



Finlex Markt Report

Oktober 2026 –

Cyber · Claims · Künstliche Intelligenz

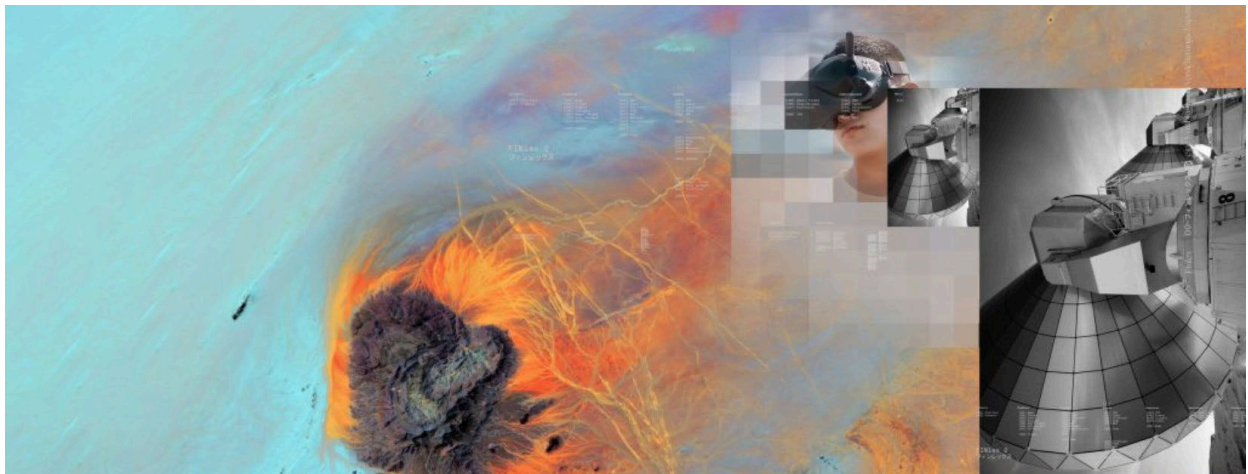
Marktbericht für Kooperationsmakler in Deutschland und Österreich

Auszug für BDVM Pressegespräch - kommentiert und erläutert von Dr. Sven Erichsen

Finlex Markt Report 2026

Inhaltsverzeichnis

Cyber.....	3
Stimmungsbild Cyber zum Renewal 2026/2027	3
Auswirkungen auf den Cyber-Markt Schadentrends, Bedrohungslage und Umfeld	4
Künstliche Intelligenz unterstützt die Angriffsseite messbar.....	5
Großschäden und Systemrisiko.....	6
Marktveränderungen durch Anbieter	7
Zeichnungsverhalten der Cyber-Versicherer	8
Besonderheiten des österreichischen Marktes in Cyber	9
Claims	11
Schadenentwicklung und -ausblick Cyber.....	11
Cyber – Schadenentwicklung	11
Cyber – Schadenausblick	12
Künstliche Intelligenz.....	14
Auswirkungen auf die Versicherungsbranche und Bedarf nach neuen Versicherungslösungen	14
KI in der Versicherungswirtschaft: breite Adoption, dünne Wertschöpfung.....	14
Aufsichtsrechtliche Erwartungen: KI-Governance ist prüfbar geworden.....	15
Neue Haftungsrisiken – und warum sie in der D&O ankommen.....	16
Neue Versicherungslösungen für KI-Risiken	17
KI in der Verteidigung – und was Unternehmen jetzt tun sollten	18
Autorenprofile.....	19

