten das Vertrauen der Investoren.
- Die Inflation ging in vielen Regionen zurück, doch die hohen Lebenshaltungskosten und die Lohnstagnation führten weltweit zu Arbeitsunruhen und Streiks.
- Schwankende Energiemärkte aufgrund von Konflikten, Produktionskürzungen und Sanktionen führten zu unvorhersehbaren Betriebskosten in energieintensiven Branchen.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Die anhaltende Fragmentierung des Welthandels, bedingt durch Protektionismus und politische Unsicherheit, wird wahrscheinlich zu höheren Betriebskosten und der Erschwerung des Marktzugangs führen.
- Die Konkurrenz um wichtige Mineralien und technologische Produktionskapazitäten wird sich verschärfen und Einfluss auf wirtschaftliche Allianzen haben.
- Aufgrund der hohen Staatsverschuldung besteht die realistische Möglichkeit, dass Sparmaßnahmen erzwungen werden und damit das Risiko von Unruhen erhöhen.

S Sozial

STRATEGISCHE RISIKOFAKTOREN 2025

- Die von der Generation Z angeführte digitale Mobilisierung führte zu dezentralen Protesten im Globalen Süden gegen regionale und sich überschneidende Missstände, darunter Korruption und hohe Jugendarbeitslosigkeit.
- Der KI-bedingte Verlust von Arbeitsplätzen wurde zu einem öffentlichkeitswirksamen Thema, da die Entlassungen in den Unternehmen explizit mit der Einführung autonomer Systeme und KI-Agenten begründet wurden.
- Migration und Grenzkontrollen sind nach wie vor eine akute Sicherheitspriorität, da es aufgrund der anhaltenden Konflikte und der durch den Klimawandel verursachten Naturkatastrophen zu massiven Migrationsströmen kommt.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Die globale Kluft zwischen den Generationen wird sich vertiefen, da die jüngere Bevölkerung mehr soziale Gerechtigkeit fordert, was zu einem verstärkten physischen und digitalen Aktivismus im gesamten Globalen Süden führt.
- Der soziale Zusammenhalt wird sich wahrscheinlich weiter verschlechtern, da widersprüchliche Informationen im Internet, wirtschaftlicher Druck und politisches Misstrauen Polarisierung und extremistische Narrative anheizen.
- Die Kürzung globaler Hilfsbudgets wird die humanitären Bemühungen wahrscheinlich belasten und das Gesundheits- und Migrationsrisiko erhöhen.

Die Analyse der politischen, wirtschaftlichen, sozialen, technologischen, rechtlichen und ökologischen Faktoren (Political, Economic, Social, Technological, Legal, Environmental; PESTLE) umreißt die wichtigsten externen Faktoren, die als prägend für das Geschäftsumfeld im Jahr 2025 identifiziert wurden, sowie die Faktoren, die voraussichtlich im Jahr 2026 zu beobachten sein werden. Sie zeigt die Faktoren auf, die die Unternehmensstrategie, die Risikoexposition und die Entscheidungsfindung von Unternehmen aller Branchen weltweit beeinflussen.

Die Analyse verdeutlicht, wie geopolitische Instabilität, wirtschaftliche Volatilität, gesellschaftlicher Wandel, technologische Abhängigkeit, regulatorische Komplexität und Umweltstressfaktoren zusammenwirken und so Risiken und Chancen für Unternehmen schaffen. Durch die Ermittlung aktueller strategischer Faktoren und deren erwarteter Auswirkungen bietet die Analyse einen strukturierten Überblick über Trends auf Makroebene. Diese müssen Unternehmen überwachen, sich an sie anpassen und in ihre langfristige Planung und Resilienzstrategien einbeziehen.

T Technologisch

STRATEGISCHE RISIKOFAKTOREN 2025

- Die Anfälligkeit der vernetzten IT-Infrastruktur ist durch mehrere großflächige Internetausfälle, z. B. bei Cloudflare, und größere Ausfälle von Rechenzentren deutlich geworden.
- Die Zunahme hochkarätiger Cyberangriffe mit Ransomware und Eingriffen in die Lieferkette führte in allen Branchen zu erheblichen Betriebsausfällen.
- Die Konkurrenz um wichtige Mineralien, die für moderne Technologien und Halbleiter wichtig sind, hielt an und prägte die nationale Sicherheitspolitik.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Da Länder zunehmend ihren Anspruch auf KI-Systeme geltend machen, werden Unternehmen mit einer stets stärkeren multipolaren digitalen Ordnung konfrontiert sein, darunter unterschiedliche Sicherheitsanforderungen, Vorschriften und Einhaltung von Gesetzen in verschiedenen Regionen.
- Die immer schneller voranschreitende Entwicklung von Quantentechnologien verschärft die geopolitische Konkurrenz, was zu verstärkten Exportkontrollen führt und gleichzeitig die langfristigen Sicherheitsrisiken für Unternehmen erhöht.
- Die Verlagerung der Produktion erhöht die Betriebskosten der Unternehmen, stärkt aber die Sicherheit der Lieferkette.

L Rechtlich

STRATEGISCHE RISIKOFAKTOREN 2025

- Die globalen Governance-Strukturen standen zunehmend unter Druck bzw. wurden nicht eingehalten, was zu Ausfällen und Verstößen gegen internationales Recht führte.
- Die Ausweitung internationaler Sanktionen gegen strategische Industriezweige und Länder eskalierte weiter, was für Unternehmen Betriebs- und Reiserisiken mit sich brachte.
- Die Verzögerung bei der Regulierung von Hochrisikotechnologien, einschließlich KI, ermöglichte die Ausnutzung durch böswillige Akteure und schuf Unsicherheit bei der Einhaltung von Vorschriften.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Die rechtliche Verantwortung für Fahrlässigkeit im Internet, Datenschutzverletzungen und Umweltschäden wird weiter zunehmen, was die Finanz- und Reputationsrisiken für Unternehmen erhöht.
- Rechtsstreitigkeiten über territoriale Ansprüche, Seerechte und den Zugang zu Ressourcen werden wahrscheinlich zunehmen und sich auf die Seewege und multinationale Risiken auswirken.
- Die Ausweitung staatlicher Notstandsbefugnisse, die häufig in Zeiten von Unruhen eingeführt werden, wird wahrscheinlich den Geschäftsbetrieb erschweren und die bürgerlichen Freiheiten einschränken.

E Ökologisch

STRATEGISCHE RISIKOFAKTOREN 2025

- Der Druck auf die Wasserressourcen erreichte in mehreren wichtigen Wirtschaftszonen (z. B. Südeuropa, Südasien) ein ernsthaftes Ausmaß und führte zu lokalen Störungen in der Landwirtschaft und Industrie.
- Hochkarätige Gerichtsverfahren, in denen gegen Unternehmen wegen angeblicher Greenwashing-Behauptungen eingeleitet wurden, schufen Präzedenzfälle und brachten Risiken für den Ruf von Marken mit sich.
- Anhaltend extrem hohe Temperaturen, Hitzewellen und extreme Wetterereignisse überall auf der Welt verursachten schwere Infrastrukturschäden und Lieferkettenprobleme.

ERWARTETE STRATEGISCHE FAKTOREN 2026

- Unternehmen, denen einen Mitschuld an der Verschlechterung des Klimas gegeben wird, müssen sich verstärkt mit rechtlichen Schritten und Protesten auseinandersetzen.
- Extreme Wetterereignisse und Naturkatastrophen nehmen an Häufigkeit und Intensität zu und stören die globalen Logistiknetze, beschädigen die Energieinfrastruktur und gefährden die Sicherheit der Arbeitskräfte.
- Die klimabedingte Ressourcenknappheit wird die grenzüberschreitenden Spannungen verschärfen und das Konfliktrisiko erhöhen.

Unternehmens-sicherheit

1

Bedrohungsakteure zielen für maximale Wirkung auf kritische nationale Infrastrukturen ab

Angriffe auf kritische nationale Infrastrukturen haben im Jahr 2025 stetig zugenommen, wobei feindliche Bedrohungsakteure sowohl kinetische als auch nichtkinetische Taktiken, Techniken und Prozeduren einsetzten. Mit der Eskalation weltweiter Spannungen in verschiedenen Krisenherden zielen staatlich geförderte Bedrohungsakteure/Akteure in der Grauzone, Aktivistengruppen, extremistische Organisationen und Einzeltäter auch weiterhin auf traditionelle kritische Infrastrukturen wie Energie, Wasser und Kommunikation sowie neue Ziele wie Rechenzentren und Flughäfen ab. Der einfache Zugang zu Tools für Cyberangriffe sowie die Verbreitung von kommerziell erhältlichen unbemannten Fluggeräten – Drohnen – haben es Bedrohungsakteuren ermöglicht, mit minimalem Aufwand maximale Schäden an kritischen nationalen Infrastrukturen anzurichten.

- Feindliche Bedrohungsakteure werden mit ziemlicher Sicherheit weiterhin auf kritische nationale Infrastrukturen abzielen, und zwar sowohl mit traditionellen Methoden wie physischer Sabotage als auch mit nichtkinetischen Verfahren wie Malware und Cyberangriffen.
- Länder werden wahrscheinlich verstärkt Erfüllungsgehilfen wie organisierte kriminelle Gruppen einsetzen, um Sabotage- und Störangriffe auf kritische Infrastrukturen durchzuführen, um den politischen Druck zu erhöhen, feindliche Nationen zu destabilisieren und Unsicherheit zu schaffen, während die Bestreitbarkeit immer besser wird.
- Um weitreichende Störungen zu verursachen, werden radikale Aktivistengruppen wahrscheinlich verstärkt physische Sabotage- und Cyberangriffe auf kritische von Unternehmen betrieben oder unterstützt werden, denen zugeschrieben wird, dass sie den Zielen der Gruppe entgegenwirken.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Verbesserte geopolitische und gesellschaftspolitische Aussichten führen zu einem Rückgang der Angriffe auf kritische Infrastrukturen, was vor allem auf ein geringeres Interesse und weniger Vorsatz der Aktivisten zurückzuführen ist. Bei nachlassenden Spannungen verringern die Länder den Einsatz von Erfüllungsgehilfen zur Durchführung von Aktionen in der Grauzone.	Verbesserung	Sehr unwahrscheinlich (10 %)
Globale Spannungen nehmen weiter zu. Im Mittelpunkt stehen anhaltende Konflikte und Krisenherde, einschließlich ökologischer, sozialer und wirtschaftlicher Themen. Aktivisten zielen zunehmend auf kritische Infrastrukturen ab, um mehr Aufmerksamkeit für ihre Anliegen zu erreichen.	Baseline	Wahrscheinlich (55 %)
Die geopolitischen Spannungen eskalieren weiter, wodurch sich mehr Länder veranlasst sehen, zunehmend direkte Angriffe auf kritische Infrastrukturen auszuführen, einschließlich des Einsatzes von Erfüllungsgehilfen als Teil umfassender Angriffsmethoden.	Verschlechterung	Unwahrscheinlich (35 %)

Handlungsempfehlungen

- Bewerten Sie die Gefährdung des Unternehmens (sowohl direkt als auch indirekt, z. B. durch Partner in der Lieferkette) durch betriebliche Auswirkungen, die sich aus einer Störung der kritischen Infrastruktur ergeben.
- Stellen Sie sicher, dass die Ausfallsicherheit und Abhilfemaßnahmen in Bezug auf die wichtigsten Versorgungsströme (wie Energie, Wasser, Telekommunikation usw.) gewährleistet sind, um im Falle einer Beeinträchtigung der Verfügbarkeit kritischer Infrastrukturen belastbare betriebliche Prozesse und Funktionen bereitzustellen.
- Beobachten Sie Regionen, die für geopolitische Umwälzungen oder Störungen anfällig sind, und behalten Sie diese im Auge, insbesondere wenn diese Regionen wichtig für die betriebliche Stabilität sind. Überwachen Sie die amtlichen Bekanntmachungen in diesen Gebieten.

Indikatoren	Auswirkungen
— Verstärkte Rhetorik im Zusammenhang mit dem Welthandel, insbesondere in Bezug auf Zölle, Sanktionen und den Zugang zu seltenen Mineralien. — Zunehmende Spannungen über Landesgrenzen hinweg in politisch instabilen Regionen. — Häufigerer und stärkerer Einsatz von Drohnen durch Bedrohungsakteure über beschränktem Luftraum. — Verstärkte Berichterstattung in den sozialen Medien über erfolgreiche Angriffe auf kritische Infrastrukturen durch Aktivistengruppen. — Vermehrte digitale Kommunikation von Aktivistengruppen, die sich zu Angriffsmethoden auf kritische Infrastruktur äußern oder Websites empfehlen.	— Unternehmen, die für kritische Infrastrukturen verantwortlich sind oder Verbindungen zu diesen Infrastrukturen haben, sind einem größeren Risiko ausgesetzt, ins Visier von Bedrohungsakteuren zu geraten. — Eingeschränkter Zugang zu kritischen Materialien bei zunehmender Isolierung aufgrund von abstreitbaren feindlichen Aktivitäten in der Grauzone gegen kritische Infrastrukturen. — Beeinträchtigung der täglichen Betriebsabläufe durch Unterbrechungen der kritischen Kommunikationsinfrastruktur. — Erhöhter Kostenaufwand und rechtliche Verantwortung im Zusammenhang mit der Verwaltung und dem Betrieb von Betreiberverträgen für kritische Infrastruktur. — Verlust kritischer Daten und Informationen und zunehmende Abhängigkeit von externen Faktoren zur Aufrechterhaltung der Datenintegrität im Zusammenhang mit der kritischen Infrastruktur von Rechenzentren.

Rückschritte der Unternehmen bei ESG-Herausforderungen treiben Aktivismus voran

Aktivistengruppen nehmen weiterhin Unternehmen ins Visier, die ihrer Meinung nach gegen Umwelt-, Sozial- und Governance-Verpflichtungen (Environmental, Social, Governance; ESG) verstoßen, indem sie langwierige Boykotte, Demonstrationen und Kritik im Internet ausüben. Unternehmen wird vorgeworfen, dass sie ihre Netto-Null-Ziele 2025 aufgrund von politischem und wirtschaftlichem Druck hinausgezögert oder ihre Richtlinien in Bezug auf Vielfalt, Gleichberechtigung und Integration als Reaktion darauf geändert haben. Diese Vorwürfe werden mit großer Wahrscheinlichkeit auch 2026 weiter bestehen – und sicherlich noch zunehmen. Dabei nutzen Aktivistengruppen verstärkt innovative und störende Maßnahmen, um ihre Ziele zu erreichen. Sie konzentrieren sich insbesondere auf Unternehmen – und Personen –, von denen sie annehmen, dass sie frühere ESG-Verpflichtungen zurücknehmen.

- Gruppen, die sich für die Umwelt, gegen Krieg und für soziale Gerechtigkeit einsetzen, werden wahrscheinlich zu Boykotten, Kapitalentzug und Sanktionen übergehen bzw. dazu aufrufen. Sie richten sich dabei gegen Unternehmen, die in ihren Augen keine deutliche Haltung zu ESG-Themen einnehmen.
- Unternehmen, die von solchen Maßnahmen betroffen sind, laufen Gefahr, in einem polarisierten Arbeitsumfeld zu operieren. Das schafft Bedingungen, die interne Bedrohungsakteure dazu motivieren können, Kampagnen zu organisieren, interne Dokumente weiterzugeben oder Missstände zu enthüllen.
- Es ist unwahrscheinlich, dass Unternehmen ihre ESG-Verpflichtungen in aller Stille verringern können, ohne dass Aktivistengruppen dies aufdecken. Externer Druck von Aktionären, politischen Entscheidungsträgern und Investoren wird Unternehmen wahrscheinlich dazu bringen, frühere ESG-Initiativen zurückzustufen oder ganz aufzugeben. Dadurch laufen sie jedoch Gefahr, weiter ins Visier genommen zu werden.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Weniger Angriffe auf Unternehmen, die ihre ESG-Verpflichtungen hinauszögern oder zurückstufen, da andere Anliegen Vorrang für Aktivistengruppen haben.	Verbesserung	Sehr unwahrscheinlich (10 %)
Unternehmen, die ESG-Verpflichtungen zurückstufen, werden weiterhin ins Visier genommen, da Aktivisten anhand von Open-Source-Daten diese Unternehmen ermitteln und die sozialen Medien nutzen, um Kampagnen und Proteste mit Boykotten, Kapitalentzug und Sanktionen zu organisieren.	Baseline	Wahrscheinlich (60 %)
Aktivistengruppen sehen in den bestehenden Ansätzen keine ausreichenden Fortschritte und gehen zu härteren Maßnahmen über, darunter Vandalismus, Besetzungen oder Bedrohung der Sicherheit von Führungskräften des Unternehmens, um Druck auszuüben.	Verschlechterung	Unwahrscheinlich (30 %)

Handlungsempfehlungen

- Bedenken Sie die Risiken, die mit öffentlichen oder offiziellen Erklärungen zu kontroversen Themen verbunden sind. Damit könnten Sie die Aufmerksamkeit engagierterer Bedrohungsakteure erregen, die wahrscheinlicher zu feindseligen oder störenden Aktionen bereit sind.
- Beobachten und bewerten Sie die Stimmung in der Belegschaft nach Ankündigungen und Mitteilungen zu ESG-Themen oder ähnlich emotionalen oder kontroversen Themen, um frühzeitige Anzeichen für Unzufriedenheit bzw. potenzielle Bedrohungen durch Insider zu erkennen.
- Ermitteln und überwachen Sie Bedrohungsakteure, die aufgrund von geplanten organisatorischen Maßnahmen und Initiativen (direkt oder indirekt) zu feindseligen Handlungen angestiftet, beeinflusst oder inspiriert werden können.

Indikatoren	Auswirkungen
— Politische Entscheidungsträger auf nationaler Ebene üben weiterhin Druck auf Unternehmen aus, ESG-Initiativen zurückzunehmen oder aufzugeben. — Aktivistengruppen weiten ihre Ziele auf sekundäre und tertiäre Einrichtungen von Unternehmen aus, denen vorgeworfen wird, ESG-Initiativen nicht vorrangig zu behandeln (z. B. Partner in der Lieferkette, Versicherer usw.). — Aktivisten konzentrieren sich verstärkt auf Einzelpersonen (CEOs, Führungskräfte) und nicht mehr auf das gesamte Unternehmen. — Etablierte Aktivistengruppen kündigen neue Kampagnen (oder die Ausweitung bestehender Kampagnen) an, die sich gegen die Rücknahme von ESG-Verpflichtungen richten.	— Unternehmen müssen den externen Druck von Interessengruppen und politischen Entscheidungsträgern gegen den externen (und internen) Druck von Aktivistengruppen abwägen, wenn sie Änderungen ihrer Grundsätze kommunizieren. — Es entstehen erhöhte Kosten für die physische Sicherheit von Führungskräften und Standorten (einschließlich Veranstaltungen wie Hauptversammlungen) in Zeiten erheblicher Kritik. — Partner der Unternehmen (z. B. Wohltätigkeits-/gemeinnützige Organisationen usw.) können ESG-Rückschritte negativ wahrnehmen. Dies kann zu öffentlicher Kritik oder zur Beendigung von Partnerschaften führen. — Anhaltende Angriffe von Aktivisten bzw. negative Informationen über Unternehmen können das Vertrauen der Verbraucher und des Marktes beeinträchtigen und zu Einnahmenverlusten der Unternehmen führen.

Massenentlassungen aufgrund von KI verstärken unternehmensfeindliche Stimmung und erhöhen Insiderrisiken

Umstrukturierungen und Massenentlassungen aufgrund von KI werden voraussichtlich auch 2026 andauern, da Unternehmen den Übergang zur Automatisierung, den Einsatz generativer KI (GenAI) und den Ausbau von Rechenzentren vertiefen und gleichzeitig Überkapazitäten beim Personal aus der Pandemiezeit korrigieren. Diese Kürzungen werden wahrscheinlich die unternehmensfeindliche Stimmung verstärken, Risiken für Insider-Aktionen erhöhen und Maßnahmen von KI-Gegnern und Arbeitnehmerrechtsnetzwerken anheizen. Diese Bedingungen führen zu einer erhöhten Verwundbarkeit bei einer ohnehin fragilen Arbeitnehmerstimmung, während Aktivistennetzwerke zunehmend Widerstand gegen die schnelle Einführung von KI organisieren.

