

# world of risk

## Aktuelle Informationen aus der Welt von Chance und Risiko

heroldconsult

Nr. 122/03.26

### Zu dieser Ausgabe

*Lieber Leser,*

der Global Risks Report 2026 des Weltwirtschaftsforums verdeutlicht, dass geopolitische, ökonomische und technologische Entwicklungen direkte Auswirkungen auf Lieferketten, Märkte, Investitionen und Kostenstrukturen haben und von Unternehmen eine strategische Neuausrichtung ihres Risiko- und Nachhaltigkeitsmanagements verlangen.

Nach einer aktuellen Umfrage des Deutschen Reiseverbands wurden bereits 70 Prozent der befragten Dienstreisenden Opfer eines digitalen Angriffs. Fast ein Viertel davon sogar mehrfach. Ein zentrales Risiko sind ungesicherte öffentliche Netzwerke in Flughäfen, Hotels oder Cafés. Für die Münchner Rück könnten sich bis 2028 die weltweiten Schäden durch Cyberangriffe auf rund 14 Billionen US-Dollar summieren.

Fehlentscheidungen sind nicht nur klassische Unternehmen stark belasten, sondern auch die tw. schon börsennotierten Fussballvereine, v. a. bei Transfers. Andererseits bieten erfolgreiche Transfers auch diverse Chancen, z. B. sportlich ambitionierte Ziele zu erreichen oder Einnahmen zu steigern. Vor diesem Hintergrund wird ein strategisches Risikomanagement im Profifußball, besonders im Zusammenhang mit Spielertransfers, zunehmend wichtiger.

Mit dem Einsatz künstlichen Intelligenz, eröffnen sich lt. KPMG neue Möglichkeiten Risiken schneller zu identifizieren und zu steuern und bieten Unternehmen die Chance, Prozesse zu optimieren und zukunftssicher zu gestalten. Geopolitische und geoökonomische Spannungen und Cyberattacken verdeutlichen die zunehmende Komplexität von Risiken für Unternehmen,

Während die KI-Einführung in Unternehmen rasant voranschreitet, hinken Sicherheit und Kontrolle dramatisch hinterher. Neue Studien und Branchenkonferenzen zeigen eine gefährliche Lücke zwischen technologischem Fortschritt und Risikomanagement. Mit den nahenden Fristen des EU KI-Gesetzes wird der Handlungsdruck für deutsche Firmen immer größer.

Eine gute Nachricht für die Wirtschaft lautet: Die Prämien in der Industrieversicherung haben einen festen Abwärtstrend ausgebildet. Gute Zeit, um neu zu verhandeln, findet der Makler Marsh.

Hier wie auch in anderen Themen freut mich schon jetzt der Dialog, vielleicht gar die Mithilfe zur Lösung mit Ihnen

*gls*  
*Joel Ford*

## Themen dieser Ausgabe

### I. Risiken

#### Gefahren

- The Global Risks Report 2026 (WEF)
- Cyber-Risiko Geschäftsreisen: 70 Prozent wurden bereits Opfer
- Munich Re: Warnung – 14 Billionen Dollar Risiko
- Chancen- und Risikoanalyse im Profifußball

### II. Risikomanagement

- Der Einsatz von künstlicher Intelligenz im Risikomanagement
- Risikomanagement: Die Bedrohungslage wird vielschichtiger
- KI-Risikomanagement: Unternehmen steuern blind in die KI-Revolution

### III. Versicherung: Prämien in der Industrierversicherung im Abwärtstrend

## I. Risiken

### Gefahren

#### The Global Risks Report 2026 (WEF)

Q. [www.marsh.com](http://www.marsh.com) vom 15.01.2026

Globale Risiken werden für Unternehmen zunehmend wirtschaftlich relevant. Der Global Risks Report 2026 des Weltwirtschaftsforums (WEF) zeigt, dass geopolitische, ökonomische und technologische Entwicklungen nicht länger abstrakte Szenarien bleiben, sondern direkte Auswirkungen auf Lieferketten, Märkte, Investitionen und Kostenstrukturen haben.