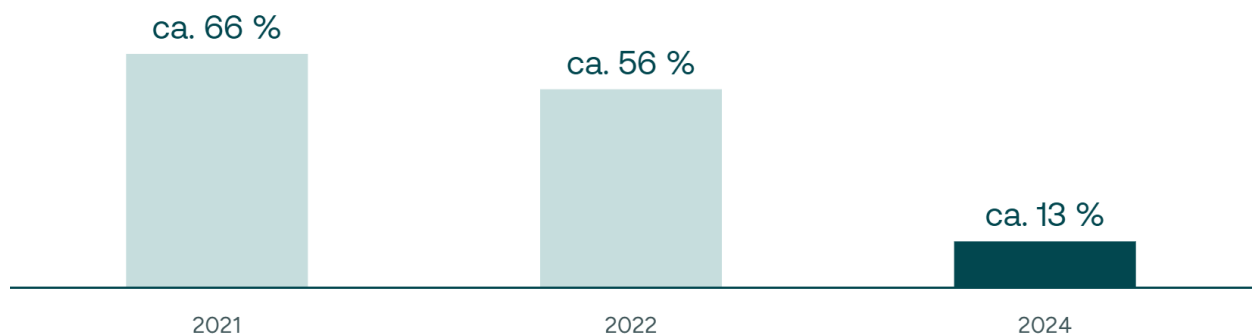


Cyber

Stimmungsbild Cyber zum Renewal 2026/2027

Die Cyber-Versicherung in der DACH-Region wächst weiter – aber sie wächst deutlich langsamer, was gleichzeitig die zentrale Veränderung gegenüber dem Vorjahr darstellt. Die BaFin-Cybermarktbefragung, veröffentlicht im April 2026, weist für das selbstständige Direktgeschäft 2024 nur noch rund 13 % Beitragswachstum aus – nach etwa 66 % (2021) und 56 % (2022); das übernommene Geschäft ging 2024 um rund 26 % zurück.¹ Die GDV-Zahlen für 2025 ergänzen dieses Bild auf Vertragsseite: Die Zahl der gewerblichen Cyberversicherungsverträge stieg um 15,7 % auf rund 157.000. Gleichwohl verfügen weiterhin nur rund 5 % der Unternehmen in Deutschland über eine Cyberversicherung. Das Wachstum beruht damit weiterhin wesentlich auf einer steigenden Marktdurchdringung bei insgesamt noch geringer Versicherungsdichte.²

Beitragswachstum im selbstständigen Cyber-Direktgeschäft



Quelle: BaFin-Cybermarktbefragung, April 2026

International bestätigt sich das Bild: Howden beziffert den Rückgang der Cyber-Raten auf 27 % seit Mitte 2022 und das globale Prämienwachstum auf aktuell rund 6 % pro Jahr – vor 2020 waren es 23 %.³ Munich Re taxiert das globale Marktvolumen auf rund 15 Mrd. USD (2025) mit einer Prognose von etwa 28 Mrd. USD für 2030 und beziffert das durchschnittliche Wachstum über den Zeitraum 2020 bis 2030 auf 15 % pro Jahr; für die

¹BaFin-Cybermarktbefragung, publiziert April 2026

² Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV), Statistiken zur deutschen Versicherungswirtschaft 2026, Abschnitt Cyberversicherung, 2026

³Howden, Cyber Report 2026 „Re-balancing“, 05.01.2026

zweite Hälfte dieses Zeitraums entspricht die Prognose rund 13 % pro Jahr.⁴ Das ist weiter Wachstum – aber eines das (zumindest kurzfristig) über Durchdringung und Exposure verdient werden muss, nicht über Rate.

Der Preisdruck ist entsprechend anhaltend. Marsh weist für Cyber Global –4 % Prämienentwicklung im zweiten Quartal 2026 aus – das zwölfte Rückgangsquartal in Folge; für Europa nennt Marsh –9%.⁵ Im US-Markt ist die Schadenquote 2025 auf 53 % gestiegen – erstmals seit der Ransomware-Spitze über 50 %. Solange die Preise weiter fallen dürfte es den Versicherern schwerfallen, die steigende Schadenquote umzukehren.

Solange die Preise weiter fallen dürfte es den Versicherern schwerfallen, die steigende Schadenquote umzukehren.