- Der KI-bedingte Personalabbau, vor allem in den Bereichen Technik, Fertigung, Kundendienst und Logistik, erhöht die Risiken für Insider-Aktionen wie Datendiebstahl, Sabotage und Missbrauch von KI-Tools. Dabei werden die Taktiken zunehmend ausgeklügelter und stellen eine wachsende Bedrohung für die finanzielle und rechtliche Stabilität sowie für den guten Ruf von Unternehmen dar, während KI-Gegner und Arbeitnehmerrechtsnetzwerke den Druck durch Online-Kampagnen und Streiks verstärken dürften.
- Punktuelle Insider-Vorfälle sind realistisch, während groß angelegte Unruhen unwahrscheinlich sind. Allerdings sind erhebliche betriebliche Auswirkungen auf Rechenzentren, digitale Dienste und automatisierte Produktionsumgebungen durch breitere Aktionen gegen KI (einschließlich insiderfremder Aktionen) möglich.
- Die Sabotage durch Insider in KI-gestützten Umgebungen kann zu unternehmens- und branchenweiten Störungen führen, während die zunehmende Komplexität der Strategien und Taktiken der Aktivistengruppen sowie steigende Risiken von Insider-Aktionen eine erhöhte Bedrohung für die betriebliche Stabilität in Branchen darstellen, die einen raschen KI-gestützten Wandel durchlaufen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
KI-bedingte Entlassungen lassen nach, da sich die Personalplanung stabilisiert, wodurch das Insider-Risiko sinkt und die unternehmensfeindliche Stimmung abnimmt.	Verbesserung	Sehr unwahrscheinlich (10 %)
Die KI-bedingte Umstrukturierung setzt sich weiterhin in einem moderaten Tempo fort, wobei ein mäßiges Insider-Risiko, anhaltende Kritik im Internet und punktueller Druck durch Aktivisten bestehen bleiben.	Baseline	Realistische Möglichkeit (50 %)
Sichtbare oder wiederholte Entlassungen verstärken die unternehmensfeindliche Stimmung, was zu einer Zunahme von Insider-Vorfällen und koordinierten Kampagnen durch Aktivistengruppen führt, die auf die Vermögenswerte und den Ruf von Unternehmen abzielen.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

- Sorgen Sie für eine gute Sicherheitslage durch verstärkte Überwachung von Insider-Bedrohungen, Verschärfung der Zugangskontrollen und Erhöhung der Sichtbarkeit von KI-fähigen Systemen, um Missbrauch oder Sabotage bei Unzufriedenheiten in der Belegschaft zu verringern.
- Treten Sie in regelmäßigen Austausch mit Behörden und Aufsichtsbehörden, um aktuelle Richtlinien zu erhalten und Präventivmaßnahmen zu koordinieren, damit Einrichtungen, Rechenzentren und automatisierte Umgebungen vor neuen Bedrohungen geschützt sind.
- Stärken Sie die Widerstandsfähigkeit des Betriebs und der Lieferkette durch die Ermittlung kritischer Abhängigkeiten, die Überprüfung von Notfallplänen und die Vorbereitung von Alternativen zur Milderung von Störungen durch Insider-Aktionen oder Eingriffe von Aktivisten.

Indikatoren	Auswirkungen
— Zunehmender KI-bedingter Abbau von Stellen in den Bereichen Technologie, Fertigung und Dienstleistungen in Regionen mit fortgeschrittener Automatisierung. — Immer mehr Unternehmen setzen sich öffentlich für den Einsatz von KI-Tools für Aufgaben ein, die zuvor von ihren Mitarbeitenden ausgeführt wurden. — Es kommt verstärkt zu öffentlichen, politischen und aktivistischen Kommentaren, die die rasche Einführung von KI kritisieren, wobei organisierte Arbeitnehmergruppen Kampagnen gegen die Automatisierungsstrategien von Unternehmen koordinieren. — Zunehmende Insider-Risiken wie Datendiebstahl, Zugangsmissbrauch oder Sabotage im Zusammenhang mit entlassenen oder unzufriedenen Mitarbeitenden.	— Erhöhte Sicherheitsanforderungen und -kosten, insbesondere für die Überwachung von Insider-Bedrohungen, Zugangskontrollen und den Schutz von KI-gestützter Infrastruktur. — Höhere Wahrscheinlichkeit von Betriebsunterbrechungen, einschließlich Ausfällen von Rechenzentren, Unterbrechungen der Versorgungskette aufgrund von Sabotageakten durch Insider oder externe Aktivisten oder Störungen in automatisierten Produktionsumgebungen. — Erhöhte regulatorische und Reputationsrisiken, sodass Unternehmen mehr auf die Auswirkungen auf die Mitarbeitenden und die öffentliche Kommunikation im Zusammenhang mit der Einführung von KI achten.

Zunehmend protektionistische Maßnahmen zur Sicherung der Unabhängigkeit von Ländern

Der zunehmende Protektionismus, angetrieben durch eskalierende geopolitische Spannungen, nationale Sicherheitserwägungen und Souveränitätsziele, hat die Marktvolatilität erhöht und die wirtschaftliche Unsicherheit für Unternehmen im Jahr 2025 vergrößert. Es wird erwartet, dass sich dieser Trend 2026 fortsetzen wird, da Regierungen den Handel zunehmend als politisches Druckmittel einsetzen und die Produktion/Dienstleistungserbringung im Inland zur Stärkung der nationalen Sicherheit und Widerstandsfähigkeit einführen.

— Angesichts der anhaltenden geo- und sozialpolitischen Spannungen werden die führenden Politiker der Welt wahrscheinlich weiterhin protektionistische Maßnahmen ergreifen. Dieser Ansatz wird wahrscheinlich bestehende Probleme wie Schwachstellen in der Lieferkette, Handelsabkommen, die als Verhandlungstaktik eingesetzt werden, und Embargos/Zölle auf wichtige Ressourcen weiter verschärfen.

— Die langfristigen Auswirkungen dieses weit verbreiteten Protektionismus können zu einer Änderung der Unternehmensstrategie führen, da der grenzüberschreitende Handel schwieriger bzw. kostspieliger wird. Das kann dazu führen, dass Unternehmen nach Lösungen im eigenen Land suchen, was die globalen Handelsbeziehungen weiter verschlechtert und Lieferketten, die sich daran anpassen, neuen Bedrohungen aussetzt.

— Die Verlagerung von Industrien, die für die Erhaltung der Verteidigungsfähigkeit und die Aufrechterhaltung kritischer nationaler Infrastrukturen von wesentlicher Bedeutung sind, wird wahrscheinlich auch in Zukunft im Fokus protektionistischer Maßnahmen stehen. Das wiederum kann jedoch die Kosten in die Höhe treiben und Komplikationen für Unternehmen mit sich bringen, die sich aus raschen Verschiebungen von Angebot und Nachfrage ergeben.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Geopolitische und gesellschaftspolitische Spannungen lassen nach, was die Volatilität der Märkte verringert. Der grenzüberschreitende Handel stabilisiert sich und die Anwendung von Zöllen und Embargos geht zurück.	Verbesserung	Sehr unwahrscheinlich (15 %)
Politiker führen weiterhin sporadisch protektionistische Maßnahmen durch, die Unternehmen zwingen, ihre Geschäftstätigkeit ständig anzupassen und ihre Handelsbeziehungen neu zu bewerten. Dies führt zu Unsicherheiten.	Baseline	Wahrscheinlich (55 %)
Der Handel wird zunehmend als politisches Druckmittel eingesetzt, was zu einer unkontrollierbaren Unsicherheit auf den globalen Märkten führt. Die Lieferketten sind aufgrund der sich rasch ändernden Handelsbedingungen erheblichen Störungen ausgesetzt.	Verschlechterung	Unwahrscheinlich (30 %)

Handlungsempfehlungen

— Stellen Sie sicher, dass alle betrieblichen Bereiche Änderungen von Vorschriften umsetzen können, und erstellen Sie realistische Notfallpläne für den Fall, dass sich protektionistische Maßnahmen auf die betriebliche Leistungsfähigkeit oder Kapazität auswirken.

— Führen Sie solide Sicherheitsverfahren für Lieferketten und Lagerbestände ein, damit Bedrohungsakteure Schwachstellen in der Übergangszeit nach der Ankündigung solcher Maßnahmen nicht ausnutzen können.

— Arbeiten Sie mit internationalen Partnern bei der Erstellung von Notfallplänen zusammen, die trotz Unsicherheiten einen unterbrechungsfreien Betrieb ermöglichen.

Indikatoren	Auswirkungen
— Regionaler Anstieg des nationalistischen Populismus, der gegen die Globalisierung der Wirtschaft eintritt. — Häufigere Kündigung von Verträgen unter Berufung auf Sicherheitsbedenken. — Umstrittenes Verhalten von Bereichen/Unternehmen, an denen andere Länder nicht beteiligt sein wollen. — Globale Krisenherde, die politische Verhandlungen erfordern. — Zunehmende protektionistische Maßnahmen von Wirtschaftsverbündeten, die zu Vergeltungsmaßnahmen führen. — Zunehmende Besorgnis hinsichtlich Datenzugriff und Spionage durch importierte Waren.	— Verschlechterung der grenzüberschreitenden Zusammenarbeit, wodurch Innovationen und Entwicklungen in den betreffenden Branchen behindert werden. — Importe/Exporte werden zunehmend von Bedrohungsakteuren ausgenutzt, die sowohl Cyber- als auch physische Aspekte kombinieren, um unentdeckt zu bleiben. — Anhaltende Unsicherheit hinsichtlich Gewinnen, Angebot/Nachfrage und Regulierungsnormen. — Erheblicher Rückgang der ausländischen Direktinvestitionen. — Weitreichendere finanzielle und betriebliche Folgen für Tochtergesellschaften, Investoren und Drittanbieter, da die Erwartungen an die Politik angepasst werden.

Bedrohungsakteure nutzen anfällige öffentliche und private Veranstaltungen aus

Bedrohungsakteure haben in den letzten Jahren zunehmend Großveranstaltungen ins Visier genommen, da sie leicht zugänglich sind, die Anwesenheit von hochrangigen Zielpersonen wahrscheinlich ist und die Möglichkeit besteht, die Aktionen in den sozialen Medien bekannt zu machen und zu verbreiten. Anhaltende geopolitische Spannungen und kontroverse gesellschaftspolitische Themen wie Umweltschutz und die Entwicklung künstlicher Intelligenz werden auch 2026 wichtige Faktoren für Aktivismus und Insider-Bedrohungen sein. Neben den bestehenden Taktiken, Techniken und Prozeduren werden die Bedrohungsakteure ihre Handlungen mit Sicherheit um innovative Methoden ergänzen, z. B. durch Ausnutzung erhöhter Besorgnis, um gefälschte Drohungen zu versenden und Störungen zu verursachen.

- Während Aktivistengruppen schon seit Jahren gezielt Veranstaltungen ins Visier nehmen, bei denen Vertreter von Unternehmen anwesend sind, ist es immer wahrscheinlicher, dass auch andere Bedrohungsakteure diese Taktik übernehmen, um in einem weniger kontrollierten Umfeld Zugang zu wichtigen Personen oder Vermögenswerten zu erhalten.
- Die Teilnahme großer Unternehmen an Veranstaltungen birgt die Gefahr, dass sensible Informationen ausspioniert werden, die später zur Rufschädigung, Erpressung oder zum Verkauf an konkurrierende Unternehmen genutzt werden könnten.
- Bedrohungsakteure werden dabei immer findiger und werden wahrscheinlich mehrere Datenquellen nutzen, um Informationen über ihr Ziel zu sammeln, z. B. Hotels in der Nähe von Veranstaltungen, in denen sich Zielpersonen potentiell aufhalten können, oder mögliche Beförderungsrouten zu und von Veranstaltungen. Mit diesen Informationen können dann Aktionen durchgeführt werden, die mit dem Ereignis in Verbindung stehen, aber nicht währenddessen ausgeführt werden.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Verbesserte Sicherheitsvorkehrungen für Veranstaltungen und hochrangige Zielpersonen veranlassen Bedrohungsakteure dazu, andere Wege für ihre Angriffe zu verfolgen, da die Erfolgsaussichten bei Veranstaltungen geringer sind. Weniger Unterbrechungen von Veranstaltungen durch Angriffe von Bedrohungsakteuren.	Verbesserung	Sehr unwahrscheinlich (10 %)
Bedrohungsakteure zielen weiterhin auf Veranstaltungen ab und stören sie, wobei sie neue und bestehende Methoden einsetzen. Veranstaltungen werden weiterhin sowohl durch das Eingreifen von Bedrohungsakteuren als auch durch verschärfte Sicherheitsprotokolle gestört bzw. behindert.	Baseline	Wahrscheinlich (60 %)
Bedrohungsakteure erzielen durch gezielte Anschläge auf Veranstaltungen immer wieder Erfolge. Die Wahrnehmung der Erfolge führt zu weiteren Versuchen und verstärkt Störungen. Erhebliche Auswirkungen auch auf Veranstaltungen, die nicht Ziel von Angriffen sind, aufgrund verstärkter Sicherheitsmaßnahmen als Reaktion auf die erhöhte Bedrohungslage.	Verschlechterung	Unwahrscheinlich (30 %)

Handlungsempfehlungen

- Verbessern Sie die operative Sicherheit im Zusammenhang mit der Teilnahme an externen Veranstaltungen durch eingeschränkte Veröffentlichung bestimmter Veranstaltungsdetails (z. B. Teilnehmende). Vermeiden Sie es, Details wie Veranstaltungsausweise oder Akkreditierungen in sozialen Medien zu veröffentlichen.
- Ziehen Sie angemessene Hintergrundüberprüfungen der Teilnehmenden in Betracht, damit Bedrohungsakteure keinen rechtmäßigen Zugang zu Veranstaltungen erhalten.
- Stellen Sie sicher, dass die Sicherheitsvorkehrungen für hochrangige Zielpersonen nicht am Einlass enden. Denken Sie daran, dass Bedrohungsakteure auch außerhalb, in der Nähe oder auf dem Weg zu und von Veranstaltungen Anschläge verüben könnten.

Indikatoren	Auswirkungen
— Konten von Veranstaltungen in sozialen Medien geraten verstärkt ins Visier, basierend auf Personen oder Unternehmen, die an der Veranstaltung teilnehmen. — Zunehmende Berichte über Veranstaltungen, die von nicht-aktivistischen Bedrohungsakteuren besucht bzw. ins Visier genommen werden, z. B. verärgerte Kunden, Kriminelle und Personen mit starken Ideologien. — Eskalation von Taktiken, Techniken und Prozeduren, die von Bedrohungsakteuren zum Stören von Veranstaltungen eingesetzt werden. — Spannungen bei treibenden Faktoren (z. B. geopolitische Konflikte) im Vorfeld oder während der Veranstaltungen. — Boykotte, die sich gegen sekundäre und tertiäre Unternehmen sowie gegen Veranstalter und Hotels richten, in denen die Teilnehmenden untergebracht sind.	— Erhöhte Sicherheitsanforderungen für Gastgebende und Teilnehmende an Veranstaltungen, was zu einer Erhöhung der Sicherheitskosten führt. — Strengere Bewerbungs- und Überprüfungsverfahren für Teilnehmende, die sich auf die Zugänglichkeit für die Öffentlichkeit und externe Unternehmen auswirken und zu Kritik führen könnten. — Unternehmen erwägen zunehmend, Veranstaltungen auf Online-Plattformen zu verlagern, um die Gefahr von Störungen zu minimieren. — Unternehmen möchten hochrangige Führungskräfte aufgrund von Sicherheitsbedenken lieber nicht zu öffentlichen Veranstaltungen schicken.

Nachhaltigkeitsbedenken behindern ressourcenintensive Infrastrukturprojekte

Die Nachfrage nach ressourcenintensiven Infrastrukturprojekten wie Rechenzentren, Generatoren für erneuerbare Energien und Halbleiteranlagen wird 2026 weiter steigen, da Regierungen Projekte aus strategischen und wirtschaftlichen Gründen subventionieren und Unternehmen auf KI-gesteuerte Dienste und Abläufe umstellen. Für solche Projekte werden umfangreiche Ressourcen wie Energie, Wasser, Land und kritische Mineralien benötigt. Dies wiederum verstärkt die Bedenken von Regulierungsbehörden, politischen Entscheidungsträgern und sozioökonomischen Akteuren wie Umweltaktivisten und Arbeitnehmern hinsichtlich der Nachhaltigkeit.

— Dieser Anstieg wird durch das Wettrüsten im Bereich KI/Digitales auf strategischer geopolitischer Ebene und auf Marktebene angetrieben, da Unternehmen ihre KI- und Digitalstrategien zur Steigerung der Wettbewerbsfähigkeit vorantreiben. Das führt zu einer steigenden Nachfrage nach Rechenzentren und Halbleitern und begünstigt den laufenden Wandel hin zu sauberen Energietechnologien wie Elektrofahrzeugen und erneuerbarer Energieerzeugung, für die kritische Mineralien benötigt werden.

— Die Ressourcenintensität dieser Infrastrukturprojekte hat aufgrund der Auswirkungen auf die Wasserversorgung, die Energieressourcen, die Verfügbarkeit von Land und den Müll zu Protesten, Sabotage, Klagen und Untersuchungen durch Aktivisten, Regulierungsbehörden und Regierungen geführt. Darüber hinaus sind sie hochrangige Ziele für staatliche Akteure und Spionage- und Sabotagetaktiken. Diese sind zwar nicht durch Nachhaltigkeitsaspekte motiviert, zeigen aber die Anfälligkeit des Sektors auf.

— Eine weitere Expansion dieser Projekte im Jahr 2026 wird dazu führen, dass der Druck auf Entwickler und Regierungen wächst, strengere Umweltauflagen umzusetzen, Verzögerungen bei den Plänen für den Übergang zu digitaler und künstlicher Intelligenz zu riskieren und die Genehmigungsverfahren für künftige Projekte zu verschärfen, obwohl die ESG-Verpflichtungen weltweit als rückläufig angesehen werden.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Technologische Durchbrüche und veränderte globale Nachfragestrukturen führen zu einer Verringerung ressourcenintensiver Infrastrukturprojekte, sodass sich Nachhaltigkeitsbedenken verringern.	Verbesserung	Sehr unwahrscheinlich (10 %)
Die weltweite Nachfrage nach Infrastrukturen hält an und führt zu einer weiteren Ausweitung von Bauprojekten, die im politischen und öffentlichen Diskurs immer schärfer diskutiert werden.	Baseline	Wahrscheinlich (65 %)
Die Nachfrage wächst deutlich, was zu einer stärkeren Belastung der Ressourcen führt und Störungen in betrieblichen Abläufen, eine polarisierende politische Rhetorik und verstärkten Aktivismus zur Folge hat.	Verschlechterung	Unwahrscheinlich (25 %)

Handlungsempfehlungen

— Bewerten Sie Ihre Beteiligung an ressourcenintensiven Infrastrukturen, insbesondere in Regionen, in denen die Kontroverse um die Belastung von Ressourcen und die Schädigung der Umwelt zunimmt.

— Informieren Sie sich über die Stimmung im Internet in Bezug auf Infrastrukturprojekte und verstärken Sie Ihr Engagement auf lokaler Ebene, um Bedenken hinsichtlich der Nachhaltigkeit auszuräumen. Informieren Sie transparent über den Ressourcenbedarf, den Zeitrahmen von Projekten und den wirtschaftlichen Nutzen.

— Behalten Sie mögliche Änderungen von Vorschriften zur Ressourcennutzung und zu Umweltauswirkungen im Auge, um operative Auswirkungen auf Projektfristen und Unterbrechungen der Lieferkette zu minimieren.