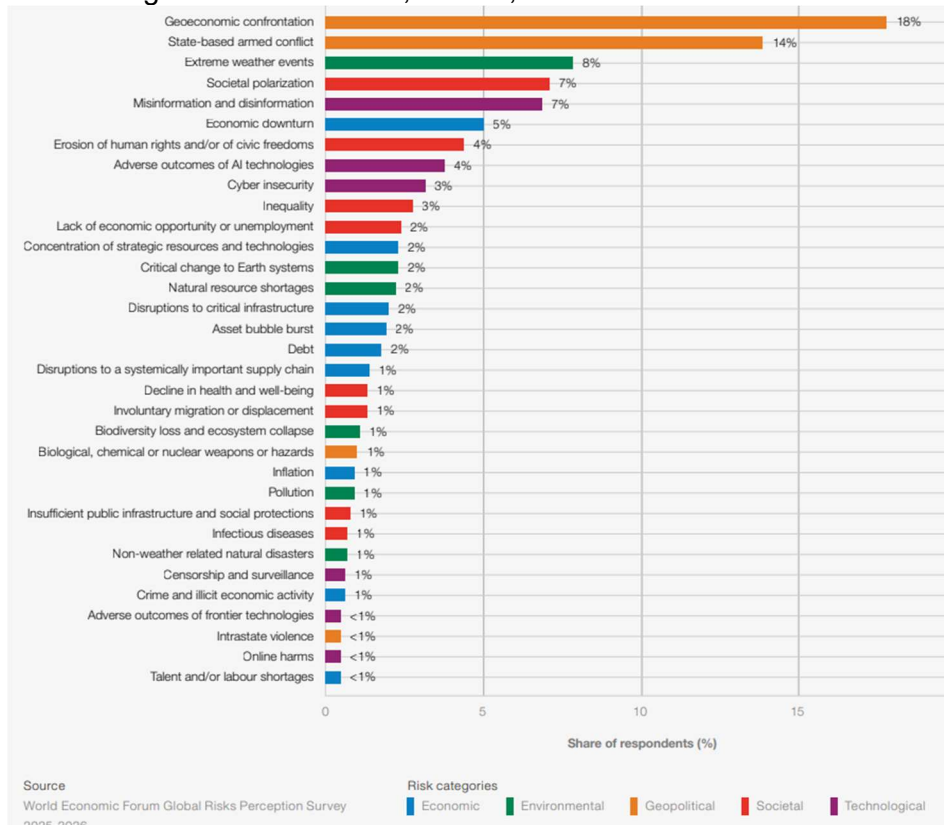


Abb.: Current Global Risk Landscape

Es zeigt sich eine deutliche Verschärfung des globalen Risikoumfelds und verlangt von Unternehmen eine strategische Neuausrichtung ihres Risiko- und Nachhaltigkeitsmanagements.

## **Cyber-Risiko Geschäftsreisen: 70 Prozent wurden bereits Opfer**

**Q: [www.ad-hoc-news.de](http://www.ad-hoc-news.de) vom 09.02.2026**

Nach einer aktuellen Umfrage des Deutschen Reiseverbands (DRV) wurden bereits 70 Prozent der befragten Dienstreisenden Opfer eines digitalen Angriffs. Fast ein Viertel davon sogar mehrfach.

Die Bedrohung ist für die Betroffenen greifbar: Rund 60 Prozent der Vielreisenden schätzen das Cyber-Risiko auf Reisen als hoch ein. Die Zahlen unterstreichen, wie wichtig technische und verhaltensbasierte Schutzmaßnahmen sind – für Mitarbeiter und Unternehmen gleichermaßen.

Ein zentrales Risiko sind ungesicherte öffentliche Netzwerke in Flughäfen, Hotels oder Cafés. Hier können Angreifer den Datenverkehr leicht abfangen. Die Lösung ist ein Virtuelles Privates Netzwerk (VPN). Es baut einen verschlüsselten Tunnel für alle Daten auf – selbst in unsicheren Netzen.

Geschäftsreisende sind ein besonders attraktives Ziel für Cyberkriminelle – eine aktuelle Umfrage zeigt, dass 70 % der Dienstreisenden bereits Opfer digitaler Angriffe wurden. Unternehmen brauchen jetzt praxisnahe Schutzkonzepte: VPN, Verschlüsselung, 2FA und Endpoint-Protection. Der kostenlose E-Book-Leitfaden „Cyber Security Awareness Trends“ fasst aktuelle Bedrohungen, KI-Risiken und sofort umsetzbare Maßnahmen für kleine und mittlere Unternehmen zusammen.