Für das Renewal 2026/2027 heißt das: **Für gut aufgestellte Risiken bleibt der Markt attraktiv.** Wer Prämienvorteile realisieren will, sollte dies jetzt tun und dabei nicht nur die Rate, sondern Versicherungssumme, Sublimits und – neu bzw. verstärkt – die Absicherung der Lieferkette sowie von Cyber-Crime bzw. Social Engineering Betrug Schäden in den Blick nehmen. Denn das Risikobewusstsein in den Chefetagen ist hoch: Cyber bleibt im Allianz Risk Barometer 2026 mit 42 % der Nennungen das Top-Risiko, ein Rekordwert.⁶

Auswirkungen auf den Cyber-Markt | Schadentrends, Bedrohungslage und Umfeld

Die Bedrohungslage 2025/2026 ist paradox. Die Zahl der Ransomware- und Erpressungsfälle bleibt hoch, zugleich sinkt die tatsächliche Zahlungsbereitschaft der betroffenen Unternehmen. Chainalysis beziffert die Ransomware-Zahlungen für 2025 auf 820 Mio. USD und damit unter dem Vorjahr, während deutlich mehr Organisationen auf Leak-Sites genannt wurden. Die Zahlungsquote fiel auf ein historisch niedriges Niveau. Der Coalition 2026 Cyber Claims Report bestätigt diese Entwicklung aus Claims-Perspektive: Initiale Forderungen bleiben hoch, am Ende zahlen jedoch deutlich weniger Unternehmen, und verhandelte Zahlungen liegen häufig erheblich unter den Ausgangsforderungen. Deutschland zählt bei Leak-Site-Nennungen weiterhin zu den besonders betroffenen Ländern.⁷

Damit verschiebt sich die Risikobewertung: Entscheidend ist nicht allein, ob ein Angriff stattfindet oder wie hoch die erste Forderung ausfällt, sondern ob das Unternehmen den Vorfall schnell erkennt, eindämmt, verhandelt und den Betrieb wiederherstellen kann. Coalition zeigt, dass professionelle Schadensteuerung und Verhandlung die tatsächlich geleisteten Zahlungen deutlich reduzieren können; zugleich bleiben die Folgekosten eines Angriffs – insbesondere Betriebsunterbrechung, Forensik, Wiederherstellung und Datenexfiltration – der eigentliche Kostentreiber. Für die Versicherung ist das die entscheidende Verschiebung: Der Blick wandert von der reinen Lösegelddeckung hin zu Incident Response, Wiederherstellung, Betriebsunterbrechung und Datenmanagement.⁸

Ebenso relevant für das Underwriting: **79 % der Angriffe waren identitätsbasiert, und in 97 % der Fälle mit kompromittierten Zugangsdaten war MFA aktiviert** – die Angreifer umgehen sie über andere Lücken in der Absicherung, Phishing-resistente Verfahren fehlen.⁹ Die Aussage „wir haben MFA“ ist damit als

⁴Munich Re, Global Cyber Risk and Insurance Survey 2026

⁵Marsh, Global Insurance Market Index Q2 2026, 23.07.2026; Marsh, Europe Insurance Rates Q2 2026; abweichende Zusammenfassung bei Insurance Journal, 23.07.2026. Die Diskrepanz ist nicht auflösbar; beide Werte stammen aus Marsh-Material.

⁶Allianz Risk Barometer 2026, 14.01.2026

⁷Chainalysis, Crypto Crime Report 2026, 27.02.2026

⁸Coalition, 2026 Cyber Claims Report

⁹Sophos, State of Ransomware 2026

Risikoindikator nicht mehr ausreichend; entscheidend ist die vollständige Abdeckung aller Zugänge einschließlich Administratoren, VPN und Drittzugriffe.

Die Aussage „wir haben MFA“ ist damit als Risikoindikator nicht mehr ausreichend; entscheidend ist die vollständige Abdeckung aller Zugänge einschließlich Administratoren, VPN und Drittzugriffe.