Indikatoren	Auswirkungen
— Verstärkter Bau neuer Rechenzentren, halbleiterbasierter Produkte und Projekte für erneuerbare Energien. — Erhöhte Aufmerksamkeit für Wasserknappheit, Engpässe der Netzkapazität oder Landnutzungskonflikte rund um Projektstandorte, auch in den Nachrichten und sozialen Medien. — Verstärkte Proteste, einschließlich lokaler Kampagnen und Klagen, gegen Projekte und beteiligte Unternehmen. — Zunehmende gerichtliche Stopps oder Blockierung geplanter Infrastrukturprojekte aufgrund von lokalem Widerstand. — Zunehmende Verschwörungstheorien über die Infrastrukturen und Technologien.	— Sorgfältigere Prüfungen führen zu Änderungen von Vorschriften und strengeren Nachhaltigkeitsanforderungen. — Höhere Projektkosten und Verzögerungen bei Infrastrukturprojekten aufgrund strengerer Vorschriften und längerer Genehmigungsverfahren. — Unternehmen, die auf diese Infrastrukturen angewiesen sind, haben mit Lieferengpässen und instabilen Lieferketten zu kämpfen. — Zunahme der Häufigkeit, des Umfangs und der Intensität des Aktivismus gegen Entwickler und damit noch stärkere Verzögerungen. — Erhöhte Bedrohung durch extremistische Aktionen, einschließlich Sabotage und Zerstörungen.

Reaktion der Behörden auf Drohnengefahr fördert weitere Instrumentalisierung

Westliche Behörden zögern noch immer, der Bedrohung durch Drohnen für Verkehrsknotenpunkte, militärische Einrichtungen und andere kritische nationale Infrastrukturen entgegenzutreten, während bei den Drohnen weiter technologische Fortschritte erzielt werden. Dies gibt Bedrohungsakteuren (einschließlich Aktivisten, Terroristen und staatlich unterstützten Personen) auch 2026 Möglichkeiten für Störaktionen. Die Zunahme nicht genehmigter Drohnenaktivitäten über sensiblen Gebieten in den letzten Jahren hat Bedenken hinsichtlich der weitreichenden Auswirkungen auf die betroffenen Einrichtungen zur Folge und zu einer erhöhten Unsicherheit beigetragen. Zudem wird die Fähigkeit von Behörden kritisiert, gegen erkannte hybride Bedrohungen vorzugehen.

- Die kommerzielle Verfügbarkeit und die Fortschritte bei der Leistungsfähigkeit von Drohnen werden die Weiterentwicklung von Taktiken, Techniken und Prozeduren bei deren Einsatz vorantreiben. Bedrohungsakteure, darunter auch kriminelle Organisationen, werden dabei lokal gestartete, entbehrliche Geräte einsetzen, um Wohn-, Freizeit-, Gewerbe- und Industriegebiete anzugreifen.
- Es wird auch weiterhin dazu kommen, dass Drohnen als alternative Protestmöglichkeit eingesetzt werden. Dabei werden Ängste ausgenutzt, um größtmögliche Publicity zu erzielen oder das Bewusstsein zu schärfen sowie Vermögenswerte aufzuzeichnen, Behauptungen untermauern und kritischen Narrativen Glaubwürdigkeit zu verleihen.
- Die Auswirkungen von Betriebsstörungen aufgrund verdächtiger Drohnensichtungen in der Nähe von kritischen Infrastrukturen und Transportknotenpunkten werden wahrscheinlich weiterhin von feindlichen Ländern, die eine hybride oder Grauzonen-Kriegsführung anstreben, ausgenutzt und als Waffe eingesetzt.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Flächendeckender Einsatz von Spezialausrüstung zur Drohnenabwehr sowie Bestimmungen, die sicherstellen, dass die betroffenen Parteien die Befugnis/Fähigkeit haben, Drohnen sicher abzufangen. Behörden führen klare Einsatzregeln für verdächtige Aktivitäten von Drohnen ein.	Verbesserung	Sehr unwahrscheinlich (10 %)
Gegner nutzen weiterhin die zögerliche Vorgehensweise aus und testen die Fähigkeiten zur Erkennung von und Reaktion auf Drohnen, hinzu kommen Verpflichtungen aus gemeinsamen Verteidigungsabkommen, die Einsatzgrenzen beeinflussen.	Baseline	Sehr wahrscheinlich (80 %)
Eskalation durch einen (versehentlichen oder absichtlichen) Zusammenstoß mit einer Drohne. Gelingt es nicht, wirksame Abschreckungsmaßnahmen zu ergreifen, werden die Angriffe von Drohnen auf kritische Infrastrukturen und Verkehrsknotenpunkte zunehmen, und die Lahmlegung von Systemen führt zu einem verstärkten Einsatz durch feindliche Akteure.	Verschlechterung	Sehr unwahrscheinlich (10 %)

Handlungsempfehlungen

- Überprüfen Sie Schwachstellen bei der Luftaufklärung, um sicherzustellen, dass Verfahren für das Eindringen in den Luftraum über Betriebsstandorten umgesetzt werden und geheime Anlagen nicht sichtbar sind.
- Informieren Sie sich über Vorschriften zu Luftraumbeschränkungen über Grundstücken und stellen Sie sicher, dass die Mitarbeitenden (einschließlich Security-Auditoren) im Umgang mit Situationen im Zusammenhang mit Einsätzen von Drohnen geschult und ausgerüstet sind.
- Behalten Sie online verfügbares Bildmaterial im Auge, das die Grenzen des Geländes bzw. die Sicherheitsmaßnahmen vor Ort zeigt und damit Informationen für feindliche Aktivitäten, weitere Aufklärungsmaßnahmen bzw. Proteste oder direkte Aktionen liefert.

Indikatoren	Auswirkungen
— Vermehrter Einsatz von Drohnen zur Feindaufklärung, um Informationen für gezielte Aktionen zu erhalten. — Erhöhte Verfügbarkeit und Zugang zu Drohnentechnologie, insbesondere zu billigen oder „Wegwerf“-Geräten. — Ein erhöhtes Bewusstsein und die weitere Eskalation tragen dazu bei, dass vermehrt verdächtige Drohnenaktivitäten gemeldet werden, die feindlichen Ländern zugeschrieben werden, sodass ein erhöhter Bedarf an Drohnenerkennungssystemen besteht. — Anhaltende Kontroversen rund um Bestimmungen für militärische Behörden zur Bekämpfung von Drohnenbedrohungen, insbesondere in der Nähe sensibler Standorte, die an zivile Bauwerke in städtischen Gebieten grenzen.	— Anhaltendes Risiko von Luftraumsperrungen aufgrund verdächtiger Drohnenaktivitäten, wobei Akteure ohne bösen Vorsatz aufgrund gestiegener Ängste unbeabsichtigt Störungen verursachen. — Wachsende Aufmerksamkeit für kommerzielle Drohnenerkennungssysteme, insbesondere für Technologien, die von Unternehmen mit Sitz in Staaten entwickelt wurden, die von westlichen Regierungen als feindlich angesehen werden. — Erhöhte Nachfrage nach Investitionen in die Drohnenabwehr zum Schutz kritischer Offshore-Anlagen/Transitwege. — Online-Enthüllungen eingesetzter Sicherheitsmaßnahmen, die möglicherweise von anderen Bedrohungsakteuren ausgenutzt werden.

Risiken für Unternehmen durch zunehmende Abhängigkeit von Cloud-Umgebungen

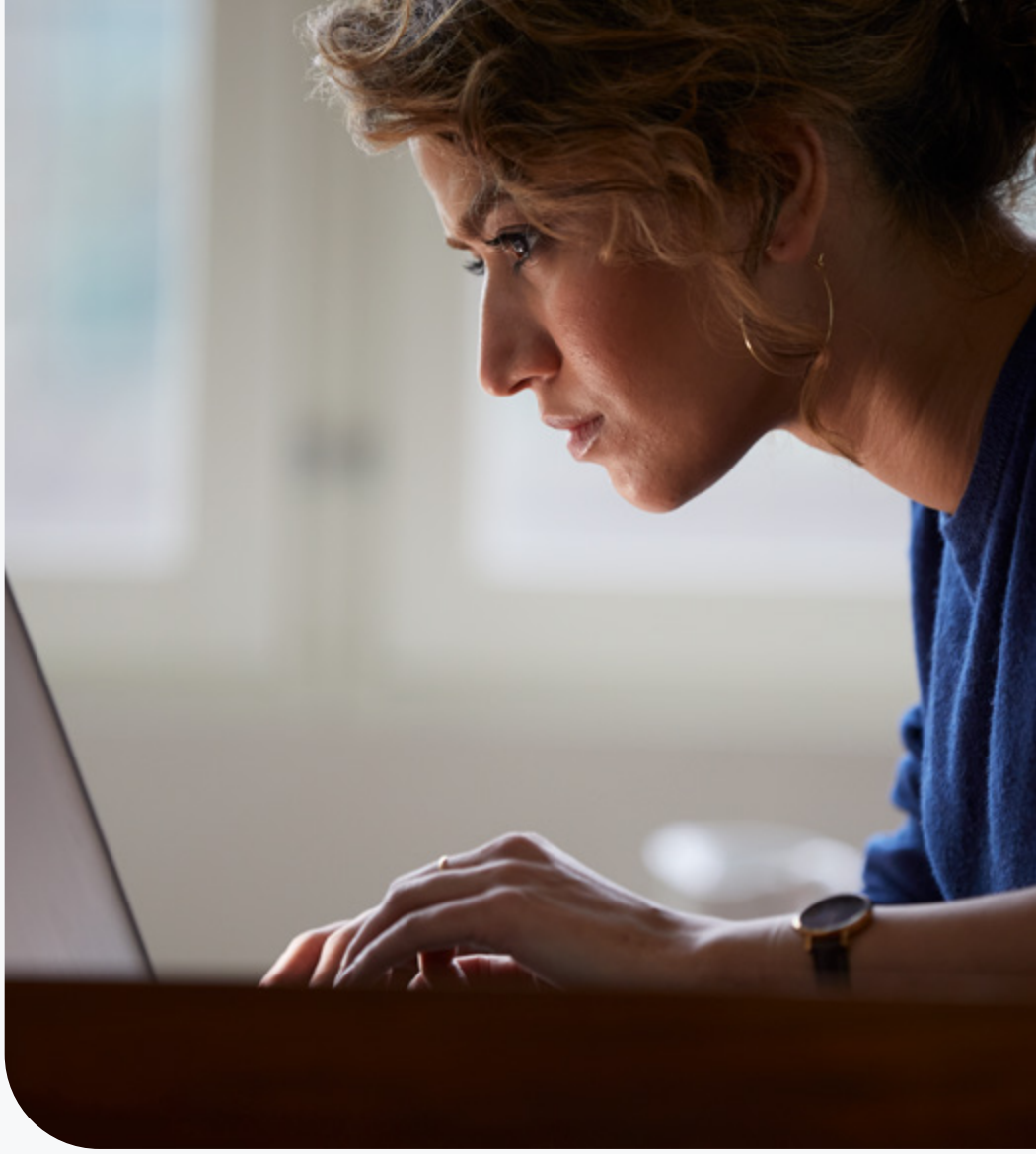
Die Cyberbedrohungen für Unternehmen werden zunehmen, da immer mehr Unternehmen ihren Betrieb auf cloud-basierte Software-as-a-Service-Modelle (SaaS) umstellen und damit den mit Cloud-Diensten verbundenen Bedrohungen wie Ausfällen, Datenschutzverletzungen und Fehlkonfigurationen stärker ausgesetzt sind. Die digitale Infrastruktur wird von großen Cloud-Anbietern wie Amazon Web Services, Microsoft Azure und Google dominiert, aber Unternehmen nutzen oft mehrere Plattformen. Dies erhöht ihre Anfälligkeit für digitale Risiken, insbesondere wenn Unternehmen hybrides Arbeiten und KI in ihre Abläufe integrieren.

- GenAI wird die Bedrohung durch den Diebstahl von Anmeldedaten und Phishing erhöhen, da sie diese Methoden durch Automatisierung zugänglicher und wirksamer macht und die technische Schwelle für durchführbare Angriffe senkt.
- Cloud-basierte digitale Infrastrukturen begünstigen diese Art von Angriffen, da Kriminelle menschliche Fehler ausnutzen können, indem sie schnell agieren. Dies erschwert die Erkennung und Verhinderung und macht große Mengen sensibler, unverschlüsselter Daten angreifbar.
- Die rasche Migration von Unternehmen zu mehreren SaaS-Anbietern wird weiterhin zu erheblichen Schwachstellen im Bereich des Identitäts- und Zugriffsmanagements führen, wodurch Cyber- und Insider-Bedrohungen zunehmen.
- Cloud-Ausfälle werden weiterhin sporadisch auftreten, den Unternehmensbetrieb erheblich stören und die Wahrscheinlichkeit von Angriffen erhöhen, mit denen diese Ausfälle ausgenutzt werden.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Unternehmen erkennen die wachsende Bedrohung und investieren ausreichend in die Cloud-Sicherheit, um die Gefahr von Datenschutzverletzungen zu verringern. Lieferanten verbessern die Sicherheit und die technische Ausfallsicherheit, um Vorfälle abzumildern und zu vermeiden.	Verbesserung	Sehr unwahrscheinlich (15 %)
Unternehmen migrieren weiterhin zu cloud-basierten SaaS-Anbietern, was die globalen Auswirkungen von Sicherheitsvorfällen und -ausfällen verstärkt und zu immer größeren Datenschutzverletzungen und Cyberbedrohungen führt.	Baseline	Wahrscheinlich (70 %)
Probleme mit Cloud-Anbietern treten immer häufiger auf und verursachen u. a. umfangreiche Datenverluste. Unternehmen sind gezwungen, ihren Betrieb von cloud-basierten Systemen zu trennen.	Verschlechterung	Sehr unwahrscheinlich (15 %)

Handlungsempfehlungen

- Stellen Sie sicher, dass alle Mitarbeitenden sowie Dritte/Anbieter über Datenschutz- und Cybersicherheitsverfahren und -praktiken informiert und auf dem neuesten Stand sind, z. B. starke Passwörter und die Identifizierung und Überprüfung von Anfragen zu Anmeldeinformationen.
- Schulen Sie Mitarbeitende in der Erkennung von KI-gesteuerten Imitationstaktiken, wie z. B. Deepfake-Anrufe, Phishing-/Vishing-Versuche.
- Investieren Sie in moderne, automatisierte Cloud-Sicherheitstools, wie Cloud Security Posture Management und Multi-Faktor-Authentifizierung.
- Stellen Sie sicher, dass Notfallpläne und betriebliche Ausfallsicherungen vorhanden sind, um Unterbrechungen bei Cloud-Ausfällen zu minimieren.



Indikatoren	Auswirkungen
— Unternehmen beschleunigen die Umstellung auf mehrere SaaS-Cloud-Systeme. — Cloud-Ausfälle und Datenschutzverletzungen treten immer häufiger auf, was zu Störungen in mehreren Sektoren führt und opportunistische Angriffe erleichtert. — Zunehmende Bestrebungen von Behörden und Regierungen, robustere Sicherheits- und technische Maßnahmen zu erlassen, um die Kontinuität der Bereitstellung und den Schutz von Daten innerhalb von Cloud-Diensten zu gewährleisten, einschließlich erheblicher rechtlicher und finanzieller Auswirkungen bei Nichtbeachtung. — Größere Angriffe, Ausfälle oder Datenschutzverletzungen führen zu einer Verunsicherung in der Branche hinsichtlich einer übermäßigen Migration zu Cloud-Diensten.	— Cloud-Ausfälle führen zu erheblichen Unterbrechungen des Geschäftsbetriebs in verschiedenen Sektoren, einschließlich Behörden und kritischer nationaler Infrastruktur. — Unternehmen sind ständig Datenschutzverletzungen und dadurch entstehenden Datenlecks ausgesetzt, was zu erheblichen Rechtskosten, Rufschädigung und möglichen Geschäftseinbußen führen kann. — Die Nichteinhaltung gesetzlicher Vorschriften, z. B. im Bereich Datenschutz, birgt für Unternehmen finanzielle und Reputationsrisiken. — Unternehmen müssen ihr Sicherheitsbudget überdenken, um die zunehmende Cyberbedrohung und die damit verbundenen Folgen abzumildern.

Bedrohung der Informationslandschaft durch aufkommende GenAI

Die Möglichkeiten der künstlichen Intelligenz schreiten schneller voran als die Fähigkeit der Menschen, authentische Inhalte von Fälschungen zu unterscheiden. Die technologischen Fortschritte tragen wahrscheinlich zu einer weiteren Untergrabung des Vertrauens in Institutionen bei und schaffen Bedingungen, unter denen Unternehmen greifbaren und störenden Bedrohungen durch Reputationsangriffe, Marktmanipulationen und Betriebsunterbrechungen ausgesetzt sind. Die Informationslandschaft zersplittert weiter, da die traditionellen Medien an Glaubwürdigkeit verlieren, während der Einfluss ungeprüfter alternativer Quellen im Mainstream weiter zunimmt.

— Das Vertrauen in und die Arbeit mit althergebrachten Medieninstitutionen hat einen historischen Tiefstand erreicht. Dieses Vakuum wird zunehmend von Influencern, Möchtegern-Journalisten ohne redaktionelle Aufsicht und alternativen Medien gefüllt, von denen viele ein größeres Publikum als die etablierten Zeitungen erreichen und Interaktion über Verifikation stellen.

— Staatliche und nichtstaatliche Akteure verfügen über modernste Fähigkeiten im Bereich GenAI und haben bereits gezeigt, dass sie Informationsumgebungen manipulieren wollen. Alternative Medienumgebungen auf Plattformen wie Telegram, X und neu entstehenden dezentralen Netzwerken werden wahrscheinlich als primäre Vertriebskanäle dienen.

— Tools zum Klonen von Stimmen, zum Austauschen von Gesichtern und zur Texterstellung ermöglichen es jedem motivierten Akteur, innerhalb weniger Stunden überzeugende künstliche Inhalte von Führungskräften, Beamten oder Personen des öffentlichen Lebens zu erstellen. Unternehmen werden 2026 und darüber hinaus wahrscheinlich regelmäßig Angriffen über künstliche Medien ausgesetzt sein, die u. a. darauf abzielen, den Betrieb zu stören oder sensible Informationen zu erlangen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die Technologie zur Erkennung von KI hält mit den KI-Fähigkeiten Schritt und beschränkt die Wirkung künstlicher Inhalte. Außerdem schaffen die Richtlinien der Plattformen wirksame Barrieren, da die angesprochenen Zielgruppen durch gestiegene Medienkompetenz bessere Prüfgewohnheiten entwickelt.	Verbesserung	Sehr unwahrscheinlich (20 %)
Angriffe durch künstliche Medien nehmen deutlich zu, bleiben jedoch kontrollierbar, wobei die Erkennung nur schwer mit der Qualität der generierten Inhalte mithalten kann, aber dennoch einen gewissen Schutz bietet. Allerdings sorgen immer wieder öffentlichkeitswirksame Unternehmensvorfälle für Störungen.	Baseline	Realistische Möglichkeit (40 %)
Künstliche Inhalte überfordern die Erkennungs- und Überprüfungssysteme, und das Vertrauen der Öffentlichkeit schwindet weiter. Angriffe auf Unternehmen werden durch generierte Inhalte erleichtert und nehmen sowohl an Häufigkeit als auch an Wirksamkeit zu.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

— Richten Sie mehrstufige Authentifizierungen für die Kommunikation von Führungskräften ein, darunter auch verifizierte Kanäle, von denen die Interessengruppen wissen, dass sie im Krisenfall vertrauenswürdig sind. Richten Sie Codewort-Systeme für sensible Mitteilungen ein, die nicht durch Fälschungen nachgeahmt werden können.

— Entwickeln Sie Tools zur Überwachung sozialer und alternativer Medien im Hinblick auf die Erwähnung von Marken und Führungskräften und legen Sie Verfahren zur Identifizierung, Meldung und Entfernung von generierten Inhalten fest.

— Setzen Sie Führungskräfte keinen unkontrollierten Umgebungen aus, die wahrscheinlich hochwertiges Quellmaterial für Deepfakes liefern können. Prüfen Sie öffentliche Auftritte und Rednerverpflichtungen auf Aufzeichnungskontrollen.