Doch laut DRV schreiben nur 41 Prozent der Unternehmen die VPN-Nutzung verbindlich vor. Dabei ist sie nur eine von mehreren essenziellen Basismaßnahmen:

- Verschlüsselung der Gerätefestplatten bei Diebstahl
- Zwei-Faktor-Authentifizierung (2FA) für wichtige Konten
- Deaktivierung von Dateifreigabe und Bluetooth, wenn nicht benötigt

Bevor die Reise beginnt, sollten alle Geräte zudem vollständig aktualisiert sein. Veraltete Software ist eine der größten Sicherheitslücken.

Neben digitalen lauern auch physische Gefahren. Der einfachste Angriff ist der Diebstahl eines unbeaufsichtigten Laptops. Geräte sollten nie aus den Augen gelassen werden – auch nicht kurz.

Oft unterschätzt wird das „Shoulder Surfing“, das Mitlesen von Bildschirminhalten in Flugzeugen oder Bahnen. Hier helfen Blickschutzfolien. Sie sorgen dafür, dass nur die Person direkt vor dem Display etwas erkennt. Auch diskrete Telefonate sind wichtig: Vertrauliche Themen bespricht man besser nicht laut in der Öffentlichkeit.

Die Verantwortung liegt nicht allein beim Reisenden. Unternehmen müssen klare Richtlinien schaffen und sensibilisieren. Hier hapert es oft: 45 Prozent der Geschäftsreisenden fühlen sich nur teilweise über Cyber-Risiken informiert, 13 Prozent sogar kaum oder gar nicht.

Nur etwa die Hälfte der Firmen hat Vorgaben zur Passwortsicherheit (49 %) oder zur Nutzung von 2FA (53 %). Regelmäßige, praxisnahe Sicherheitsschulungen sind noch immer nicht Standard. Dabei sind geschulte Mitarbeiter die wichtigste „menschliche Firewall“.

Die fortschreitende Digitalisierung verschärft die Lage. Die Zunahme von Remote Work und die Nutzung von Künstlicher Intelligenz (KI) bringen neue Fallstricke. Mitarbeiter sollten keine vertraulichen Daten in öffentliche KI-Tools eingeben – der Datenschutz ist dort oft unklar.

Zukünftige Sicherheitskonzepte setzen auf „Advanced Endpoint Protection“ und die Möglichkeit, Geräte aus der Ferne zu löschen. Investitionen in klare Richtlinien, moderne Technologie und kontinuierliche Schulung werden zum Wettbewerbsvorteil. Sie schützen nicht nur Daten, sondern stärken auch das Vertrauen der Mitarbeiter.

## **Munich Re: Warnung – 14 Billionen Dollar Risiko**

**Q: deraktionär.de vom 25.03.2026**

Die Bedrohung durch Cyberkriminalität wächst rasant und rückt damit auch den Rückversicherer Munich Re verstärkt in den Fokus. Immer häufiger treffen hochprofessionelle Angriffe Unternehmen, Behörden und ganze Volkswirtschaften – mit teils enormen finanziellen Folgen. Das müssen Anleger des Rückversicherers dazu wissen.

Bis zum Jahr 2028 könnten sich die weltweiten Schäden durch Cyberangriffe laut Munich Re auf rund 14 Billionen US-Dollar summieren. Das wäre mehr als die kombinierte Wirtschaftsleistung von Deutschland, Japan und Indien.

Besonders dynamisch entwickelt sich der Bereich Ransomware. Die Zahl öffentlich erfasster Angriffe ist laut Munich Re im vergangenen Jahr um fast 50 Prozent gestiegen – und auch im Jahr 2026 setzt sich diese Entwicklung ungebrems fort. Unternehmen, Behörden und ganze Volkswirtschaften geraten zunehmend unter Druck.

Die Experten des Rückversicherers beobachten einen strukturellen Wandel: Cyberkriminalität entwickelt sich zu einer hochorganisierten, arbeitsteiligen Branche. Der Einstieg wird einfacher, da weniger technisches Know-how und Kapital nötig sind.

Ransomware-Angriffe gelten als besonders lukrativ. Kriminelle Netzwerke bieten mittlerweile komplette Baukastensysteme an – inklusive Geldwäsche-Tools, Marketingstrukturen und sogar „Kundensupport“ für Opfer. Nach der Zerschlagung großer Gruppen sind viele kleinere, schwerer zu verfolgende Einheiten entstanden. Das erhöht die Zahl der Angriffe und sorgt für stärkere Schwankungen im Schadenverlauf.