Der BSI-Lagebericht 2025 beschreibt die Lage für Deutschland unverändert als angespannt: durchschnittlich 119 neue Schwachstellen pro Tag (+24 %), 950 Ransomware-Vorfälle im Berichtszeitraum, **80 % der Angriffe trafen KMU**. Bei KRITIS-Betreibern erreichten zwar 80 % einen ISMS-Reifegrad von 3 oder höher, bei der Angriffserkennung aber nur 48 %.¹⁰ Ein Google-Bericht sah Deutschland im April 2026 wieder auf Platz 1 der Ziele europäischer Cyber-Erpresser – begründet unter anderem mit unzureichender Abwehr im Mittelstand.¹¹

119

neue Schwachstellen pro Tag (+24 %)

950

Ransomware-Vorfälle im Berichtszeitraum

80 %

der Angriffe trafen KMU

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2025

Künstliche Intelligenz unterstützt die Angriffsseite messbar

Was im Vorjahresreport noch als absehbare Entwicklung beschrieben wurde, ist 2026 belegt. Anthropic hat im November 2025 die erste dokumentierte, überwiegend **KI-orchestrierte** Cyberspionagekampagne offengelegt: Rund 30 Zielorganisationen, 80 bis 90 % der Kampagne von der KI ausgeführt, lediglich vier bis sechs kritische menschliche Entscheidungspunkte.¹² Eine Folgeanalyse von 832 gesperrten Konten (März 2025 bis März 2026) zeigt, dass 67 % der Akteure KI zum Schreiben von Malware nutzten.¹³ Die Google Threat Intelligence Group hat im Februar 2026 mehrere KI-gestützte Malware-Familien beschrieben, die Code zur Laufzeit generieren oder sich selbst umschreiben.¹⁴

Am unmittelbarsten spürbar ist der KI-Effekt beim **Social Engineering**. Allianz Trade berichtet, dass sich die Schäden aus Fake-President-Betrug 2024 verdreifacht haben (+200 %) und 2025 um weitere 81 % gestiegen sind – bei **sinkenden Fallzahlen** (–13 %). Der Durchschnittsschaden liegt im einstelligen Millionenbereich, Großschäden im zweistelligen. Beim Bestellerbetrug stiegen die Schäden 2025 um 139 %, die Fälle um 61 %.¹⁵ KI-generierte Phishing-Mails erreichen laut Aon eine Klickrate von 54 % gegenüber 12 % bei herkömmlichen Mails.¹⁶

¹⁰BSI, Die Lage der IT-Sicherheit in Deutschland 2025, veröffentlicht 11.11.2025, Berichtszeitraum Juli 2024 bis Juni 2025

¹¹Google, zitiert nach Versicherungswirtschaft heute, 20.04.2026

¹²Anthropic, Disrupting the first reported AI-orchestrated cyber espionage campaign, 13.11.2025

¹³Anthropic, Mapping AI-enabled cyber threats to MITRE ATT&CK, 03.06.2026

¹⁴Google Threat Intelligence Group, Distillation, experimentation, integration: adversarial use of AI, 12.02.2026

¹⁵Allianz Trade, Alarmstufe KI: Schäden durch Fake-President-Betrug vervielfachen sich, 20.01.2026

¹⁶Aon, AI Risk 2026: What Business Leaders Need to Know, 07.05.2026

Klickrate von Phishing-Mails



Quelle: Aon, AI Risk 2026

Für die Beratung folgt daraus zweierlei. Erstens: Die Sensibilisierung und kontinuierliche Schulung der Mitarbeitenden ist wichtiger denn je – und sie muss Deepfakes in Video- und Telefonkonferenzen ausdrücklich einbeziehen, nicht nur E-Mails. Zweitens, und deckungsrechtlich zentral: Vertrauensschadenfälle wie Fake President und Payment Diversion Fraud sind **kein klassischer Cyberschaden**. Ob sie über einen Crime-Baustein in der Cyber-Police, über eine eigenständige Vertrauensschadenversicherung oder gar nicht gedeckt sind, ist im Einzelfall zu prüfen. Angesichts der Schadenentwicklung ist dies der aus Maklersicht dringendste Abgleich im Portfolio und aus Kundensicht eine mögliche Deckungslücke, die es zu schließen gilt.