Indikatoren	Auswirkungen
— Zunehmende Verbreitung und Zugang zu Tools für die Mediengestaltung mit GenAI. — Ersteller alternativer Medien erreichen ein größeres Publikum als die traditionellen Nachrichtenkanäle, und die Algorithmen der Plattformen bevorzugen Inhalte von Möchtegern-Journalisten und Influencern gegenüber herkömmlichen Medien. — Unternehmenskrisen haben ihren Ursprung zunehmend in alternativen Quellen und nicht in der traditionellen Berichterstattung. Die Überprüfungsstandards sinken und künstliche Medien verbreiten sich schnell, bevor sie entlarvt werden. — Gruppen von Bedrohungsakteuren nutzen zunehmend GenAI, um Falschinformationen zu verbreiten, feindliche Aktionen zu ermöglichen und den Ruf von Unternehmen anzugreifen.	— Das Vertrauen und die Moral der Mitarbeitenden leiden, wenn künstlich erstellte Inhalte in der internen Kommunikation verwendet werden. Unzufriedene Mitarbeitende vervielfältigen oder erstellen selbst künstliche Medien, um ihr eigenes Unternehmen anzugreifen. — Bedrohungen durch Insider nehmen zu, da Mitarbeitende Mitteilungen von Führungskräften nicht auf Echtheit prüfen können. — Verschwörungstheorien und Fälschungen untergraben das Vertrauen der Öffentlichkeit und der Wirtschaft. — Künstlich erzeugte Medienkampagnen zielen auf Partner in der Lieferkette ab und verbreiten falsche Behauptungen über Qualität, Sicherheit oder Geschäftspraktiken. B2B-Beziehungen leiden, wenn die Authentifizierung der Kommunikation von Partnern nicht verlässlich ist.

Zunehmende Instrumentalisierung der sozialen Medien zur Erleichterung von Massen-Doxxing-Kampagnen

Die Nutzung sozialer Medien zur Unterstützung von Fehlinformations- und Desinformationskampagnen hat im Jahr 2025 erheblich zugenommen. Dies liegt daran, dass die Geschwindigkeit und das Ausmaß, in dem Narrative erstellt, vervielfältigt und als Waffe eingesetzt werden können, durch Verbesserungen der GenAI-Technologien möglich geworden sind. Diese rasche Vervielfältigung kann auch zu gezieltem Doxxing führen, da falsche oder hetzerische Inhalte als Rechtfertigung für die Veröffentlichung von personenbezogenen Daten einer Person in den sozialen Medien und als Aufruf zum Mobbing verwendet werden.

- KI-Tools (einschließlich frei zugänglicher großer Sprachmodelle wie ChatGPT, Gemini und Grok) können für die Suche nach personenbezogenen Informationen zu Zielpersonen eingesetzt werden und können, wenn keine Datenschutzmaßnahmen ergriffen – oder diese umgangen – werden, möglicherweise Einzelheiten wie Kontaktnummern, Familiennamen und Wohnadressen liefern.
- Die Nachwirkungen der Ermordung von Charlie Kirk machen deutlich, dass die sozialen Medien zunehmend zur Identifizierung von Zielen für Vergeltungsmaßnahmen wie koordiniertes Mobbing, Doxxing und Einschüchterung in der realen Welt durch Akteure genutzt werden, die versuchen, eine aufgeheizte öffentliche Stimmung auszunutzen.
- Die anhaltende sozio-politische Polarisierung und die Zunahme der tatsächlichen oder wahrgenommenen wirtschaftlichen Unsicherheit werden wahrscheinlich zu wachsender Unzufriedenheit und negativen Gefühlen gegenüber bestimmten Unternehmen führen. Dies wird höchstwahrscheinlich dazu führen, dass CEOs und leitende Angestellte als öffentliches Gesicht eines Unternehmens verstärkt ins Visier geraten.
- Unterschiedliche Gesetze zum Schutz der Privatsphäre und des Datenschutzes werden die konsequente Durchsetzung und Regulierung weiterhin erschweren und Regierungen möglicherweise dazu veranlassen, Beschränkungen und Einschränkungen für soziale Netzwerke in Erwägung zu ziehen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Strengere Datenschutzgesetze begrenzen den öffentlichen Zugang zu personenbezogenen Daten und erhöhen die Transparenz von Plattformen bei Moderation und Algorithmen. Zugleich führen schärfere Regelungen und Sanktionen zu einem konsequenteren Vorgehen gegen Online-Mobbing, Belästigung und Doxxing.	Verbesserung	Sehr unwahrscheinlich (20 %)
Bedrohungsakteure nutzen weiterhin soziale Medien aus, um die schnelle Verbreitung personenbezogener Daten von Führungskräften in Organisationen sowie politischen Gegnern zu erleichtern. Dies führt zu erhöhten physischen Sicherheitsrisiken für die betroffenen Personen und zu Störungen innerhalb der Organisationen.	Baseline	Wahrscheinlich (55 %)
Bedrohungsakteure setzen zunehmend soziale Medien ein, um Doxxing-Kampagnen aufgrund wahrgenommener organisationaler Ungerechtigkeiten sowie sozio-politischer Konflikte durchzuführen.	Verschlechterung	Unwahrscheinlich (25 %)

Handlungsempfehlungen

- Stellen Sie sicher, dass regelmäßige Überprüfungen der öffentlich zugänglichen personenbezogenen Daten von Führungskräften des Unternehmens durchgeführt werden, und entfernen Sie alle Daten, die für Angriffe genutzt werden könnten.
- Überwachen Sie die sozialen Medien, um Veränderungen in der Online-Stimmung zu erkennen, die dazu führen könnten, dass Führungskräfte des Unternehmens zur Zielscheibe werden.
- Stellen Sie sicher, dass Pläne für die Reaktion auf Vorfälle vorhanden sind und regelmäßig durchgespielt werden, um Doxxing wirksam zu bekämpfen und die Führungskräfte und Geschäftsstandorte des Unternehmens zu schützen.

Indikatoren	Auswirkungen
— Feststellung, dass Social-Media-Plattformen eine schwache oder uneinheitliche Moderation der Inhalte haben. — Zunehmende Polarisierung in den sozialen Netzwerken, wobei Inhalte auf den Plattformen immer wieder reproduziert werden. — Zunehmender digitaler Aktivismus und Nutzung sozialer Medien für die Durchsetzung „sozialer Gerechtigkeit“. — Allgemeine Zunahme von Belästigungen und Angriffen auf Unternehmen und Einzelpersonen in den sozialen Netzwerken. — Vermehrter Einsatz von Bot-Netzen und durch Algorithmen gesteuerten Systemen zur Darstellung und Verbreitung von Fehl- und Desinformation. — Veröffentlichung von Datenbanken mit CEOs und anderen Führungskräften, insbesondere für Unternehmen, die einer verstärkten öffentlichen Meinungsbildung und Unzufriedenheit ausgesetzt sind.	— Für Führungskräfte in Unternehmen besteht ein erhebliches Risiko für die persönliche Sicherheit, wenn sie Ziel einer Massen-Doxxing-Kampagne werden. — Die zunehmende Besorgnis darüber, wie einfach Doxxing-Kampagnen über soziale Medien durchgeführt werden können, könnte zu strengeren Vorschriften und Compliance-Anforderungen für soziale Medien führen, insbesondere in Bereichen wie dem Datenschutz. — Unternehmen müssen möglicherweise in Ressourcen für das Krisenmanagement investieren, um Fälle von Doxxing, das auf Führungskräfte abzielt, zu überwachen, zu identifizieren und darauf zu reagieren.


ASIA
AFRICA
SOUTH
AUSTRALIA
Indian
Ocean
North
Atlantic
Ocean
South
Atlantic
Ocean

Global

2

Gemeinsame sozioökonomische Missstände treiben weitere Proteste der Generation Z voran

In mehreren Ländern, darunter Algerien, Madagaskar, Mexiko, Nepal und Peru, kam es im Jahr 2025 zu groß angelegten Protesten gegen die Regierung, die hauptsächlich von jungen Menschen der Generation Z angeführt wurden. Die Demonstrierenden prangerten dabei schlechte wirtschaftliche Bedingungen, politische Instabilität und Korruption auf Regierungsebene an. Die öffentlichkeitswirksamen Erfolge dieser Gruppen, die in einigen Fällen einen Regimewechsel herbeiführten, dürften in Verbindung mit gemeinsamen sozioökonomischen Faktoren die Ausbreitung und Intensivierung solcher Protestaktionen im Jahr 2026 fördern.

- Es ist sehr wahrscheinlich, dass die Länder des Globalen Südens auch in Zukunft besonders stark von Protesten betroffen sein werden, da in diesen Regionen Studenten-/Jugendproteste aufgrund wirtschaftlicher und politischer Missstände begünstigt werden.
- Gewaltsame Auseinandersetzungen zwischen Demonstrierenden und lokalen Behörden führen mit hoher Wahrscheinlichkeit zu landesweiten Störungen und stellen eine Bedrohung für öffentliche Gebäude und als regierungsnah wahrgenommene Unternehmen dar. Das Schwenken von Bannern, Slogans und die weitverbreitete Verwendung von Jugendsymbolen werden höchstwahrscheinlich ausgenutzt, um weitere Teilnehmende für die Demonstrationen zu gewinnen.
- Die Nutzung sozialer Medien wird mit ziemlicher Sicherheit ein entscheidendes Merkmal der Proteste der Generation Z bleiben, da sie es den Bewegungen ermöglichen, dezentral zu kommunizieren und Aktionen zu koordinieren, was landesweite Störungen verschärft und die Reaktionsfähigkeit der lokalen Behörden beeinträchtigt.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Der Trend der Generation Z verlangsamt sich, aber es finden weiterhin Proteste statt, wobei weniger Gewalt und Zusammenstöße mit den Strafverfolgungsbehörden gemeldet werden.	Verbesserung	Unwahrscheinlich (15%)
Die Proteste breiten sich weiter aus und ziehen weitere Teilnehmende an, was zu großen Veränderungen der politischen Lage führt, ohne dass alle Forderungen der Demonstrierenden erfüllt werden.	Baseline	Wahrscheinlich (40 %)
Der Erfolg früherer Demonstrationen der Generation Z fördert die Bildung neuer Gruppen. Gewaltsame Proteste breiten sich weltweit aus und verschärfen die Unsicherheit in Regionen, die bereits unter Instabilität leiden.	Verschlechterung	Wahrscheinlich (45 %)

Handlungsempfehlungen

- Überwachen Sie verstärkt Online-Plattformen, die von den Bewegungen der Generation Z zur Koordinierung ihrer Aktivitäten genutzt werden, darunter Discord, Facebook, Instagram, LinkedIn, Reddit, TikTok und X.
- Den Sicherheitsteams wird empfohlen, Notfallpläne zu implementieren und die Sicherheitsprotokolle zu verstärken, um den Geschäftsbetrieb aufrechtzuerhalten und die Sicherheit der Anlagen und Mitarbeitenden zu gewährleisten. Bei der Umsetzung der Notfallplanung sollten flexible Arbeitsregelungen, wie z. B. Fernarbeit, berücksichtigt werden.
- Unternehmen sollten eine deutliche Kommunikation mit den Konsulaten und Botschaften pflegen, um über die Entwicklung der Situation informiert zu bleiben und die Sicherheit des Geschäftsumfelds zu beurteilen.

Indikatoren	Auswirkungen
— Gruppen aus Mitgliedern der Generation Z organisieren sich weiterhin weltweit in den sozialen Medien, wobei groß angelegte Proteste im Voraus geplant und beworben werden. — Große Protestbewegungen der Generation Z führen zu bedeutenden politischen Veränderungen. — Die politische Führung sorgt für verstärkte Sicherheitsmaßnahmen, vor allem in der Umgebung von öffentlichen Gebäuden. — In dem betroffenen Land kommt es zu zahlreichen Unruhen, bei denen Demonstrierende mit unterschiedlichen Hintergründen die sozioökonomische Politik anprangern. — Gegenreaktionen und die öffentliche Kritik im Internet an der Regierung nehmen zu.	— Aufgrund der hohen Teilnehmendenzahl und der verwendeten Taktiken, Techniken und Prozeduren wird erwartet, dass die Proteste der Generation Z den Geschäftsbetrieb und die lokalen Lieferketten stören werden. — Größere politische Veränderungen führen zu einer Änderung der Rechtsvorschriften für Unternehmen, die in dem betroffenen Land tätig sind. — Stärkere Sicherheitsmaßnahmen für Unternehmen, die sich in den Gebieten der Proteste befinden, werden zu hohen finanziellen Kosten führen. — Gewaltsame Zusammenstöße mit den örtlichen Behörden führen zu Schäden an Sachanlagen und Infrastruktur und gefährden die Sicherheit der Vermögenswerte von Unternehmen, die sich in den Gebieten der Proteste befinden.

US-Wirtschaftspolitik sorgt für weltweite Unsicherheit und Risiken

Die globale Marktinstabilität wird aufgrund der unvorhersehbaren US-Wirtschaftspolitik auch 2026 anhalten und Auswirkungen auf zahlreiche Branchen haben. Dabei sind insbesondere die Branchen betroffen, die als Motor des Handelsungleichgewichts gelten, darunter Stahl/Aluminium, Automobilbau, Elektronik/Technologie, Bekleidung, Seltene Erden, Lebensmittel und Landwirtschaft sowie Arzneimittel. Ein anhängiger Fall vor dem Obersten Gerichtshof der USA hinsichtlich der Anwendung des amerikanischen Gesetzes über internationale wirtschaftliche Notfallbefugnisse (International Emergency Economic Powers Act) durch die Trump-Regierung wird wahrscheinlich die Möglichkeiten der Regierung einschränken, willkürliche Beschränkungen festzulegen. In diesem Fall sind jedoch Bemühungen, gezielte, wenn auch begrenzte Steuerungsmechanismen durch Auslegungen des Handelsgesetzes (Trade Act) von 1974 oder des Handelserweiterungsgesetzes (Trade Expansion Act) von 1962 anzuwenden, realistisch möglich.

- Auch wenn der Einsatz direkter militärischer Maßnahmen nach wie vor in weiter Ferne liegt, deutete die US-Rhetorik im Jahr 2025 darauf hin, dass die USA militärische Operationen in Erwägung ziehen, um Einfluss auf strategisch bedeutsame Orte (wie Grönland oder den Panamakanal) zu nehmen und damit auf die wahrgenommenen geoökonomischen Bedrohungen ihrer Gegner zu reagieren.
- Anzeichen dafür, dass die USA die Anwendung von Gewalt in Erwägung ziehen oder anderweitig Druck auf Partner ausüben, um ihre strategische Position zu stärken, werden zu einer deutlich negativen Marktstimmung führen und die bestehenden Verbündeten der USA weiter entfremden.
- Unternehmen, die Unsicherheiten abmildern möchten, könnten durch Maßnahmen wie Lagerhaltung, Near-/Offshoring und Überprüfung der Logistik- und Lieferkettenbeziehungen weitere Marktinstabilität verursachen. Ansätze wie die zunehmende Digitalisierung und Zentralisierung bergen ihre eigenen Risiken, wie z. B. eine erhöhte Anfälligkeit für Bedrohungen der Cybersicherheit.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die USA setzen ihre gezielten Beschränkungen mit gerichtlich erzwungenen Obergrenzen fort, was die negative Marktstimmung aufrechterhält, wenn auch die Ziele berechenbarer und enger werden.	Verbesserung	Wahrscheinlich (55 %)
Die USA erlassen weiterhin unvorhersehbar und willkürlich Beschränkungen, z. B. um politische Meinungsverschiedenheiten mit Handelspartnern abzustrafen. Dies veranlasst die Verbündeten der USA dazu, nach alternativen Handelspartnern zu suchen, um die Beschaffung kritischer Waren sicherzustellen.	Baseline	Realistische Möglichkeit (40 %)
Die USA führen militärische Operationen durch, um die Kontrolle über strategische wirtschaftliche Engpässe zu erlangen, was die globale wirtschaftliche Instabilität und die regionale Sicherheit verschlechtert.	Verschlechterung	Fernliegend (5 %)

Handlungsempfehlungen

- Erwägen Sie die Ausarbeitung von Eskalationsplänen, um die Entscheidungsfindung bei sich schnell ändernden Vorschriften zu steuern und dabei die betriebliche Kontinuität in den betroffenen Regionen aufrechtzuerhalten.
- Prüfen oder implementieren Sie Strategien zur Verlustvermeidung und -minderung, insbesondere bei Unternehmen mit globalen Lieferketten.
- Unternehmen, die in der Lieferkettenlogistik tätig sind, sollten die Auswirkungen auf das Geschäft prüfen, die sich aus dem Verlust der von amerikanischen Unternehmen erbrachten Dienstleistungen (einschließlich KI- und GPS-basierter Systeme) ergeben.

Indikatoren	Auswirkungen
— Der Oberste Gerichtshof fällt Anfang 2026 ein Urteil, das die Befugnisse der Exekutive bei der Festlegung von Zöllen und Ausfuhrkontrollen einschränken soll. — Das Weiße Haus weist das Handelsministerium an, Untersuchungen im Rahmen des Handelserweiterungsgesetzes durchzuführen. — Die politische Rhetorik der US-Regierung in Bezug auf die Übernahme/Kontrolle strategischer Schlüsselgebiete nimmt zu. — Bilaterale Abkommen zwischen den Verbündeten der USA (z. B. Westeuropa, Kanada) und China und den Mittelmächten (z. B. Kolumbien) vertiefen sich. — KI-gestützte Marktlösungen zur Bewältigung von Problemen in der Lieferkette entstehen rasch.	— Kostenschwankungen wirken sich auf die Finanzprognosen und die Unternehmensbewertung aus. — Die Märkte werden zunehmend opportunistisch oder unrentabel, was zu einer Verlagerung des Geschäftsbetriebs führt. — Es entstehen erhöhte Ausgaben zur Behebung von Sicherheitslücken aufgrund neuer/ungewohnter Prozesse und Protokolle. — Die US-Politik führt dazu, dass bestimmte Branchen oder Unternehmen aufgrund von Verstößen gegen die Vorschriften finanzielle Verluste erleiden. — Unternehmen sind einer starken Bedrohung durch Insider ausgesetzt, insbesondere wenn sie in kritischen Branchen tätig sind.

Verbreitung von Terrormaterial auf Open-Source-Plattformen treibt die Terrorgefahr durch Einzeltäter voran

Extremistische Inhalte, terroristische Manifeste und ideologische Propaganda werden sich auch 2026 im Internet weiter verbreiten, u. a. in den gängigen sozialen Medien, auf Gaming-Plattformen und dezentralen Datentauschbörsen. Diese Inhalte ermöglichen es selbst Einzeltätern, d. h. Einzelpersonen ohne formale Verbindungen zu etablierten Terrorgruppen, Anschläge mit wenig oder gar keiner Unterstützung von außen zu planen und durchzuführen. Der einfache Zugang zu detaillierten Anleitungen für die Planung von Angriffen und die Auswahl von Zielen in Verbindung mit der Verfügbarkeit von neuen Technologien wie Drohnen und 3D-Druckern wird die Bedrohungslage für die physische Sicherheit weiter verändern.