Hinzu kommt die technologische Aufrüstung der Angreifer. Deepfakes, Stimmenklone und synthetische Identitäten werden zunehmend eingesetzt, um Sicherheitsmechanismen zu umgehen. Betroffen sind nahezu alle Branchen – besonders häufig jedoch staatliche Einrichtungen sowie Industrie- und Technologieunternehmen.

Für Munich Re ergibt sich daraus ein zweischneidiges Bild: Einerseits wächst der Bedarf an Cyberversicherungen und damit das Prämienpotenzial. Andererseits steigen auch die Risiken durch schwer kalkulierbare Großschäden und eine zunehmende Volatilität.

Unter dem Strich dürfte Munich Re eher ein Profiteur des strukturell wachsenden Cybermarkts sein, sofern der Konzern die steigenden Risiken im Griff behält. Die starke Marktstellung, die Preissetzungsmacht und die professionelle Risikopolitik sprechen weiterhin für den Titel. Anleger halten daher weiter an der Aktie fest.

## **Chancen- und Risikoanalyse im Profifußball**

**Q: risknet.de vom 25.03.2026**

Der europäische Profifußball gilt sportlich gesehen weltweit als Leistungsmaßstab des modernen Fußballs. Zeitgleich stellt der europäische Profifußball einen der dynamischsten und volatilsten

Märkte im internationalen Sportgeschäft dar [vgl. Sparkasse, o. J.]. Der Markt ist durch schwankende Rahmenbedingungen geprägt (z. B. Auf- und Abstieg, Verletzungen, Sponsoreneinstieg und -ab sprung), wodurch Transferprozesse erheblich an Komplexität und Risiko gewinnen. Die hohe finanzielle und sportliche Volatilität zeigt sich insbesondere im Abstieg, welcher Millionen kosten kann (TV-Gelder, Sponsoren), oder in Verletzungen von Schlüsselspielern, welche ganze Saisonziele gefährden können. Zusätzlich steigen in den letzten Jahrzehnten nicht nur die Transferbeträge für einzelne Spieler kontinuierlich an, sondern auch die gesamten Transfersummen einzelner Vereine oder ganzer Ligen innerhalb einer Transferperiode [vgl. Sportschau 2025a]. Aufgrund dessen können Fehlentscheidungen bei Transfers immer größere Ausmaße – sowohl finanziell als auch sportlich – annehmen und Vereine immens belasten. Andererseits bieten erfolgreiche Transfers auch diverse Chancen, wie z. B. sportlich ambitionierte Ziele erreichen oder Einnahmen steigern zu können. Vor diesem Hintergrund wird ein strategisches Risikomanagement im Profifußball, besonders im Zusammenhang mit Spielertransfers, zunehmend wichtiger.

Während die Forschung und Literatur zwar tiefgehende Einblicke über die Funktionsweise des Transfermarktes oder Financial Fair Play bieten, wie auch umfassende Erkenntnisse zu ökonomischen Entwicklungen im Profifußball liefern, wird das Thema des Risikomanagements im Zusammenhang mit Transfers im Profifußball nur selten umfassend bzw. detailliert beleuchtet. Beispielsweise untersucht Huth [vgl. Huth 2011], wie derivative Finanzinstrumente genutzt werden können, um finanzielle Risiken von Fußballvereinen zu reduzieren. Darüber hinaus analysiert Henke [vgl. Henke 2003] verschiedene Versicherungsprodukte sowie deren Rolle im wirtschaftlichen Risikomanagement deutscher Profi-Fußballvereine. Des Weiteren hat Borussia Dortmund dem Aktiengesetz folgend bereits ein Risikomanagementsystem implementiert, welches ein konzernweites integriertes sowie systematisches Verfahren darstellt, bei dem Risiken fortlaufend identifiziert, bewertet, gesteuert und unabhängig kontrolliert werden. Jedoch werden im Rahmen der sechs Risikobereiche (strategische und volkswirtschaftliche Risiken, Personalrisiken, Wettbewerbsrisiken, Liquiditätsrisiken und ökologische Entwicklung), sämtliche Risiken, welche mit Transfers einhergehen, nur teilweise (als High-Priority-Risiken) betrachtet und nicht separat als zusätzlicher Bereich genauer beleuchtet [vgl. Borussia Dortmund GmbH & Co. KGaA 2025].