Großschäden und Systemrisiko

Die Großschäden des Berichtszeitraums haben zwei Lehren geliefert. Die erste betrifft die **Schadenhöhe im Systemausfall**. Der Angriff auf Jaguar Land Rover ab dem 31.08.2025 führte zu einem vollständigen Produktionsstopp; das Cyber Monitoring Centre bewertete das Ereignis als systemisches Ereignis der Kategorie 3 mit einem volkswirtschaftlichen Schaden von rund 1,9 Mrd. GBP (Spanne 1,6 bis 2,1 Mrd.) und über 5.000 betroffenen britischen Organisationen – ohne Datenschutzvorfall und Lösegeld.¹⁷ Die zweite Lehre ist unbequemer: JLR hatte die über einen Makler vorbereitete Cyber-Platzierung **vor dem Vorfall nicht finalisiert** und war damit praktisch unversichert.¹⁸ Ein klares Argument um mit bisher unversicherten Kunden in den Platzierungsprozess zu starten bzw. dessen Abschluss zu forcieren.

ca. 1,9 Mrd.
GBP

volkswirtschaftlicher Schaden des
JLR-Angriffs (Spanne 1,6 bis 2,1
Mrd.)

über 5.000

betroffene britische Organisationen

Kategorie 3

systemisches Ereignis

Quelle: Cyber Monitoring Centre, 22.10.2025

Der Angriff auf die MUSE-Plattform von **Collins Aerospace** am 19.09.2025 traf Check-in- und Gepäcksysteme unter anderem in Brüssel, Berlin, Dublin und London-Heathrow gleichzeitig.¹⁹ Er steht für die inzwischen dominante Schadenmechanik: **Der Angriff findet bei einem Dienstleister statt, der Schaden entsteht beim Kunden**. Dienstleistervorfälle machten 2024 bereits 22 % der eingetretenen Schäden aus – gegenüber 0 % im Jahr 2023.²⁰ Die BaFin bestätigt dieses Muster für den Finanzsektor: Rund die Hälfte aller 2025 gemeldeten schwerwiegenden IKT-Vorfälle hatte ihren Ursprung bei externen Dienstleistern.²¹ **Contingent Business Interruption ist damit 2026 kein Zusatzbaustein mehr, sondern Kernbestandteil einer belastbaren**

¹⁷Cyber Monitoring Centre, Statement on the Jaguar Land Rover Cyber Incident, 22.10.2025

¹⁸The Insurer, Exclusive: Jaguar Land Rover failed to secure cyber insurance deal ahead of attack, 23.09.2025

¹⁹CNBC, What we know about the cyberattack that hit major European airports, 21.09.2025

²⁰Resilience, Collins Aerospace outage: vendor risk, 2025

²¹BaFin, Fachartikel v. 16.07.2026

Cyber-Deckung – mit besonderem Blick auf Haftzeiten, Wartezeiten und die Frage, ob auch nicht-böswillige Ausfälle (Fehlkonfiguration, fehlerhaftes Update) erfasst sind.

Contingent Business Interruption ist damit 2026 kein Zusatzbaustein mehr, sondern Kernbestandteil einer belastbaren Cyber-Deckung

Marktveränderungen durch Anbieter

Im DACH-Cyber-Markt prägen 2026 **Konsolidierung und Arbeitsteilung** das Bild.