- Einzeltäter werden mit ziemlicher Sicherheit der am schwierigsten zu überwachende Bedrohungsfaktor für Sicherheitsdienste bleiben, da sie nicht in etablierte Netzwerke eingebunden sind und nur einen minimalen digitalen Fußabdruck hinterlassen. Einzeltäter reproduzieren dabei häufig Taktiken, Techniken und Prozeduren, die in offen verfügbaren Handbüchern zu finden sind, insbesondere Angriffe von geringer Komplexität wie Angriffe mit Fahrzeugen, Nahkampfwaffen und Handfeuerwaffen.
- Die zunehmende Politisierung und Fragmentierung von sozialen Netzwerken in Verbindung mit der Unfähigkeit der Moderation von Inhalten, damit Schritt zu halten, schafft ideale Bedingungen für die Radikalisierung von Nutzern dieser Netzwerke.
- Extremistische Gruppen experimentieren bereits mit dem Einsatz von GenAI-Tools, was auf ein mittel- bis langfristiges Nutzungspotenzial hindeutet. Es ist sehr wahrscheinlich, dass KI eingesetzt wird, um bestehende Systeme zur Moderation von Inhalten zu umgehen und Krisen durch die schnelle Erstellung und Verbreitung von Propaganda zur Aufwiegelung zu Gewalt auszunutzen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die Verbreitung von offen zugänglichem extremistischem Material wird durch eine verbesserte Moderation von Inhalten verringert, wodurch der Weg zur Radikalisierung von Einzeltätern verlangsamt und potenzielle Extremisten in etablierte (und überwachte) Bahnen gelenkt werden.	Verbesserung	Sehr unwahrscheinlich (10 %)
Angriffe durch Einzeltäter bleiben auf dem derzeitigen Niveau, da extremistische Inhalte weiterhin über öffentliche Plattformen zugänglich sind und Einzelpersonen die Möglichkeit bieten, sich von Gruppen unabhängig zu radikalisieren.	Baseline	Wahrscheinlich (55 %)
Der Umfang und die Detailliertheit des öffentlich zugänglichen terroristischen Materials nehmen erheblich zu, was weltweit zu einem Anstieg von Anschlägen durch Einzeltäter führt.	Verschlechterung	Unwahrscheinlich (35 %)

Handlungsempfehlungen

- Entwickeln Sie Szenario-Pläne für gängige terroristische Anschlagsarten, einschließlich Angriffsszenarien mit Nahkampfwaffen, Sprengstoffen, Schusswaffen, Feuerwaffen, Fahrzeugen, Entführungen gegen Lösegeld und Erpressung sowie mit Schadstoffen, einschließlich chemischer, biologischer, radiologischer und nuklearer Waffen.
- Stellen Sie sicher, dass die Mitarbeitenden die Anzeichen und Verfahren für die Meldung potenziell radikalisierter Personen kennen und bieten Sie Schulungen und Hilfsmittel an, um die Mitarbeitenden zu unterstützen und zu fördern.
- Führen Sie Überwachungs- und Meldeverfahren zur Ermittlung und Überprüfung potenzieller Bedrohungen durch Personal vor Ort, lokale Nachrichten und soziale Medien ein, wobei alle Informationen mit offiziellen/glaubwürdigen Quellen abgeglichen werden müssen.

Indikatoren	Auswirkungen
— Nationale Sicherheitsbehörden geben Warnungen heraus bzw. erhöhen die Terrorstufen und warnen vor zunehmenden Bedrohungen durch Einzeltäter im Zusammenhang mit der Radikalisierung im Internet. — Ausweitung von Propagandainhalten, die auf bisher unerschlossene regionale oder demografische Gruppen abzielen (z. B. in verschiedene Sprachen übersetzte Propaganda). — Erhebliche Zunahme der Verbreitung, des Herunterladens oder des erneuten Einstellens von extremistischen Handbüchern und Propaganda auf Open-Source-Plattformen. — Technologieplattformen lösen ihre Moderationsteams für die Inhalte auf oder ändern ihre Richtlinien, sodass mehr extremistische Inhalte unkontrolliert verbreitet werden können.	— Unternehmen in großen Ballungsräumen sind aufgrund der erhöhten Bedrohungslage und der verstärkten Sicherheitsmaßnahmen mit Betriebsstörungen konfrontiert. — Das Zielprofil für Einzeltäter erweitert sich, da extremistische Online-Inhalte mit persönlichen Problemen zusammentreffen, wobei auch Privatunternehmen als Ziel in Frage kommen. — Es ist wahrscheinlicher, dass Unternehmen Rufschädigungen erleiden und potenziellen behördlichen Maßnahmen ausgesetzt sind, wenn ihre Dienste, Plattformen oder Produkte für die Produktion, das Hosting oder die Verbreitung von terroristischem Material missbraucht werden.


Kazakhstan
Uzbekistan
Turkey
Iraq
Jordan
Pakistan
Egypt
Saudi Arabia
UAE
Oman
Bangladesh
Morocco
Algeria
Tunisia
Mauritania
Mali
Niger
Chad
Sudan
Senegal
Guinea
Burkina Faso
Sierra Leone
Ivory Coast
Ghana
Togo
Benin
Nigeria
Cameroon
Ethiopia
Sri Lanka
Gabon
Uganda
Kenya
DRC
Tanzania
Angola
Zambia
Malawi
Mozambique
Madagascar
Namibia
Botswana
South Africa

AMEA

Sicherheitslage im Nahen Osten wird nach Waffenstillstand im Gazastreifen komplexer

Wichtige Entwicklungen im Nahen Osten haben auch 2025 die Sicherheitslage in der gesamten Region verschärft. Hinzu kamen das Scheitern des ersten Waffenstillstands zwischen Gaza und Israel im März, der 12-tägige Konflikt zwischen dem Iran und Israel im Juni sowie die Einstellung der Atomverhandlungen zwischen dem Iran und den USA. Während im Gazastreifen seit Oktober ein zweiter Waffenstillstand gilt, ist die Lage im Nahen Osten weiterhin angespannt. Für viele der wichtigsten Faktoren der Spannungen in der Region ist zu Beginn des Jahres 2026 keine Lösung in Sicht.

— Die USA und andere Länder versuchen, eine internationale Task Force im Gazastreifen einzurichten, um die Regierungsführung und die Stabilität nach dem Konflikt zu unterstützen. Es gilt als wahrscheinlich, dass Israel sich gegen die Beteiligung bestimmter Staaten, insbesondere der Türkei, aussprechen wird, sodass Meinungsverschiedenheiten über die künftige Verwaltung des Gebiets bestehen bleiben.

— Nachdem der Iran und seine Erfüllungsgehilfen 2025 in Konflikten mit Israel erhebliche Verluste erlitten haben, werden sie ihre Fähigkeiten wahrscheinlich regenerieren und erneuern, um danach zu früheren strategischen Zielen und Taktiken zurückzukehren. Während eine weitreichende Einflussnahme 2026 aufgrund des Ausmaßes der Verluste wahrscheinlich schwierig sein wird, werden Angriffe auf wichtige strategische und ideologische Ziele (wie Aktionen an der jemenitischen Grenze) mit ziemlicher Sicherheit fortbestehen.

— Die Atomgespräche zwischen dem Iran und den USA sind nach wie vor festgefahren, und es gibt kaum Anzeichen für Fortschritte. Da keine unmittelbare Einigung erkennbar ist, werden die bilateralen Spannungen mit ziemlicher Sicherheit auch 2026 anhalten und die Risiken für westliche Einrichtungen durch die iranische Kriegsführung in der Grauzone, z. B. durch Cyberangriffe, weiterhin bestehen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Es wird ein langfristiges Friedensabkommen für Gaza abgeschlossen. Verbesserte Beziehungen zwischen Israel und den USA und Iran/Syrien führen zu formellen Sicherheitsvereinbarungen und einer Deeskalation der Sicherheitslage.	Verbesserung	Sehr unwahrscheinlich (10 %)
Kaum Fortschritte bei den Atomverhandlungen zwischen dem Iran und den USA und vereinzelte Zusammenstöße im Nahen Osten (Gaza, Libanon, Syrien), die zu einem erneuten bewaffneten Konflikt und weiterer Unsicherheit führen könnten.	Baseline	Realistische Möglichkeit (50 %)
Erneuter bewaffneter Konflikt an verschiedenen Schauplätzen, in den Israel verwickelt ist (Gaza, Iran, Libanon, Syrien), was zu weiteren Angriffen auf die Seeschifffahrt im Roten Meer führt und den Handelsverkehr stört.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

— Entwickeln Sie detaillierte Pläne zur Geschäftskontinuität, die verschiedene Störungsszenarien berücksichtigen, darunter die Schließung von Seerouten, die Unterbrechung des regionalen Bankverkehrs und der Lieferkette auf lokaler, regionaler und globaler Ebene.

— Überprüfen und verbessern Sie die Cybersicherheitsmaßnahmen zum Schutz vor staatlich unterstützten Angriffen, insbesondere im Hinblick auf kritische Infrastrukturen und sensible Daten.

— Schärfen Sie das Bewusstsein, dass die Spannungen im Nahen Osten auch weiterhin Bedrohungsakteure auf internationaler Ebene, einschließlich Aktivisten und Terroristen/Extremisten, motivieren können.

Indikatoren	Auswirkungen
— Zunahme von Zwischenfällen im Gazastreifen/ Libanon, an denen israelische Streitkräfte und iranische Erfüllungsgehilfen wie die Hamas/Hisbollah beteiligt sind. — Starke Zunahme von Zwischenfällen im Roten Meer und im Persischen Golf, insbesondere mit Schiffen mit Verbindungen zu israelischen oder westlichen Interessen. — Plötzliche Änderungen bei den israelischen Truppenbewegungen bzw. -einsätzen im Gazastreifen, im Libanon und in Syrien. — Scheitern der Gespräche über die internationale Eingreiftruppe im Gazastreifen und dessen Verwaltung nach dem Konflikt. — Eskalation der israelischen Spannungen mit Syrien/ Iran, einschließlich einer verschärften Rhetorik im Gazastreifen.	— Rasche Äderungen in der regionalen Dynamik infolge wechselnder Loyalitäten, z. B. in den Beziehungen der USA zu Israel/Syrien. — Erneute Störungen der regionalen Versorgungsketten und Schifffahrtsrouten, insbesondere im Energie- und Seeverkehrssektor. — Zunehmende Häufigkeit bzw. Intensivierung der Aktivitäten der weltweiten Pro-Palästina-Bewegung, die eine Bedrohung für westliche Unternehmen mit tatsächlichen bzw. vermeintlichen Verbindungen zu Israel darstellt. — Strategische Änderungen in der Geschäftstätigkeit aufgrund regionaler Entwicklungen, die eine neue Sicherheitsdynamik schaffen.

Militante Islamisten weiten Aktivitäten in Westafrika aus

Verschiedene islamistische Gruppen, darunter Boko Haram und Islamischer Staat – Provinz Westafrika, haben 2025 ihre Anschläge in der Sahelzone und in Westafrika fortgesetzt. Diese richteten sich gegen Zivilisten, Militärangehörige, Regierungseinrichtungen und Unternehmen. Länder wie Burkina Faso, Niger und Mali werden weiterhin die Auswirkungen des Abzugs der westlichen militärischen Unterstützung bei der Terrorismusbekämpfung spüren. In Mali wird die Eskalation wahrscheinlich weiterhin am stärksten sein, was auf den wachsenden Einfluss der Terroristengruppe Dschamaat Nusrat al-Islam wal-Muslimin (JNIM) zurückzuführen ist, die Ende 2025 die Treibstoffversorgung zwischen Senegal und der malischen Hauptstadt Bamako unterbrochen hat.

- Die betroffenen Staaten werden wahrscheinlich zunehmend international isoliert, da ausländische Regierungen Reisewarnungen zum Schutz ihrer Bürger herausgeben. Dies wird höchstwahrscheinlich die wirtschaftlichen Herausforderungen verschärfen, Investitionen und Wachstum bremsen und extremistische Gruppen weiter stärken, insbesondere in abgelegenen Gebieten, in denen die Bemühungen zur Terrorismusbekämpfung nach wie vor unzureichend sind.
- Islamistische Gruppen, insbesondere die JNIM, werden wahrscheinlich zunehmend grenzüberschreitende Operationen durchführen und dabei Gebiete mit schwacher staatlicher Kontrolle wählen, um grenzüberschreitende Anschläge und möglicherweise auch Anschläge im Ausland zu verüben. Diese Bemühungen werden wahrscheinlich durch den zunehmenden Einsatz fortschrittlicher Technologien wie Drohnen zur Durchführung von Anschlägen noch verstärkt.
- Angriffe auf ausländische Anlagen, Bergbaubetriebe und kritische Infrastrukturen werden wahrscheinlich eskalieren und möglicherweise koordinierte Erpressungen, Entführungen gegen Lösegeld und vorsätzliche Unterbrechungen der regionalen Versorgungsketten zwischen den Binnenstaaten der Sahelzone und den Küstenhäfen umfassen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die Länder der Region starten gemeinsam mit internationalen Partnern regionale Anti-Terror-Operationen und treiben die Gruppen in immer entlegenere Gebiete.	Verbesserung	Sehr unwahrscheinlich (10 %)
Islamistische Gruppen verüben nach wie vor Anschläge. Sie bleiben jedoch eine inländische Bedrohung innerhalb einzelner Länder oder begrenzter geografischer Gebiete. Die Regionen sind nach wie vor feindselig gegenüber Ausländern und Unternehmen eingestellt.	Baseline	Realistische Möglichkeit (40 %)
Islamistische Gruppen treiben die Eskalation voran und weiten ihre Anschläge grenzüberschreitend aus, was eine zunehmende Bedrohung für die politische Stabilität, ausländische Vermögenswerte und Interessen in der gesamten Region darstellt.	Verschlechterung	Realistische Möglichkeit (50 %)

Handlungsempfehlungen

- Überwachen Sie die Hinweise und öffentlichen Erklärungen der Regierung, einschließlich Einschränkungen für bestimmte Regionen und Unterregionen, Sicherheitseinsätze und Sicherheitsvorkehrungen, wie z. B. die Anweisung, sich in Sicherheit zu bringen.
- Für Unternehmen, die in brisanten Regionen tätig sind, sollten starke Sicherheits- und Personalschutzmaßnahmen sowie Notfallmaßnahmen/Kontinuitätspläne für den Fall eines Anschlags eingeführt werden.
- Entwickeln und pflegen Sie Kommunikationspläne mit dem Personal in brisanten Regionen, um eine zügige Übermittlung von Warnungen und Änderungen der Sicherheitsvorkehrungen zu gewährleisten.

Indikatoren	Auswirkungen
— Die Angriffe nehmen an Häufigkeit und Schwere zu und richten sich zunehmend gegen stärker bevölkerte Gebiete. — Angriffe werden auch in zuvor nicht betroffenen Regionen/Ländern durchgeführt. — Entführungen, Lösegeldforderungen und Erpressungen von Ausländern nehmen zu. — Mobilitätseinschränkungen und Unterbrechungen der Lieferkette, die extremistischen Gruppen zugeschrieben werden, nehmen zu. — Regionale Regierungen organisieren Treffen, um koordinierte Maßnahmen zur Terrorismusbekämpfung zu planen. — Weitere Reisewarnungen ausländischer Regierungen, die sich auch auf Nachbarländer erstrecken.	— Die nationalen Unruhen in den betroffenen Regionen eskalieren und führen zu Protesten und gewaltsamen Zusammenstößen in urbanen Gebieten. — Wichtige Versorgungsketten für Mineralien aus den Regionen werden unterbrochen, was sich auf die Tätigkeit abhängiger Sektoren auswirkt. — Die humanitären Herausforderungen in den betroffenen Regionen eskalieren, darunter Hungersnöte, Krankheitsausbrüche und eingeschränkter Zugang zu wichtigen Hilfsgütern. — Ausländische Staatsangehörige sind einem erhöhten Sicherheitsrisiko ausgesetzt, das sich auch auf Bürger im Ausland, diplomatisches Personal und Geschäftsleute auswirkt.

Aufstrebende Märkte bieten Chancen und Risiken für Unternehmen

Die Milderung oder Beendigung von Konflikten in der gesamten AMEA-Region im Jahr 2025 hat Möglichkeiten für erneute Investitionen im Privatsektor eröffnet. Die Wiedereingliederung Syriens in die internationale Gemeinschaft bzw. Weltwirtschaft unter dem neuen Regime von Präsident Ahmed al-Scharaa ist das beste Beispiel. Auch der anhaltende Waffenstillstand im Gazastreifen, weniger intensive Kämpfe bzw. ein begrenzter Waffenstillstand in Myanmar, die Entwaffnung der Arbeiterpartei Kurdistans (PKK) und Friedensabkommen in der Demokratischen Republik Kongo und zwischen Armenien und Aserbaidschan werden 2026 wahrscheinlich Chancen bieten.

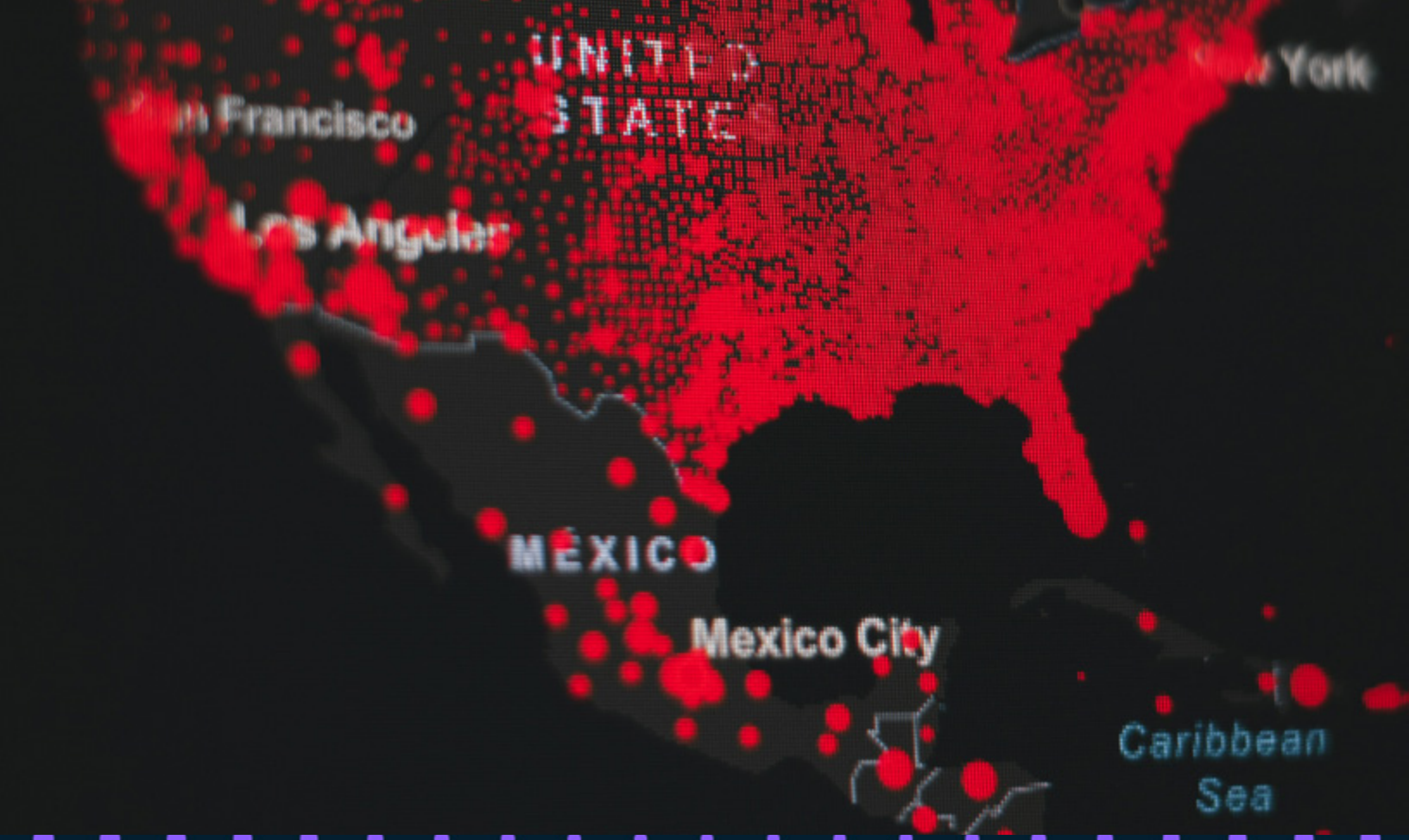
- Der Zugang zu bisher unerreichbaren Märkten und lukrativen Aufträgen für den Wiederaufbau und die Entwicklung dürfte ausländische Direktinvestitionen fördern, die zusammen mit ausländischer Staatshilfe, der Aufhebung von Sanktionen und der Rückkehr von Arbeitskräften aus dem Ausland die humanitären Bedingungen verbessern und das Wirtschaftswachstum ankurbeln können.
- Trotz der Deeskalation von Konflikten bleibt die Sicherheitslage in vielen Fällen prekär. Zu den Risiken gehören ehemalige Kämpfer, die in die Kriminalität abrutschen oder Racheanschläge verüben, um Behörden zu untergraben, anhaltende soziopolitische Spannungen, die Entwicklungs- und Wiederaufbaubemühungen behindern, oder eine erneute Eskalation von Konflikten in einem Krisenherd.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Der schnelle wirtschaftliche Aufschwung in Ländern, die einen Konflikt hinter sich haben, wird durch eine Versöhnung ehemals konkurrierender Gruppierungen und erhebliche finanzielle Unterstützung durch internationale Partner vorangetrieben.	Verbesserung	Sehr unwahrscheinlich (10 %)
Der Waffenstillstand bzw. die Beendigung des Konflikts hält an, es kommt jedoch weiterhin zu moderaten Sicherheitsproblemen. Der wirtschaftliche Wiederaufbau schreitet allmählich voran, wird jedoch durch anhaltende Spannungen beeinträchtigt.	Baseline	Realistische Möglichkeit (50 %)
Der Konflikt bricht erneut aus, wenn neue konkurrierende Fraktionen des herrschenden Regimes zu den Waffen greifen oder frühere Rivalen beschließen, in den Konflikt zurückzukehren oder sich an gewaltsamen Aufständen zu beteiligen.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

- Unternehmen, die erneut in diese Märkte eintreten möchten, sollten eine strenge Due-Diligence-Prüfung und Risikobewertung für die Geschäftstätigkeit in dem Land durchführen und robuste Notfallpläne für eine Reihe möglicher Sicherheitsprobleme erstellen.
- Arbeiten Sie mit überprüften und vertrauenswürdigen Einheimischen zusammen, um die Komplexitäten im Land nach dem Konflikt zu bewältigen. Dazu sollten sowohl Personen gehören, die während des Konflikts im Land geblieben sind, als auch Migranten, die vor den Kämpfen geflohen sind, und Doppelstaatsangehörige, die mit der Sprache und Kultur sowohl des Gastlandes als auch des beteiligten Unternehmens vertraut sind.
- Investieren Sie in vielschichtige und angemessene Sicherheitsmaßnahmen, einschließlich vertrauenswürdiger lokaler Mitarbeitender, interner Sicherheits- und Nachrichtendienstmitarbeitender und etablierter Kanäle mit Schlüsselpersonen, einschließlich Friedenstruppen und Botschaftspersonal.