Der ausführlichen Artikel kann unter <https://www.risknet.de/themen/risknews/chancen-und-risikoanalyse-im-profifussball/> aufgerufen werden.

## **II. Risikomanagement**

### **Der Einsatz von künstlicher Intelligenz im Risikomanagement**

**Q. [www.kpmg.com/de](https://www.kpmg.com/de) vom 30.01.2026**

In Zeiten zunehmender wirtschaftlicher Unsicherheit gewinnt das Risikomanagement an Bedeutung. Ein effizientes Finanzrisikomanagement kann entscheidend sein, um finanzielle Risiken frühzeitig zu identifizieren, Gegenmaßnahmen zu ergreifen und so den Fortbestand eines Unternehmens zu sichern.

In unserer globalisierten Welt und einer vielfältigen Verzahnung von Wirkung und Gegenwirkung gewinnen operative Risiken an Bedeutung. Sie haben direkte Auswirkungen auf das Finanzrisikomanagement, insbesondere auf Marktrisiko, Kreditrisiko und Liquiditätsrisiko. Ein Beispiel dafür ist die Havarie der „Ever Given“, die den Suezkanal blockierte und die Weltwirtschaft beeinflusste.

Mit dem Einsatz moderner Technologien, insbesondere der künstlichen Intelligenz (KI), eröffnen sich neue Möglichkeiten, Risiken schneller zu identifizieren und zu steuern. KI-Technologien transformieren das Treasury und das Risikomanagement und bieten Unternehmen die Chance, Prozesse zu optimieren und zukunftssicher zu gestalten. Viele Unternehmen sind sich dessen bereits

bewusst. Unsere Studie „KI in Finance“ zeigt, dass fast 50 Prozent der befragten Unternehmen KI einsetzen, um Risiken schneller zu erkennen.

Im Finanzrisikomanagement geht es nicht darum, Risiken zu vermeiden, sondern sie frühzeitig zu erkennen und gezielt zu steuern – KI kann dabei zum entscheidenden Faktor werden.

Für das Finanzrisikomanagement bietet KI speziell in den Bereichen Identifikation von Risiken, Bewertung und Vorhersage von Risiken, Automatisierung und Effizienzsteigerung und Compliance sowie regulatorische Anforderungen wesentliches Potenzial.

Andererseits bringt der Einsatz von künstlicher Intelligenz im Finanzrisikomanagement auch spezifische Herausforderungen mit sich:

1. Datenqualität und -verfügbarkeit
2. Komplexität der Modelle und Erklärbarkeit
3. Überanpassung (Overfitting)
4. Abhängigkeit von der Technologie
5. Datenschutz und Datenethik

Letztlich ist aber der Einsatz von KI im Finanzrisikomanagement vielversprechend, da die relevanten Risiken gewissen Logiken unterliegen und dank moderner Treasury-Management-Systeme oft eine gute Datengrundlage vorhanden ist. Die nächsten Schritte für KI im Treasury könnten somit folgende sein:

- Datenqualität sicherstellen: Überprüfen und Verbessern der Qualität sowie Verfügbarkeit der Daten, um eine solide Grundlage für KI-Analysen zu schaffen.
- Mensch-KI-Interaktion optimieren: Implementieren einer effizienten Arbeitsteilung zwischen Risikomanager und KI-Systemen, um Routinetätigkeiten zu automatisieren und komplexe Analysen zu unterstützen.
- Schulungen durchführen: Schulung der Risikomanager im Umgang mit KI-Tools, um deren Potenzial voll auszuschöpfen und die Akzeptanz zu erhöhen.
- Compliance und Datenschutz gewährleisten: Sicherstellen, dass alle eingesetzten KI-Systeme den gesetzlichen und regulatorischen Anforderungen entsprechen und die Daten sicher verwaltet werden.

## Risikomanagement: Die Bedrohungslage wird vielschichtiger

Q: [www.dvz.de](http://www.dvz.de) vom 20.01.2026

Geopolitische und geoökonomische Spannungen, Cyberattacken und künstliche Intelligenz: Internationale Umfragen verdeutlichen die zunehmende Komplexität von Risiken für Unternehmen, auch in der Transport- und Logistikbranche. Ein Überblick:



Zuletzt hatten die Bedenken hinsichtlich der Handelspolitik abgenommen, wie die globale Führungskräfteumfrage von McKinsey zeigt. Während im Juni und September handelspolitische Veränderungen noch die am häufigsten genannte potenzielle Störung der Weltwirtschaft waren, galten zum Jahresende geopolitische Instabilität und Konflikte wieder als das größte Risiko. Auch die Inflation landet wieder unter den fünf größten wahrgenommenen Risiken, wobei sie am häufigsten in Nordamerika genannt wird.