Erstens der Beginn einer Konsolidierung. Zurich hat im März 2026 die Übernahme von Beazley für 8,1 Mrd. GBP angekündigt – Beazley hält rund 10 % des Weltmarkts im Cyber; mit Abschluss der Transaktion, erwartet in der zweiten Jahreshälfte 2026, wird Zurich zum größten CyberVersicherer.²² Daneben ziehen sich erneut Assekuradeure aus dem Cybergeschäft zurück, darunter DGC AG (ehemals Cogitanda), sowie Victor (Marsh-Tochter).

Zweitens die neue Arbeitsteilung zwischen Traditionalisten und MGAs. Der markanteste Vorgang: Allianz Commercial hat im Mai 2026 verkündet, das gesamte Cyber-Neugeschäft auf Coalition zu verlagern, nachdem die Partnerschaft seit August 2024 bestanden hatte.²³ Diese Entscheidung wird bereits im Herbst 2026 für die DACH-Region umgesetzt. Das ist mehr als eine Einzelentscheidung: Es ist das Eingeständnis, dass technologiegetriebenes Cyber-Underwriting eine eigene Fähigkeit ist, die sich nicht ohne Weiteres im Konzern aufbauen lässt. Für Makler sind daher zunehmend zwei Fragen getrennt zu beantworten: „Welcher Risikoträger steht hinter dem Risiko?“ und „Über welche Zeichnungsplattform bzw. welches MGA erfolgt die Zeichnung?“.

*Für Makler sind daher zunehmend zwei Fragen getrennt zu beantworten:
„Welcher Risikoträger steht hinter dem Risiko?“ und „Über welche
Zeichnungsplattform bzw. welches MAG erfolgt die Zeichnung?“*

Drittens der weitere Kapazitätsausbau der spezialisierten Anbieter. Anbieter wie Stoik und Baobab nehmen erneut Venture Capital auf, um ihr Wachstum zu beschleunigen und ihr Leistungsangebot auszubauen. Baobab erhielt 2025 in einer Series-A-Runde 12 Mio. EUR, Stoik folgte Anfang 2026 mit einer Series-C-Finanzierung über 20 Mio. EUR. Die Mittel sollen insbesondere für den Ausbau von Cybersecurity- und Präventionsservices, die Weiterentwicklung der Technologie und des Produktangebots sowie die Expansion in weitere europäische Märkte eingesetzt werden. Die Leistungsangebote umfassen inzwischen beispielsweise auch Managed Detection & Response (MDR).

Gleichzeitig drängen weiterhin internationale Anbieter auf den europäischen und deutschen Cyberversicherungsmarkt. Auch etablierte deutsche Versicherer, die sich bislang zurückhaltend gezeigt haben, öffnen sich der Cybersparte.

Für Kunden bedeutet dieses Umfeld weiter **mehr Auswahl und oft innovative Leistungen** – bei gleichzeitig größerer Spreizung der Bedingungswerke. CyberDirekt berichtete im Oktober 2025 über „gravierende Bedingungsänderungen“ bei mehreren etablierten Anbietern und über erhebliche Preisunterschiede zwischen den Top-Anbietern.²⁴ Der reine Preisvergleich greift damit zu kurz; der strukturierte Bedingungs- und Servicevergleich ist der eigentliche Mehrwert der Maklerleistung. Mit der Expansion und dem schnellen Wachstum einzelner Anbieter steigen zugleich die Anforderungen an deren Vertriebs- und Servicestrukturen.

²²SecurityWeek, März 2026; Global Finance, 06.05.2026

²³Versicherungswirtschaft heute, 07.05.2026; Allianz Commercial, Partnerschaft mit Coalition, 2024

²⁴CyberDirekt, zitiert nach Versicherungswirtschaft heute, 16.10.2025

Im Markt ist allerdings zu beobachten, dass die Betreuung einer wachsenden Zahl von Maklerpartnern nicht immer in gleicher Qualität skaliert. Neben Produktqualität, Deckungsumfang, Preis und weiteren Faktoren kann daher auch die Qualität und Verlässlichkeit der Servicierung ein relevantes Kriterium bei der Empfehlung eines Versicherers sein.