Indikatoren	Auswirkungen
— Nachhaltige Einbeziehung der wichtigsten geopolitischen Blöcke in Verhandlungen zwischen Konfliktparteien. — Offizielle Wiederaufnahme diplomatischer Beziehungen und Wiedereröffnung von Botschaften durch große Länder. — Aussetzung bzw. Lockerung von Sanktionen und Zöllen gegen Länder, die in Konflikte verwickelt sind. — Unternehmen, die ihre Tätigkeit auf Gebiete ausweiten, die zuvor von Konflikten betroffen waren. — Erhöhte Rückkehrquote von Geflüchteten in die betroffenen Länder.	— Die Wiedereingliederung mehrerer Länder/Gebiete in die Weltwirtschaft wird wahrscheinlich zu einer Verschiebung der Lieferketten führen und lukrative wirtschaftliche Möglichkeiten eröffnen. — Unternehmen, die stark in aufstrebende Märkte investieren, sind höchstwahrscheinlich einem erheblichen Risiko ausgesetzt, wenn der Konflikt wieder aufflammt oder sich die Sicherheitslage destabilisiert. — Unternehmen, die eng mit den neuen Behörden oder einer einzelnen Gruppierung zusammenarbeiten, laufen Gefahr, in verbleibenden Kämpfen ein legitimes Ziel zu werden. — Umgekehrte Migrationstrends werden möglicherweise zu neuen Spannungen in Fragen wie Landbesitz usw. führen.



Nord- und Südamerika

4

Neuausrichtung der USA auf Lateinamerika verschärft die politische Unsicherheit und regionale Instabilität

Die Neuausrichtung der amerikanischen Außenpolitik gegenüber Lateinamerika nach der Rückkehr von Donald Trump ins Präsidentenamt wird sich voraussichtlich 2026 fortsetzen. Dieser Ansatz zielte ursprünglich auf die Bekämpfung des Drogenhandels durch organisierte Kriminalität ab, hat sich aber inzwischen zu einer Durchsetzung des US-Einflusses in der Region entwickelt und trägt erheblich zur politischen Unsicherheit und regionalen Instabilität bei. Das erneute Engagement der USA in der Region ist höchstwahrscheinlich eine Reaktion auf die wachsende Besorgnis über den zunehmenden politischen und wirtschaftlichen Einfluss Chinas in Lateinamerika.

— Die USA haben in den frühen Morgenstunden des 3. Januar Luftangriffe auf Bodenziele in Venezuela durchgeführt und dabei Präsident Nicolas Maduro festgenommen. US-Präsident Trump hat seitdem angedeutet, dass die USA einen Machtwechsel in dem Land herbeiführen werden. Es wurden weitere Maßnahmen angedroht, falls die nationalen Behörden nicht kooperieren. Allerdings wurden die Pläne für einen Machtwechsel nicht im Detail öffentlich bekannt gegeben, und die Lage bleibt instabil.

— Die Wiederinbetriebnahme und Modernisierung von US-Militäreinrichtungen in der Karibik kann die langfristige Stationierung von modernsten militärischen Anlagen erleichtern. Die lateinamerikanischen Länder werden dies höchstwahrscheinlich als Sicherheitsbedrohung wahrnehmen, was zu einer Stärkung der wirtschaftlichen und militärischen Beziehungen zu den strategischen Rivalen der USA führen könnte.

— Die USA werden wahrscheinlich ihre Kriegsführung in der Grauzone in Lateinamerika und der Karibik ausweiten, insbesondere in Ländern, die als den USA nicht freundlich gesinnt gelten. Die Trump-Regierung hat bewiesen, dass sie bereit ist, einen Regimewechsel zu erzwingen und mit aufrührerischer Rhetorik Einfluss auf die Außenpolitik zu nehmen, was mit ziemlicher Sicherheit zu einer weiteren politischen Spaltung in Lateinamerika führen wird.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die USA arbeiten mit den nationalen Behörden zusammen, um einen friedlichen und geordneten Machtwechsel in Venezuela zu überwachen, und reduzieren ihre militärische Aufrüstung in der Karibik.	Verbesserung	Sehr unwahrscheinlich (10 %)
Die Lage in Venezuela ist nach wie vor instabil und unbeständig, da Einzelheiten eines von den USA geführten Machtwechsels weiterhin unklar sind. Gleichzeitig setzen die USA die Regime in Ländern wie Kolumbien und Kuba weiter unter Druck.	Baseline	Wahrscheinlich (65 %)
Die Sicherheitslage in Venezuela verschlechtert sich, da konkurrierende Gruppierungen versuchen, die Macht über das Land zu erlangen, während die USA weitere Maßnahmen gegen die Führung gegnerischer Regime ergreifen.	Verschlechterung	Unwahrscheinlich (25 %)

Handlungsempfehlungen

— Bewerten Sie die Exposition bzw. Abhängigkeit von den Lieferketten/Handelsrouten bestimmter Regionen und diversifizieren Sie bzw. minimieren Sie die durch geopolitische Ereignisse verursachten Unterbrechungen.

— Entwickeln Sie Notfallpläne für gestörte diplomatische Beziehungen und Zeiten erhöhter Bedrohung bzw. Unruhen und investieren Sie in Daten zu geopolitischen Risiken, um entstehende Konflikte zu überwachen, zu antizipieren und darauf zu reagieren.

— Entwickeln Sie detaillierte Pläne zur Geschäftskontinuität, die verschiedene Störungsszenarien berücksichtigen, darunter die Schließung von Seerouten, die Unterbrechung des regionalen Bankverkehrs und die Unterbrechung der Lieferkette für Unternehmen auf regionaler und globaler Ebene.

Indikatoren	Auswirkungen
— Laufende Erneuerung und Modernisierung der militärischen Infrastruktur der USA in der Karibik, darunter Luftwaffenstützpunkte und Marineeinrichtungen, mit zusätzlicher Verlegung von modernster Hardware in die Region. — Verstärkte anti-amerikanische Botschaften aus verschiedenen lateinamerikanischen Ländern und umgekehrt aus den USA. — Demonstrationen in lateinamerikanischen Ländern unter Berufung auf den US-Imperialismus mit der Forderung, die Einmischung der USA in die inneren Angelegenheiten zu beenden und die Beziehungen zu den USA abzubrechen. — Ankündigung einer verstärkten Zusammenarbeit bzw. von Abkommen zwischen lateinamerikanischen Staaten und strategischen Rivalen der USA. — Änderungen bei der Entscheidung der USA, in bestimmten Ländern Lateinamerikas direkte Maßnahmen zu ergreifen.	— Zunehmende Komplexität der Einhaltung von Vorschriften für multinationale Unternehmen, die in Lateinamerika und den USA tätig sind. — Vermehrte Proteste und direkte Aktionen gegen mit den USA verbundene Unternehmen durch Pro-Lateinamerika- bzw. Anti-US-Aktivistengruppen, die sich negativ auf die Geschäfte der Unternehmen auswirken. — Die regionale Unsicherheit untergräbt das Vertrauen der Investoren und verringert ausländische Investitionen. — Verschlechterung der diplomatischen Beziehungen, selbst zwischen langjährigen Verbündeten, was zu Behinderungen des Reiseverkehrs von Mitarbeitenden und im bilateralen Handel führt.

Zunahme des politischen Extremismus in Umfang und Häufigkeit in den USA

Politischer Extremismus hat in den letzten zwei Jahren in den USA erheblich zugenommen, was auf die Verschärfung bestehender politischer Spaltungen und die zunehmende Verbreitung von und den Zugang zu rechts- und linksextremen politischen Ansichten in der amerikanischen Gesellschaft zurückzuführen ist. Ein zunehmend unmoderiertes und parteiisches Umfeld in den sozialen Medien führt dazu, dass sich Einzelpersonen immer stärker radikalisieren bzw. radikalisiert werden. Da die derzeitige Regierung ihre spalterische Politik und Rhetorik wahrscheinlich nicht zurücknimmt, ist weiterer politisch motivierter Extremismus 2026 sehr wahrscheinlich.

- Der Einsatz der Einwanderungs- und Zollbehörde (ICE) und anderer Behörden zur Bekämpfung der illegalen Einwanderung, Kürzungen bei den Bundesbehörden und die wirtschaftlichen Auswirkungen der globalen Handelszölle werden die politische Polarisierung weiter vorantreiben. Aktivistische und extremistische Gruppen werden sich höchstwahrscheinlich weiterhin auf diese Themen und diejenigen, die sie fördern, umsetzen oder unterstützen, konzentrieren.
- Die landesweiten Aktionstage gegen die Regierungspolitik werden wahrscheinlich fortgesetzt und bieten Brennpunkte und Plattformen für potenziellen politischen Extremismus sowohl von Anti-Trump-Protestierenden als auch von Gegendemonstrierenden.
- Extreme Aktionen wie Attentate, Sabotageakte, Gewalt und schwerer Vandalismus werden mit ziemlicher Sicherheit weiterhin geplant werden, angetrieben durch aufrührerische Rhetorik, eine stark spaltende Politik und die zunehmende Normalisierung extremer Standpunkte in den Mainstream- und alternativen Medien.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Polarisierende Maßnahmen und Botschaften politischer Akteure werden zurückgefahren, um extremistischen Reaktionen entgegenzuwirken. Die Moderation in etablierten wie auch alternativen Medienkanälen verbessert sich, wodurch die individuelle Exposition gegenüber extremistischen Inhalten und Ideologien reduziert wird.	Verbesserung	Fernliegend (5 %)
Die politische Polarisierung hält auf dem aktuellen Niveau an und treibt weiterhin politischen Extremismus sowohl von links- und rechtsgerichteten als auch von randständigen Akteuren voran.	Baseline	Wahrscheinlich (70 %)
Die Regierung Trump verschärft ihren Kurs und hält in kontroversen Politikfeldern wie der Einwanderung an hardline-Maßnahmen fest. Aktivistengruppen werden zunehmend als ‚terroristische' Organisationen eingestuft, was Aktivisten in den Untergrund drängt und das Potenzial für Radikalisierung sowie extremistische Handlungen erhöht.	Verschlechterung	Unwahrscheinlich (25 %)

Handlungsempfehlungen

- Informieren Sie sich über die Lage der Proteste und Demonstrationen, die als Plattform für politischen Extremismus dienen könnten, insbesondere in Zeiten erhöhter politischer Aktivität, wie z. B. bei den Zwischenwahlen 2026.
- Erwägen Sie die Überprüfung von Portfolios, um alle Elemente zu identifizieren, die als mit einer politischen Partei/Gruppe/Bestimmung verbunden wahrgenommen und von extremistischen Akteuren ins Visier genommen werden könnten.
- Unternehmen wird empfohlen, ein umfassendes Verständnis der Trends in Bezug auf die Taktiken, Techniken und Prozeduren politischer Extremisten zu wahren, die Bedrohungsaktionen planen oder erfolgreich durchführen.

Indikatoren	Auswirkungen
— Politiker der etablierten Parteien äußern und verbreiten weiterhin extremistische Rhetorik. — Die Protestlandschaft ist nach wie vor stark ausgeprägt, wobei symbolische Ereignisse, wie z. B. landesweite Feiertage, als Brennpunkte für Unruhen dienen. — Umstrittene oder polarisierende Bestimmungen werden trotz politischer und öffentlicher Gegenreaktionen umgesetzt oder verstärkt. — Die Trump-Regierung führt Maßnahmen zum Schutz von Bundesvermögen vor politischer Gewalt ein. — Aktivistengruppen werden als terroristische Organisationen eingestuft, um die Strafverfolgung zu erleichtern.	— Unternehmen, denen Verbindungen zu politischen Initiativen nachgesagt werden, leiden unter Sicherheitsbedrohungen im Zusammenhang mit politischem Extremismus. — Die zunehmende politische Polarisierung und Radikalisierung wird das Risiko von Bedrohungen durch Insider erhöhen, insbesondere in Unternehmen, die kontroversen Themen nahestehen. — Das Vertrauen des Auslands in die US-Wirtschaftslage wird wahrscheinlich schwinden, solange der politische Extremismus stark bleibt. — Es ist sehr wahrscheinlich, dass ausländische Gegner die Normalisierung des politischen Extremismus ausnutzen, um ihn gegen Unternehmen in strategisch wichtigen Sektoren zu richten.

Verschiebung des US-Ansatzes vom „Krieg gegen den Terror“ zum „Krieg gegen das Verbrechen“

Die Trump-Regierung hat die militärischen Operationen der USA in den letzten Monaten des Jahres 2025 von der Terrorismusbekämpfung auf die Verbrechensbekämpfung verlagert. Eine Fortsetzung oder Eskalation dieses Ansatzes ist auch Anfang 2026 sehr wahrscheinlich. Während das US-Militär früher im Krieg gegen den Terror einen Ansatz zur Aufstandsbekämpfung verfolgte, verwendet die Trump-Regierung zunehmend die Bezeichnung „Terroristen“, um kriminelle Gruppen und Personen, die als Gegner der Ziele der US-Regierung angesehen werden, ins Visier zu nehmen. Dazu gehört die Einstufung mehrerer Drogenkartelle in Lateinamerika als ausländische terroristische Organisationen, ebenso wie ausländische und inländische linke Gruppen/Philosophien, einschließlich der Antifa in den USA und der Antifa Ost in Deutschland.

- Die Einstufung ausländischer und inländischer krimineller Gruppen als ausländische terroristische Organisationen ermöglicht es der Trump-Regierung, ihren Ansatz bei der Bekämpfung dieser Gruppen zu ändern und den Einsatz militärischer Mittel gegen strategische Ziele zu ermöglichen.
- Die Trump-Regierung hat zwar ihre Absicht bekundet, Ressourcen in die Bekämpfung der Kriminalität in den USA zu investieren, doch hat dies zu einer Zunahme der Angriffe auf ausländische organisierte Verbrecherbanden geführt, von denen viele jetzt als ausländische terroristische Organisationen gelten, sowie zu einer Zunahme von Razzien gegen oppositionelle Protestgruppen. Dies ermöglicht den USA den Zugriff auf erweiterte Ressourcen, um ausländische Gegner ins Visier zu nehmen, die als mitschuldig an kriminellen Aktivitäten gelten, einschließlich ausländischer Regierungen.
- Donald Trump wird wahrscheinlich weiterhin versuchen, die amerikanische Nationalgarde einzusetzen, um die Kapazitäten zur Verbrechensbekämpfung und Strafverfolgung in den Städten der USA zu erweitern. Sollten diese Einsätze zu innerstaatlichen bzw. internationalen Angriffen eskalieren, würde dies höchstwahrscheinlich rechtliche und verfassungsrechtliche Probleme nach sich ziehen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die US-Regierung schränkt die Nutzung der Bezeichnung „Terroristen“ als Vorwand zur Bekämpfung von kriminellen und aktivistischen Gruppen ein. Während einige kriminelle Gruppen als ausländische terroristische Organisationen eingestuft werden, werden die militärischen Aktivitäten der USA eingeschränkt.	Verbesserung	Sehr unwahrscheinlich (10 %)
Die Trump-Regierung stuft weiterhin ausländische kriminelle Gruppen als ausländische terroristische Organisationen ein, um den Einsatz militärischer Kräfte gegen inländische Gruppen, die als solche bezeichnet werden, zu erleichtern.	Baseline	Wahrscheinlich (70 %)
Die weit verbreitete Kriminalisierung von Oppositionsgruppen und Aktivisten führt zum Einsatz von militärischen Mitteln im In- und Ausland und fördert Unruhen und rechtliche Anfechtungen.	Verschlechterung	Unwahrscheinlich (20 %)

Handlungsempfehlungen

- Bewerten Sie die Exposition bzw. Abhängigkeit von den Lieferketten/Handelsrouten bestimmter Regionen und diversifizieren Sie bzw. minimieren Sie die durch geopolitische Ereignisse verursachten Unterbrechungen.
- Entwickeln Sie Notfallpläne für gestörte diplomatische Beziehungen und Zeiten erhöhter Bedrohung bzw. Unruhen und investieren Sie in Daten zu geopolitischen Risiken, um entstehende Konflikte zu überwachen, zu antizipieren und darauf zu reagieren.
- Informieren Sie sich über innen- und außenpolitische Beziehungen, da die Beziehungen der US-Politik und der Trump-Regierung sowohl das inländische als auch das ausländische Handelsumfeld beeinflussen können.

Indikatoren	Auswirkungen
— Fortgesetzte Einstufung ausländischer krimineller Vereinigungen als ausländische terroristische Organisationen, wodurch die US-Regierung einen Präzedenzfall für die Einstufung inländischer Vereinigungen schaffen würde. — Die Trump-Regierung setzt weiterhin die Nationalgarde ein, um gegen Proteste gegen die Regierung vorzugehen, und veröffentlicht Berichte, in denen die Kriminalisierung linker Aktivistengruppen gefordert wird. — Zunehmend hetzerische Rhetorik zwischen republikanischen und demokratischen Politikern, die zu weiteren Schuldzuweisungen für innenpolitische Probleme führt. — Gewalttätige Angriffe, die von ausländischen kriminellen Organisationen verübt werden, werden als terroristische Aktivitäten eingestuft, sodass die Regierung die Möglichkeit hat, dagegen vorzugehen.	— Ein zunehmend restriktives soziales Umfeld, in dem politische Opposition zunehmend kriminalisiert wird. — Unternehmen, die im Ausland tätig sind, werden zunehmend von negativen Einstellungen gegenüber der US-Regierung betroffen sein. — Ausländische kriminelle Gruppen, die als ausländische terroristische Organisationen eingestuft werden, werden immer gewalttätiger und radikaler, was möglicherweise Auswirkungen auf Unternehmen weltweit haben wird. — Der Druck der USA auf ausländische Regierungen wächst, sich an die Einstufung als ausländische terroristische Organisationen zu halten und kriminelle Aktivitäten linker Gruppen im Inland zu bekämpfen, was zu politischer Unsicherheit in den betroffenen Ländern führt.