## **KI-Risikomanagement: Unternehmen steuern blind in die KI-Revolution**

**Q: ad-hoc.news vom 25.03.2026**

Die rasante Einführung von KI in Unternehmen überholt Sicherheitskontrollen. Studien belegen Schatten-KI, neue Angriffsflächen und mangelnde Governance, während das EU-KI-Gesetz ab August 2026 voll durchgreift.

Während die KI-Einführung in Unternehmen rasant voranschreitet, hinken Sicherheit und Kontrolle dramatisch hinterher. Neue Studien und Branchenkonferenzen zeigen eine gefährliche Lücke zwischen technologischem Fortschritt und Risikomanagement. Mit den nahenden Fristen des EU KI-Gesetzes wird der Handlungsdruck für deutsche Firmen immer größer.

Seit August 2024 gelten bereits erste Teile der neuen EU-Regulierung, und viele Unternehmen riskieren unwissentlich Bußgelder bei der Nutzung von KI-Systemen. Dieser kostenlose Leitfaden zeigt Ihnen kompakt und verständlich, welche Pflichten für Ihr Unternehmen gelten und wie Sie die Anforderungen rechtssicher umsetzen. EU-KI-Verordnung kompakt: Jetzt kostenlosen Umsetzungsleitfaden sichern

Eine aktuelle Studie der Purple Book Community offenbart eine tiefe Kluft. Zwar behaupten 90 Prozent der befragten Cybersicherheitsmanager, einen Überblick über ihre KI-Nutzung zu haben. Gleichzeitig bestätigen oder vermuten jedoch 59 Prozent die Existenz von Schatten-KI in ihren Systemen. Dabei nutzen Mitarbeiter nicht genehmigte KI-Tools – eine massive Sicherheitslücke. Noch alarmierender: 70 Prozent der Organisationen haben bereits Schwachstellen durch KI-generierten Code in ihren Live-Systemen entdeckt. Das Entwicklungstempo der KI überholt schlichtweg die traditionellen Sicherheitsprüfungen.

Die Zahlen sind eindeutig: Über die Hälfte der Unternehmen (52 Prozent) setzt generative KI bereits voll oder teilweise ein. Das zeigt eine globale Studie von OpenText. Doch die notwendigen Kontrollmechanismen fehlen. Nur jedes fvierte Unternehmen hat eine vollständige KI-Reife in Sachen Cybersicherheit erreicht. Weniger als die Hälfte (43 Prozent) verfügt über eine risikobasierte Strategie zur Steuerung ihrer KI-Systeme. Unternehmen bauen also auf wackeligem Fundament – sie führen mächtige Technologien ein, ohne die passenden Sicherheitsvorkehrungen zu treffen.

Auf der RSA Conference 2026 rückte ein bisher übersehenes Risiko in den Fokus: der „GPU-Blindspot“. Moderne KI-Systeme laufen massiv auf Grafikprozessoren (GPUs). Herkömmliche Sicherheitstools überwachen jedoch vor allem CPUs und Betriebssysteme. Die Aktivitäten auf den GPUs bleiben für Sicherheitsteams unsichtbar. Damit entsteht eine komplett neue Angriffsfläche, die alte Tools nicht abdecken können. Die Branche reagiert: Laut einer Umfrage halten 62 Prozent KI-gestützte Abwehrtools für notwendig, und 73 Prozent planen, ihre Cybersecurity-Budgets zu erhöhen.

Angesichts neuer Angriffsflächen und verschärfter Gesetze sind über 70 % der deutschen Unternehmen unzureichend auf Cyberangriffe vorbereitet. Dieser Experten-Report enthüllt effektive Strategien, wie Sie Ihre IT-Sicherheit ohne Budget-Explosion stärken und sich gegen aktuelle Bedrohungen wappnen.

Der Druck bekommt ein festes Datum: Ab dem 2. August 2026 werden die meisten Verpflichtungen des EU KI-Gesetzes durchsetzbar. Das betrifft nicht nur EU-Firmen, sondern weltweit jedes Unternehmen, dessen KI-Systeme in der Union genutzt werden. Die Verordnung stuft KI-Anwendungen nach Risiko ein. Für Hochrisiko-KI gelten dann strenge Auflagen zu Dokumentation, Überwachung und Governance. Zwar wurden Fristen für bestimmte Hochrisiko-Systeme bis 2027/2028 gestreckt, doch die allgemeinen Pflichten und Verbote bleiben akut. Unternehmen müssen jetzt handeln.

Laut einer Analyse von Deloitte muss das Risikomanagement grundlegend neu gedacht werden. Es geht nicht mehr nur um Technik, sondern um Kultur und Prozesse. Die Experten fordern drei strategische Schritte: Unternehmen müssen ihre KI „besitzen“, indem sie Agenten intern entwickeln, um Transparenz zu gewährleisten. Compliance-Teams müssen von Routineaufgaben befreit und zu strategischen Risikoerkennern umfunktioniert werden. Und es braucht übergreifende Governance-Frameworks, um verschiedene KI-Systeme zu orchestrieren.

In Deutschland verschärft das neue KRITIS-Dachgesetz die Lage zusätzlich. Für kritische Infrastrukturen sind physische und digitale Resilienz nun eng verknüpft. Wer jetzt in proaktives KI-Risikomanagement investiert, handelt nicht nur aus Pflicht. Er baut Vertrauen bei Kunden auf und sichert sich einen klaren Wettbewerbsvorteil. Die Balance zwischen Innovation und Sicherheit wird zum entscheidenden Erfolgsfaktor der kommenden Jahre.

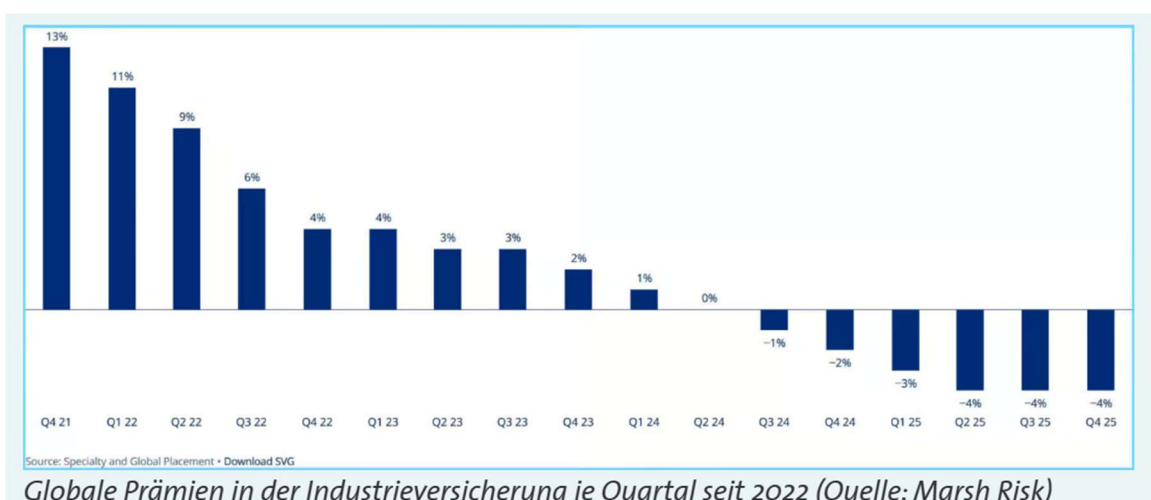
### III. Versicherung

#### Prämien in der Industrieversicherung im Abwärtstrend

Q: [www.pfefferminzia.de](http://www.pfefferminzia.de) vom 24.02.2026

Gute Nachrichten für die Wirtschaft: Die Prämien in der Industrieversicherung haben einen festen Abwärtstrend ausgebildet. Gute Zeit, um neu zu verhandeln, findet man beim Makler Marsh.