NETHERLANDS
Amsterdam
Rotterdam
Hanover
Bielefeld
GERMANY
Essen
Dusseldorf
Cologne
Antwerp
Brussels
BELGIUM
Lille
English Channel
London
Frankfurt am Main
Mannheim
Luxembourg
Saarbrucken
Paris

Europa

5

Rekrutierung von Zivilisten verändert die Bedrohungslage in Europa

Feindliche Akteure nutzen zunehmend Zivilisten, sowohl unwissentlich als auch wissentlich, um ihre strategischen Ziele in europäischen Ländern voranzutreiben, wodurch sich das traditionelle Profil der Bedrohungsakteure verändert und die Zuordnung und Schutzmaßnahmen für Regierungen und Unternehmen erschwert werden. China wurde beschuldigt, seine Staatsangehörigen und dazu gezwungene Einzelpersonen zur Spionage gegen sensible Standorte einzusetzen. Russland hat Berichten zufolge Einzelpersonen rekrutiert, um kriminelle Handlungen wie Brandstiftung zu begehen oder Drohnen zu steuern, die auf kritische nationale Infrastrukturen abzielen, während der Iran beschuldigt wurde, französische und schwedische organisierte kriminelle Gruppen zu beschäftigen und pro-palästinensische Gruppen zu finanzieren, um seine Interessen im Ausland durchzusetzen.

- Der zunehmende Einsatz von Zivilisten durch Bedrohungsakteure wird wahrscheinlich durch die Bemühungen um die Zerschlagung traditioneller Spionagenetzwerke im Westen inmitten erhöhter geopolitischer Spannungen angeheizt, was höchstwahrscheinlich auch 2026 und darüber hinaus andauern wird, wenn die Spannungen weiterhin bestehen bleiben.
- Dieser Trend wird wahrscheinlich zu einer Zunahme von feindlicher Aufklärung, Sabotage und gezielten Angriffen führen, die für die Behörden immer schwieriger zu erkennen oder zu verhindern sind. Dies macht verstärkte Überwachungs- und Schutzmaßnahmen erforderlich, während Methoden der Fernrekrutierung den Bedrohungsakteuren operative Sicherheit bieten.
- Obwohl dieser Ansatz die Zuschreibung erschwert, wird er mit ziemlicher Sicherheit die geopolitischen Spannungen verschärfen und das Misstrauen der westlichen Staaten gegenüber Ausländern aus gegnerischen Ländern erhöhen. Es besteht auch die realistische Möglichkeit, dass sich dieser Verdacht auf Unternehmen erstreckt, die ebenfalls anfällig für Nötigung oder Ausbeutung sind.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Verbesserte Überwachung und Spionageabwehr verringern die Zahl der Zwischenfälle und verbessern die Zuschreibung von Angriffen. Das Misstrauen gegenüber Ausländern verringert sich und es kommt seltener zu Einsätzen/ Anschlägen.	Verbesserung	Unwahrscheinlich (25 %)
Die feindlichen Akteure setzen weiterhin Zivilisten ein, wobei es sporadisch zu Zwischenfällen kommt, die jedoch überschaubar bleiben.	Baseline	Unwahrscheinlich (25 %)
Die feindlichen Akteure nutzen zunehmend die Zivilbevölkerung aus, was zu einer Zunahme von Anschlägen führt. Die Zuschreibung von Anschlägen wird immer schwieriger, und die Unternehmen sind höheren Betriebs- und Sicherheitsrisiken ausgesetzt.	Verschlechterung	Wahrscheinlich (55 %)

Handlungsempfehlungen

- Verbessern Sie die Bedrohungserkennung und die Sicherheitsprotokolle an sensiblen Standorten, einschließlich verstärkter Cybersicherheitsmaßnahmen, Überwachung, Mitarbeiterüberprüfung und Zugangskontrollen.
- Führen Sie regelmäßig umfassende Mitarbeiterschulungen zu Social Engineering, Risiken von Nötigung und zum Erkennen verdächtiger Verhaltensweisen bei gleichzeitiger Förderung eindeutiger Meldewege für potenzielle Bedrohungen durch Insider durch.
- Überwachen Sie Aktivitäten gegnerischer Länder und neue Rekrutierungstaktiken, einschließlich Propagandakampagnen, und halten Sie sich auf dem Laufenden, was die Einhaltung von Vorschriften und Bestimmungen im Zusammenhang mit auf Zivilisten abzielenden Bedrohungen betrifft.

Indikatoren	Auswirkungen
— Zunahme von Sabotage-/Spionagevorfällen, die sich gegen sensible Regierungs-/Wirtschaftsstandorte richten. — Zunahme gezielter Angriffe auf regimekritische Gemeinschaften oder Gemeinschaften, die als feindlich gegenüber gegnerischen Ländern angesehen werden. — Online-Inhalte zielen mit ihrer Propaganda/ Rekrutierung zunehmend auf Zivilisten ab, insbesondere auf verschlüsselten Plattformen. — Zunahme der Verhaftungen von Zivilisten, die Verbindungen zu staatlichen Akteuren haben sollen, auch wenn sie nicht ideologisch motiviert sind. — Zunahme von Angriffen mit eingeschränkter Komplexität, einschließlich des verstärkten Einsatzes leicht zugänglicher ziviler Drohnentechnologie zur Störung kritischer Infrastrukturen und zur Durchführung feindlicher Aufklärungsmaßnahmen.	— Unterbrechungen der kritischen Infrastruktur, der Lieferketten und der Geschäftskontinuität werden immer häufiger und lassen sich immer schwerer verhindern. — Für Unternehmen entstehen höhere Kosten für Sicherheit und Einhaltung von Vorschriften und sie sind einer erhöhten Gefahr von Angriffen durch Insider ausgesetzt. — Das Risiko von Reputationsschäden nimmt durch das Durchsickern sensibler Informationen und die Wahrnehmung von Sicherheitsmängeln zu. — Erhöhte Spannungen nach Zwischenfällen zwischen Ländern stören die Wirtschaftsbeziehungen und führen zu Maßnahmen gegen ausländische Unternehmen aus den verfeindeten Ländern, die deren Geschäftstätigkeit und Marktzugang behindern.

Zunahme der migrantenfeindlichen Stimmung in ganz Europa

Die zunehmende illegale Migration in Europa hat in der Öffentlichkeit heftige Gegenreaktionen ausgelöst und die Stimmung gegen Migranten in der gesamten Region geschürt – ein Trend, der sich 2026 noch verschärfen dürfte. Dieser Wandel geht mit einem Anstieg der rechten Rhetorik einher, wobei viele rechte Gruppen die zunehmende Migration als zentrales politisches Thema darstellen. Infolgedessen haben mehrere europäische Regierungen Maßnahmen zur Bekämpfung der illegalen Einwanderung ergriffen, die sowohl die öffentliche Meinung als auch den politischen Diskurs weiter spalten.

- Rechte/rechtsextreme Gruppen werden wahrscheinlich weiterhin Proteste organisieren, um Druck auf die europäischen Regierungen auszuüben, damit sie sich mit der illegalen Migration befassen, insbesondere wenn die Einwanderungszahlen weiter steigen.
- Die zunehmende politische Polarisierung und das Aufkommen alternativer Medien werden wahrscheinlich dazu führen, dass gegnerische Gruppen vermehrt feindliche Aktionen durchführen. Organisierte Proteste werden wahrscheinlich zu Gegendemonstrationen führen, was das Risiko von Zusammenstößen zwischen gegnerischen Gruppen bzw. Sicherheitskräften erhöht.
- Proteste gegen die Einwanderung werden weiterhin von hochrangigen Persönlichkeiten unterstützt und besucht werden, was zu einer erhöhten Teilnehmendenzahl führt. Diese Veranstaltungen werden wahrscheinlich zusätzlichen Auftrieb erhalten, wenn sie auf Vorfälle reagieren, in die angeblich Migranten verwickelt sind, insbesondere wenn die Straftaten gewalttätiger oder sexueller Natur sind. Die Spannungen können durch Störungen der Informationsversorgung seitens feindlich gesinnter Länder und Gruppen von Bedrohungsakteuren angeheizt werden.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die Häufigkeit und Intensität von Gewalt und Unruhen im Zusammenhang mit Migrationsströmen nehmen ab, wenn die Regierungen die damit verbundenen Probleme lösen.	Verbesserung	Sehr unwahrscheinlich (15 %)
Migrationsfeindliche Proteste und Unruhen eskalieren in ganz Europa weiter, wobei angebliche kriminelle Aktivitäten im Zusammenhang mit Migranten als Brennpunkte für öffentlichkeitswirksame Demonstrationen dienen.	Baseline	Realistische Möglichkeit (45 %)
Zunahme der gewalttätigen Rhetorik nach aufsehenerregenden Straftaten, in die Migranten verwickelt sind, was einwanderungsfeindliche Gruppen dazu veranlasst, formellere und komplexere Netzwerke zu bilden, um gemeinsame Aktionen zu koordinieren.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

- Informieren Sie sich über geplante Proteste in der Nähe von Betriebsstätten und entwickeln Sie Reaktionspläne zur Bewältigung von Szenarien, einschließlich der Verbesserung von Sicherheitsmaßnahmen an Standorten und der Umsetzung von Strategien zur Minimierung von Betriebsunterbrechungen.
- Stimmen Sie sich mit den örtlichen Strafverfolgungsbehörden ab, wenn große Demonstrationen in der Nähe von Geschäftsstandorten erwartet werden.
- Vermeiden Sie öffentlichkeitswirksame Botschaften des Unternehmens zu politischen Positionen, insbesondere, wenn es um Migration geht.
- Behalten Sie den politischen Kalender im Auge und achten Sie auf die Gefahr von Unruhen, die sich daraus ergeben können.

Indikatoren

- Verstärkte Proteste in den europäischen Ländern, die von steigender illegaler Migration betroffen sind, beeinflusst von einer migrationsfeindlichen Stimmung.
- Versuche, Grenzkontrollen und asylpolitische Maßnahmen zu reformieren, scheitern und können eine große Zahl illegaler Migranten nicht von der Einreise nach Europa abhalten.
- Rechte/rechtsextreme Gruppen gewinnen weiter an Wählerstimmen, was zum Teil auf ihre entschiedene Haltung zur illegalen Migration zurückzuführen ist.
- Regierungen führen politische Maßnahmen und Vorschriften ein, darunter Einschränkungen von Protesten und verschärfte Strafen, um störende und gefährliche Aktionen einzudämmen.

Auswirkungen

- Groß angelegte Proteste und Zusammenstöße mit Sicherheitskräften werden wahrscheinlich die Transportwege, die Mobilität der Mitarbeitenden und die Lieferketten stören.
- Bei Demonstrationen in der Nähe des Standorts eines Unternehmens besteht die Gefahr, dass es zu Gewalttätigkeiten oder Sachbeschädigungen kommt.
- Mitarbeitende mit Migrationshintergrund sind in den von den Protesten betroffenen Gebieten oder in deren Umgebung möglicherweise einem erhöhten Sicherheitsrisiko, Schikanen oder Diskriminierungen ausgesetzt.
- Eskalierende soziale Spannungen werden das Engagement von Interessengruppen für Unternehmen in Europa wahrscheinlich erschweren, insbesondere für Unternehmen in politisch sensiblen Sektoren.

Europäische Regierungen während des wirtschaftlichen Wandels unter finanziellem Druck

Zahlreiche europäische Länder sehen sich aufgrund hoher Staatsausgaben, demografischer Trends und geopolitischer/geoökonomischer Herausforderungen einem zunehmenden Steuerdruck ausgesetzt, der die langfristigen Wirtschaftsaussichten und den sozialen Zusammenhalt in der Region gefährdet. Die politischen und wirtschaftlichen Spannungen zwischen den europäischen Ländern und China in Verbindung mit den angekündigten Plänen, sich weiter von Russlands natürlichen Ressourcen unabhängig zu machen, sowie andere sich abzeichnende Trends wie die Zunahme einer protektionistischen Wirtschaftspolitik und die unberechenbare Wirtschaftspolitik der USA machen es wahrscheinlich, dass sich dieser Trend 2026 und darüber hinaus fortsetzen wird.

- Die geplanten Maßnahmen zum Abbau des Haushaltsdefizits und der Staatsverschuldung Frankreichs haben 2025 zu politischer Instabilität und sozialen Unruhen geführt. Im September und Oktober fanden mehrere Massenkundgebungen und Streiks mit Hunderttausenden Teilnehmenden statt. Es ist wahrscheinlich, dass die Umsetzung ähnlicher Sparmaßnahmen in anderen europäischen Ländern als Brennpunkt für Unruhen dienen wird.
- Laut Berichten vom 17. Oktober erwägt die Europäische Kommission, individuelle Reformen für die Mitgliedstaaten als Teil eines Plans zur Bindung von Rentenreformen an eine zentrale Finanzierung im Haushalt 2028 zu erlassen, um das Steuerrisiko zu verringern, das durch die alternde Bevölkerung in der EU entsteht.
- Die EU-Mitgliedstaaten müssen nationale Diversifizierungspläne vorlegen, in denen sie darlegen, wie sie die direkten und indirekten Importe von russischem Öl und Gas bis zum 1. März 2026 einstellen wollen, während andere Sanktionen im Laufe des Jahres in Kraft treten.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Europäische Staaten setzen fiskalische Reformmaßnahmen um, während sich das makroökonomische Umfeld infolge rückläufiger geopolitischer Unsicherheiten und geringerer internationaler Wettbewerbsintensität verbessert.	Verbesserung	Sehr unwahrscheinlich (20 %)
Staaten ergreifen Maßnahmen zur Reduzierung ihrer fiskalischen Defizite, jedoch verschärfen makroökonomische und geopolitische Rahmenbedingungen die fiskalen Belastungen, was zu politischen Herausforderungen und gesellschaftlichen Unruhen führt.	Baseline	Wahrscheinlich (65 %)
Europäische Länder sind nicht in der Lage, fiskalische Reformen umzusetzen, und die wirtschaftlichen Rahmenbedingungen verschlechtern sich infolge geopolitischer Entwicklungen weiter.	Verschlechterung	Unwahrscheinlich (15 %)

Handlungsempfehlungen

- Beurteilen Sie die Wahrscheinlichkeit, dass der aktuelle Geschäftsbetrieb, Verträge oder Partnerschaften durch geplante oder zukünftige Sparmaßnahmen beeinträchtigt werden, und bewerten Sie deren Exposition.
- Integrieren Sie makroökonomische und geopolitische Indikatoren in die regelmäßige Risikoüberwachung und überwachen Sie diese proaktiv, um Anzeichen von Instabilität aufgrund von Unterbrechungen der Lieferkette und politischen Veränderungen zu erkennen.
- Suchen Sie nach Lieferketten in stabileren Ländern und beziehen Sie Umwelt-, Sozial- und Governance-Kriterien, politische und Kreditrisikokriterien in die Auswahl und Überwachung von Lieferanten ein.

Indikatoren

- Die EU weist Mitgliedstaaten an, weitere Maßnahmen gegen Haushaltsdefizite und hohe Staatsverschuldung zu ergreifen.
- Länder ergreifen Maßnahmen zum Abbau des Finanzdefizits, darunter Änderungen des Renteneintrittsalters, Kürzungen von Sozialprogrammen und Abbau von Rentenprogrammen.
- Die wirtschaftlichen Beziehungen zwischen den europäischen Ländern und den USA verschlechtern sich kurzfristig, wahrscheinlich infolge politischer Streitigkeiten.
- Länder genehmigen ihre jährlichen Haushalte nicht.
- China kündigt neue Forschungen an, die Branchen im Zusammenhang mit dem europäischen Handel betreffen oder sich gegen bestimmte europäische Importeure richten.

Auswirkungen

- Die wirtschaftlichen Bedingungen werden mit Sicherheit einen erheblichen Einfluss auf die politische Landschaft der Region haben, wobei eine Verschlechterung der Lage die Unterstützung für radikale bzw. Randparteien fördern wird.
- Sparmaßnahmen und andere Steuerreformen prägen die Unternehmenslandschaft in der Region und beeinflussen die langfristige Planung.
- Gewerkschaftsproteste/Streiks in Ländern der Region nehmen in Häufigkeit und Intensität zu.
- Erhöhte Wahrscheinlichkeit von Massenentlassungen und Arbeitsplatzverlusten in verschiedenen Branchen.

Wildcards

Platzen der KI-Blase destabilisiert globale Märkte

Die steigende Bewertung von Unternehmen, die mit künstlicher Intelligenz in Verbindung stehen, weckt zunehmend die Befürchtung, dass sich die Branche in einer Blase befindet. Viele ziehen bereits Parallelen zur Dot-Com-Blase, die um die Jahrtausendwende entstand und zu einem schweren Marktabsturz führte. Die sieben größten Unternehmen – Alphabet, Amazon, Apple, Meta, Microsoft, Nvidia und Tesla – erreichen zusammen eine Marktkapitalisierung von rund 21,5 Billionen US-Dollar, was etwa 35 % der gesamten Marktkapitalisierung im November 2025 entspricht. Sie verzeichnen trotz dieser Bedenken weiterhin steigende Investitionen, was vor allem auf die gesteigerte Produktivität und das prognostizierte Wirtschaftswachstum zurückzuführen ist, die KI-Technologien versprechen.

- Nvidia, ein wichtiger Akteur, hat einen Marktwert von ca. 5 Billionen US-Dollar, mehr als das BIP Japans. Das bedeutet, dass kleine Bewertungsänderungen, die durch Ereignisse wie verpasste Gewinnmitteilungen oder regulatorische Änderungen verursacht werden, zu erheblichen Marktschwankungen auf den globalen Märkten führen können.
- Investoren haben darauf hingewiesen, dass viele Hyperscale-Unternehmen die Kosten für Grafikprozessoren über fünf bis sechs Jahre verteilen, obwohl Nvidia neue Architekturen herausbringt, durch die der Wert der vorherigen Generationen viel schneller herabgesetzt wird. Diese Praxis wird als eine der häufigsten Betrügereien der Neuzeit bezeichnet.
- Die Bewertung der Branche wurde zum Teil durch die von mehreren Unternehmen eingegangenen Investitionsverpflichtungen vorangetrieben, die deutlich höher sind als ihre derzeitigen Jahreseinnahmen. Der Umsatz von OpenAI wird für 2025 auf ca. 20 Milliarden US-Dollar geschätzt, aber das Unternehmen hat sich verpflichtet, zwischen 2025 und 2032 ca. 1,4 Billionen US-Dollar in Unternehmen wie AWS, Microsoft und Oracle zu investieren.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Unternehmen verlangsamen die Kreditaufnahme zur Finanzierung von KI, was zu einer diversifizierteren Marktkapitalisierung und einer geringeren Volatilität in Bezug auf den Einfluss von KI führt und dazu beiträgt, ein Platzen der Blase zu vermeiden.	Verbesserung	Unwahrscheinlich (15 %)
Die Spekulationsblase wächst weiter und verschärft den Druck auf die Finanzmärkte, was zu mehr Risiko, Volatilität und Unsicherheit führt.	Baseline	Realistische Möglichkeit (40 %)
Die Bewertung von mit KI in Verbindung stehenden Unternehmen steigt weiter an, ohne dass größere technologische Durchbrüche oder signifikant höhere Einnahmen zu verzeichnen sind, was schließlich zu einem Marktabsturz führen könnte.	Verschlechterung	Realistische Möglichkeit (40 %)

Handlungsempfehlungen

- Arbeitskräfte müssen geschult werden, um die Volatilität der Märkte abzumildern und eine langfristige Widerstandsfähigkeit zu gewährleisten, indem menschliche Fähigkeiten wie ethisches Denken und komplexe Problemlösungen gefördert werden.
- Diversifizieren Sie das Anlagenportfolio mit anderen Technologien, die auf die Verbesserung der operativen Fähigkeiten abzielen und die betrieblichen Auswirkungen des Verlusts des Zugangs oder erheblicher Kostensteigerungen für KI-Fähigkeiten abmildern.
- Achten Sie auf schwankende KI-Marktsignale und Änderungen der Finanzregulierung, um Notfallpläne zu erstellen, die die Gefahr eines Zusammenbruchs verringern.