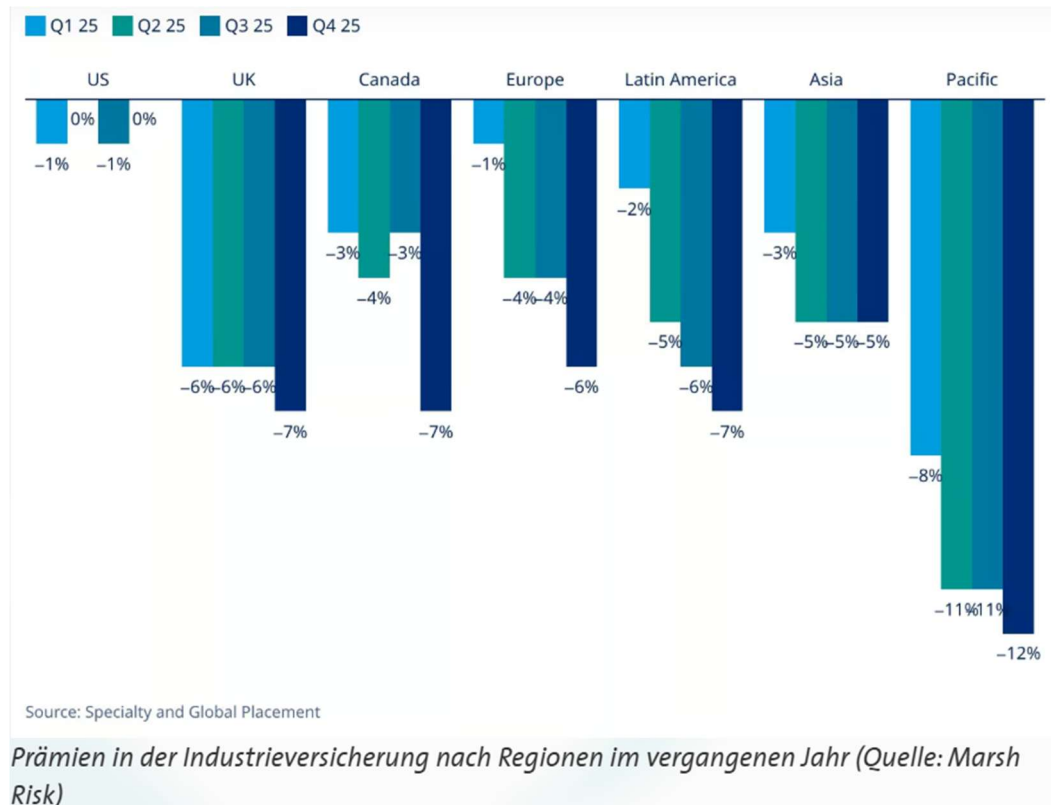
Marsh Risk beobachtet, dass inzwischen im sechsten Quartal in Folge die Prämien gesunken sind. Im vierten Quartal 2025 ging es um 4 Prozent hinab. Im zweiten und dritten Quartal lag der Schwund prozentual genau so hoch (siehe Grafik).



Warum passiert das ausgerechnet in einer Welt, in der vermeintlich alles teurer wird? Als Hauptgründe für den Rückgang der Prämienraten nennt Marsh den stärkeren Konkurrenzkampf unter den Versicherern, günstige Schadenentwicklung und die Rückversicherungskonditionen, verbunden

mit erhöhter Marktkapazität. Risiken werden also günstiger, und Versicherer kämpfen regelrecht darum, welche übernehmen zu können.

Doch die regionalen Unterschiede sind enorm. Während in den USA die Prämien im vierten Quartal im Schnitt auf der Stelle traten, ging es in der Pazifikregion um saftige 12 Prozent hinab. Es folgen Indien, Nah-Ost und Afrika (Imea) mit minus 10 Prozent. Weitere Werte zeigt die Grafik.



Für Industriekunden ist das natürlich eine tolle Sache, die sogar noch weitergehen könnte. So meint John Donnelly, Präsident für Global Placement bei Marsh Risk: „Ohne unvorhergesehene Ereignisse erwarten wir, dass sich dieser Trend im Jahr 2026 fortsetzt. In diesem Jahr dürften Kunden die Möglichkeit haben, Prämienraten zu reduzieren und umfassendere Bedingungen auszuhandeln, die die Leistungsfähigkeit ihrer Versicherungsprogramme verbessert, um so der zunehmenden Komplexität der Risiken gerecht zu werden.“

Kontakt: heroldconsult  
c/o Prof. Dr. Bodo Herold  
herold@heroldconsult.com  
www.heroldconsult.com  
Pfarrstr. 5, D 51399 Burscheid  
+49 2174 74803 0