Indikatoren	Auswirkungen
— Geringeres Vertrauen bei Technologieunternehmen und Investoren. — Die Bewertungen steigen weiter und führen zu einem neuen, nachhaltigen Markt, der sich auf Technologien konzentriert. — Die Unternehmen aus der Gruppe der sieben größten Unternehmen verfehlen Gewinn- und Umsatzziele, was die Marktvolatilität erhöht. — Unternehmen im Bereich KI führen Massenentlassungen durch oder ergreifen andere Kostensenkungsmaßnahmen. — Die wirtschaftlichen Bedingungen verschlechtern sich und haben höhere Zinssätze zur Folge. — Unternehmen bitten Regierungen um wirtschaftliche Unterstützung oder Schutz, um ihre Nachhaltigkeit zu gewährleisten.	— Eine wirtschaftliche Rezession wirkt sich negativ auf das Bruttoinlandsprodukt, die Beschäftigungsquote, den Lebensstandard und die Sparpläne aus. — Die künftige technologische Entwicklung wird sich verzögern, da das Vertrauen in hochentwickelte Technologien möglicherweise weithin verloren geht. — Es kommt zu öffentlichen Unruhen, die auf eine verstärkte Ablehnung von KI und des Finanzsektors zurückzuführen sind. — Verschärfte Finanzvorschriften aufgrund von politischem und öffentlichem Druck, um künftige Zusammenbrüche zu verhindern.

Verschärfter geopolitischer Wettbewerb in der arktischen Region

Der Wettbewerb um die Kontrolle des Zugangs zu Ressourcen, Schifffahrtsrouten und strategischen Gebieten in der Arktis nimmt zu, da die Region aufgrund der globalen Erwärmung durch die Eisschmelze leichter zugänglich wird. Dies hat zu einer zunehmenden Militarisierung der Arktis geführt und die Spannungen zwischen konkurrierenden Ländern verstärkt. Größere globale Spannungen – insbesondere zwischen Russland, den USA und den skandinavischen Ländern – werden den Wettlauf um die Behauptung und Kontrolle wichtiger Routen und Standorte in der Region 2026 wahrscheinlich beschleunigen.

— Globale Mächte wie Russland und die USA konkurrieren zunehmend um die Kontrolle über die Arktis, vor allem durch Investitionen in Technologien, die den Zugang zur Region verbessern und Einfluss ausüben sollen. Darunter fallen beispielsweise Eisbrecher, wobei beide Länder versuchen, den Zugang zu neuen potenziellen Schifffahrtsrouten zu erweitern und diese zu nutzen.

— Die NATO-Länder führen immer häufiger gemeinsame militärische Übungen in der Arktis durch. Diejenigen Länder, die über arktisches Territorium verfügen, z. B. die skandinavischen Staaten, haben Partnerschaften mit Ländern ohne arktisches Territorium aufgebaut, um die Sicherheit als Reaktion auf die russischen Bemühungen um den Ausbau der militärischen Präsenz in der Region zu erhöhen.

— Territoriale Streitigkeiten, vor allem über Gebiete, von denen man annimmt, dass darin wichtige Mineralien und andere natürliche Ressourcen vorkommen, werden Berichten zufolge über die Belange der indigenen Bevölkerung gestellt. Das unterstreicht die Ineffizienz regionaler Institutionen wie des Arktischen Rates hinsichtlich ihrer Fähigkeit, die Rechte der Bewohner der Region zu schützen.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Bemühungen, schiffbare Routen zu finden, sind erfolglos oder werden als nicht praktikabel erachtet, wodurch das Interesse an der Arktis abnimmt. Länder mit Interessen in der Region suchen nach Wegen der Zusammenarbeit, beispielsweise durch Vereinbarungen über die Begrenzung der militärischen oder industriellen Präsenz.	Verbesserung	Sehr unwahrscheinlich (10 %)
Die Militarisierung der Arktis nimmt stetig zu, während russische Angriffe in der Grauzone immer häufiger auftreten. Der Wettbewerb um Gebiete wird durch die Entdeckung großer Rohstoffvorkommen oder strategisch wichtiger Standorte angeheizt.	Baseline	Wahrscheinlich (65 %)
Russland konzentriert sich weniger auf die Ukraine (entweder aufgrund eines Waffenstillstands oder eines Strategiewechsels) und verlagert seine Bemühungen auf die Ausweitung seines Einflusses in der arktischen Region, wodurch sich das Risiko einer militärischen Konfrontation erhöht.	Verschlechterung	Unwahrscheinlich (25 %)

Handlungsempfehlungen

— Unternehmen mit Interessen in der Arktis oder Skandinavien – einschließlich Lieferketten wie Schifffahrtsrouten – wird empfohlen, die geopolitischen Entwicklungen in der Region aufmerksam zu verfolgen.

— Bereiten Sie Notfallpläne infolge möglicher bewaffneter Konfrontationen und militärischer Auseinandersetzungen in der Arktis vor. Darunter können auch die Schließung oder Einschränkung wichtiger Handelsrouten fallen.

— Unternehmen, die mit Aktivitäten im Zusammenhang mit globalen Interessen und der Entwicklung der arktischen Gebiete in Verbindung stehen, sollten das Potenzial für Gegenreaktionen und negative Auswirkungen auf ihren Ruf abschätzen, die mit der Kritik indigener Bevölkerungsgruppen verbunden sind.

Indikatoren	Auswirkungen
— Glaubwürdige wissenschaftliche Einrichtungen und Studien weisen darauf hin, dass die Eisschmelze in der Arktis anhält oder sogar zunimmt. — Länder und Bündnisse mit Interessen in der Arktis kaufen oder bauen Anlagen, die zur Ausweitung oder Festigung ihrer Präsenz genutzt werden können (z. B. Eisbrecher). — Die Militärübungen der NATO und Russlands in der Arktis nehmen an Häufigkeit und Umfang zu. — Russische Aktionen in der Grauzone, die sich gegen regionale Wettbewerber richten, werden immer häufiger und komplexer. — Indigene Gemeinschaften in der Arktis bemühen sich verstärkt, auf Missstände aufmerksam zu machen und gegen das Vorgehen regionaler Konkurrenten zu protestieren.	— Unternehmen, die in der Arktis tätig sind, insbesondere solche in strategischen Branchen, sind wahrscheinlich dem Risiko ausgesetzt, durch Bedrohungen wie Sabotage ins Visier genommen zu werden. — Rechtsstreitigkeiten um umstrittene Gebiete werden die in der Region tätigen Unternehmen wahrscheinlich vor Herausforderungen stellen. — Unternehmen mit Interessen in der Arktis werden zur Zielscheibe für Aktivismus im Zusammenhang mit indigenen Bevölkerungsgruppen. — Die Militarisierung und potenzielle Eskalationen werden wahrscheinlich zu Bedenken von Investoren und zum Rückzug aus bestimmten arktischen Anlagen führen. — Eine verbesserte Infrastruktur entlang der arktischen Schifffahrtsrouten wird wahrscheinlich die abhängigen Lieferketten stärken.

Raumfahrt erhöht die Bedrohung für die nationale Sicherheit und Privatsektoren

Die zunehmende Abhängigkeit von weltraumgestützter Technologie – und die damit verbundenen Bemühungen von einzelnen Ländern, Einfluss und Kontrolle über den Weltraum auszuüben – wird 2026 wahrscheinlich Bedrohungen der nationalen Sicherheit und der Wirtschaft verstärken. Russland, China und die USA haben 2025 ihre weltraumgestützten militärischen Mittel erheblich ausgebaut, u. a. mit Antisatellitensystemen (ASAT) und Raketenabwehrsystemen. Während die weltraumgestützte Waffenarchitektur ein längerfristiges Ziel ist, wird die Bedrohung von Kommunikations- und Geolokalisierungsnetzwerken durch natürliche Phänomene und menschliches Eingreifen, z. B. durch die Kriegsführung in der Grauzone, die auf Satelliten abzielt, wahrscheinlich weiter zunehmen.

- Kommerzielle Satelliten werden höchstwahrscheinlich in die militärischen und Grauzonenplanungen einfließen, wodurch die Gefahr besteht, dass Systeme, die wichtige Dienste wie Kommunikation, Satellitenbilder und Navigations-/Geolokalisierungsdienste bereitstellen, gestört werden.
- Darüber hinaus setzt die zunehmende Abhängigkeit von hochsensibler Technologie Unternehmen mit ziemlicher Sicherheit dem Risiko von Auswirkungen aus, die mit Phänomenen wie der Sonneneinstrahlung verbunden sind, einschließlich Ausfällen und Systemschäden. Die nächste Phase höchster Sonnenaktivität wird für Anfang 2026 erwartet und ist durch Sonneneruptionen und koronale Massenauswürfe gekennzeichnet, was wiederum das Risiko von Ausfällen wichtiger Strom- und Kommunikationsinfrastrukturen erhöht.
- Ein internationales Abkommen zur Regelung der Entwicklung militärischer oder potenziell feindlicher weltraumgestützter Technologien ist unwahrscheinlich, was das Risiko eines Wettrüstens im Weltraum und damit verbundener Bedrohungen wie Aktionen in der Grauzone erhöht.

Szenario	Status des Szenarios	Eintritts-wahrscheinlichkeit
Die Großmächte treten in einen verbindlichen Dialog über die Einschränkung weltraumgestützter Angriffsmöglichkeiten, während das solare Maximum 2026 mit minimalen Auswirkungen vorübergeht.	Verbesserung	Unwahrscheinlich (10 %)
Die Länder bauen ihre weltraumgestützten Fähigkeiten weiter aus und versuchen mit einer Grauzonenkriegsführung, kritische nationale Infrastrukturen zu stören, während die Sonnenstrahlung zu vereinzelten Störfällen führt.	Baseline	Wahrscheinlich (70 %)
Ein globales/großflächiges Infrastrukturversagen tritt aufgrund eines größeren Verlusts von Satelliten ein, sei es durch direkte militärische Eingriffe, Aktionen in der Grauzone oder extreme Weltraumwetterereignisse.	Verschlechterung	Sehr unwahrscheinlich (10 %)

Handlungsempfehlungen

- Bewerten Sie die Auswirkungen, die mit dem Verlust von Systemen einhergehen, die von der Satellitentechnologie abhängig sind, insbesondere Konnektivität (sowohl Telefonie als auch Internet), Geolokalisierung und -verfolgung sowie Bildmaterial.
- Prüfen Sie alle Abhängigkeiten von Geräten, die empfindlich auf Spitzen in der Sonneneinstrahlung reagieren, und die Auswirkungen, die mit Ausfallzeiten oder Schäden an den oben genannten Geräten verbunden sind.
- Erwägen Sie die Durchführung von Tabletop-Übungen oder Wargaming für Szenarien wie einen großen geomagnetischen Sturm und die damit verbundenen Auswirkungen.

Indikatoren	Auswirkungen
— Die US-Weltraumstreitkräfte setzen ihre Kampfsysteme wie erwartet ein und China und Russland setzen weltraumgestützte und terrestrische ASAT-Instrumente ein. — Zunehmende geopolitische Spannungen aufgrund des Einsatzes oder der Entwicklung von weltraumgestützten Technologien (einschließlich Waffen). — Dienste, die auf Satellitentechnologie angewiesen sind, melden zunehmend Störungen. — Bodenterminals, die mit Satellitenfunktionen verbunden sind, melden eine Welle von versuchten Cyberangriffen. — Die Sonnenaktivität entspricht früheren Ereignissen während des solaren Maximums, einschließlich Sonneneruptionen und koronaler Massenauswürfe.	— Ausfälle von Navigations-/GPS-Systemen führen zu Verzögerungen bei Versand und Transport. — Ein Ausfall digitaler Systeme könnte den weltweiten Zahlungsverkehr zum Erliegen bringen und zu finanzieller Unsicherheit führen. — Der fehlende Zugang zu Satelliten, die mit kritischen nationalen Infrastrukturen verbunden sind, beeinträchtigt Notdienste und die Telekommunikation erheblich. — Die Unterbrechung der Überwachung ermöglicht militärische Operationen und verschlechtert die regionale Sicherheit. — Frühwarnsysteme für Unwetter und Naturkatastrophen werden unwirksam und behindern die Evakuierungs- und Notfallplanung.

Brennpunkte und wichtige Daten

2026
Brennpunkte und wichtige Daten

JANUAR

- **1. Januar**: Gründungstag von Taiwan
- **3. Januar:** Jahrestag des Attentats auf Qasem Soleimani
- **14. Januar:** Jahrestag der tunesischen Revolution
- **15. Januar:** Jahrestag des Terroranschlags in Ra'anana 2024
- **25. Januar**: Jahrestag der ägyptischen Revolution 2011

FEBRUAR

- **1. Februar:** Jahrestag des Militärputsches in Myanmar 2021
- **11. Februar:** Tag der Islamischen Revolution (Iran)
- **14. Februar:** Jahrestag der Proteste in Bahrain 2011
- **15. Februar:** Tag der Befreiung Afghanistans
- **15. Februar:** Jahrestag der libyschen Revolution 2011
- **20. Februar:** Jahrestag der marokkanischen Reformproteste 2011

MÄRZ

- **5. März:** Wahl zum Repräsentantenhaus in Nepal
- **15. März:** Jahrestag des Terroranschlags auf Moscheen in Christchurch 2019
- **17. März:** St. Patrick's Day
- **28. März:** al-Quds-Tag
- **30. März:** Eid al-Fitr

APRIL

- **1.–9. April:** Pessach
- **5. April:** Ostersonntag
- **14. April:** Jom haScho'a

MAI

- **1. Mai:** Tag der Arbeit
- **7.–10. Mai:** Jahrestag des indisch-pakistanischen-Konflikts
- **15. Mai:** Nakba-Tag
- **25. Mai:** Jerusalemtag

JUNI

- **1. Juni:** Parlamentswahl in Äthiopien
- **4. Juni:** Jahrestag des Tian'anmen-Massakers von 1989
- **4. Juni:** Hadsch-Wallfahrt
- **13.–24. Juni:** Jahrestag des iranisch-israelischen Konflikts
- **26. Juni:** Aschura

AMEA

JULI

— **24.–28. Juli:** Jahrestag des Grenzstreits zwischen Kambodscha und Thailand

AUGUST

— **14. August:** Pakistanischer Unabhängigkeitstag
— **15. August:** Indischer Unabhängigkeitstag

SEPTEMBER

— **21. September:** Jom Kippur
— **25. September:** Sukkot

OKTOBER

— **7. Oktober:** Dritter Jahrestag der Eskalation des Gaza-Israel-Konflikts
— **9.-19. Oktober:** Jahrestag des afghanisch-pakistanischen Konflikts
— **14. Oktober:** Jahrestag des Staatsstreichs in Madagaskar

NOVEMBER

— **2. November:** Jahrestag der Balfour-Deklaration
— **8. November:** Diwali
— **30. November:** Parlamentswahlen in Kirgisistan

DEZEMBER

— **5. Dezember:** Präsidentschaftswahl in Gambia
— **5.–12. Dezember:** Chanukka
— **11. Dezember:** Jahrestag der Resolution 194 der UN-Generalversammlung von 1948
— **22. Dezember:** Wahlen im Südsudan
— **25. Dezember:** 1. Weihnachtsfeiertag
— **31. Dezember:** Silvester

2026
Brennpunkte und wichtige Daten

JANUAR

- **1. Januar:** Neujahr
- **6. Januar**: Jahrestag des Sturms auf das Kapitol
- **7. Januar:** Jahrestag des Massakers von Juliaca
- **11.–17. Januar:** al-Aqsa-Woche
- **27. Januar:** Holocaust-Gedenktag
- **27. Januar:** Isra und Miraj

FEBRUAR

- **4. Februar:** Jahrestag des Militärputschs in Venezuela 1992
- **13.–14. Februar:** Shab-e-Barat
- **13.–18. Februar:** Karneval in Rio
- **14. Februar:** Jahrestag der Schüsse bei der Siegesparade der Kansas City Chiefs 2024
- **17. Februar:** Tag der Präsidenten
- **26. Februar:** Shivaratri

MÄRZ

- **17. März:** St. Patrick's Day
- **28. März:** al-Quds-Tag
- **30. März:** Eid al-Fitr

APRIL

- **1.–9. April:** Pessach
- **5. April:** Ostersonntag
- **12. April:** Parlamentswahl in Peru

MAI

- **1. Mai:** Tag der Arbeit
- **5. Mai:** Cinco de Mayo
- **15. Mai:** Nakba-Tag

JUNI

- **26. Juni:** Aschura

Nord- und Südamerika

JULI

— **4. Juli:** Amerikanischer Unabhängigkeitstag

AUGUST

— **6. August:** Bolivianischer Tag der Unabhängigkeit

— **30. August:** Parlamentswahl in Haiti

SEPTEMBER

— **10. September:** Erster Jahrestag der Ermordung von Charlie Kirk

— **20.–27. September:** Climate Week NYC 2026

OKTOBER

— **4. Oktober:** Parlamentswahl in Brasilien

— **7. Oktober:** Dritter Jahrestag der Eskalation des Gaza-Israel-Konflikts

NOVEMBER

— **2. November:** Jahrestag der Balfour-Deklaration

— **3. November:** Zwischenwahlen in den USA

— **8. November:** Diwali

DEZEMBER

— **5.–12. Dezember:** Chanukka

— **11. Dezember:** Jahrestag der Resolution 194 der UN-Generalversammlung von 1948

— **25. Dezember:** 1. Weihnachtsfeiertag

— **31. Dezember:** Silvester

2026
Brennpunkte und wichtige Daten

JANUAR

- **1. Januar:** Neujahr
- **7. Januar**: Jahrestag des Terroranschlags auf Charlie Hebdo 2015
- **19.–23. Januar:** Weltwirtschaftsforum
- **11.–17. Januar:** al-Aqsa-Woche
- **27. Januar:** Holocaust-Gedenktag
- **27. Januar:** Isra und Miraj

FEBRUAR

- **13. Februar:** Münchner Sicherheitskonferenz
- **13. Februar:** Jahrestag des Autoanschlags in München 2025
- **13.–14. Februar:** Shab-e-Barat
- **24. Februar:** Jahrestag der russischen Invasion in der Ukraine 2022
- **28. Februar:** Jahrestag der Eisenbahnkatastrophe von Tembi

MÄRZ

- **17. März:** St. Patrick's Day
- **28. März:** al-Quds-Tag
- **30. März:** Eid al-Fitr

APRIL

- **1.–9. April:** Pessach
- **3. April:** Parlamentswahl in Ungarn
- **5. April:** Ostersonntag

MAI

- **1. Mai:** Tag der Arbeit
- **9. Mai:** Tag des Sieges
- **15. Mai:** Nakba-Tag

JUNI

- **7. Juni:** Parlamentswahl in Armenien
- **26. Juni:** Aschura

Europa

JULI

— **14. Juli:** Französischer Nationalfeiertag

AUGUST

— **24. August:** Unabhängigkeitstag der Ukraine

SEPTEMBER

— **13. September:** Parlamentswahl in Schweden

OKTOBER

— **3. Oktober:** Parlamentswahl in Lettland
— **7. Oktober:** Dritter Jahrestag der Eskalation des Gaza-Israel-Konflikts

NOVEMBER

— **2. November:** Jahrestag der Balfour-Deklaration
— **8. November:** Diwali

DEZEMBER

— **5.–12. Dezember:** Chanukka
— **11. Dezember:** Jahrestag der Resolution 194 der UN-Generalversammlung von 1948
— **25. Dezember:** 1. Weihnachtsfeiertag
— **31. Dezember:** Silvester

Kontakt

intelligence@securitas.com