Das Team von Finlex unterstützt hier weiterhin mit Portfoliotransferlösungen und einem strukturierten Angebotsvergleich für Ihre Kunden.

Auch die Grundlage der Risikobewertung unterscheidet sich weiter: Während traditionelle Versicherer die Risikosituation im Kern über Fragebögen und Risikodialoge bewerten, nutzt der Großteil der neuen Marktteilnehmer (zusätzlich) eigene Scan-Technologie und reduziert damit die Zahl der vom Kunden zu beantwortenden Fragen (teils) erheblich. Inzwischen greifen aber auch fast alle etablierten Player auf Scan-Technologie zur kontinuierlichen Bewertung ihres Portfolios zurück. Ein finaler Nachweis, dass der Einsatz von Scantechnologien die Schadenbelastung nachhaltig reduziert, steht allerdings noch aus.

Zeichnungsverhalten der Cyber-Versicherer

Das Zeichnungsverhalten bleibt 2026 zweigeteilt: **offener bei der Kapazität, unverändert diszipliniert bei den Mindeststandards.**

Risikoselektion und -bewertung: Ohne Umsetzung solider Cyber-Hygiene-Standards ist ein Zugang zur Cyber-Deckung für Unternehmen immer noch nicht möglich – daran ändert die weiche Marktpphase im Grundsatz nichts. Die geringe Versicherungsdurchdringung ist dabei nicht allein Ausdruck fehlender Nachfrage. Nach Erkenntnissen des GDV verfügt nur rund ein Drittel der deutschen Unternehmen über hinreichende IT-Schutzmaßnahmen. Regelmäßige Sicherheitsupdates, belastbare Backups, klare Zugriffsrechte und funktionierende Notfallpläne bleiben damit nicht nur zentrale Präventionsmaßnahmen, sondern häufig auch faktische Zugangsvoraussetzungen für den Versicherungsschutz.²⁵

Outside-in-Scans der IT-Systeme gehören zum Standard; Versicherer nutzen Tools, um offene Ports, auslaufende Zertifikate oder bekannte Schwachstellen eines Antragstellers aufzuspüren. Ein entsprechend kritischer Befund führt zu Rückfragen oder Ablehnung. Bei den Detail-Fragebögen sind die Themenfelder unverändert: Datensicherung, Patch-Management, Berechtigungskonzepte, Multi-Faktor-Authentifizierung, Altsysteme. **Aufklärungspflicht und Anzeigegenauigkeit** bleiben das größte vermeidbare Risiko für Versicherungsnehmer. Die einschlägigen Entscheidungen geben hier unverändert die Richtlinien vor: Das LG Kiel hat mit Urteil vom 23.05.2024 die Anfechtung einer Cyber-Police wegen arglistiger Täuschung für wirksam gehalten, weil Risikofragen zu Sicherheitssoftware und Updates objektiv falsch beantwortet wurden – bei laufenden, nicht gepatchten Altsystemen. Das OLG Schleswig hat die Berufung zurückgewiesen und klargestellt, dass ein IT-Leiter Risikofragen nicht „nach Glauben“ beantworten darf.²⁶ Demgegenüber hat das LG Tübingen entschieden, dass nicht jede falsche Angabe zum Verlust des Schutzes führt – es kommt auf Verschulden und Kausalität an; dort wurden rund 2,86 Mio. von 3,77 Mio. EUR zugesprochen.²⁷ Das LG Hagen hat eine Klage aus einer Cyber-Police bei einem CEO-Fraud-Fall abgewiesen, weil keine versicherte Netzwerksicherheitsverletzung nachgewiesen war.²⁸ Eine BGH-Entscheidung zur Cyber-Versicherung liegt weiterhin nicht vor. Für Makler bleibt es daher zentral, Kunden zur sorgfältigen und wahrheitsgemäßen Beantwortung anzuhalten und die Antworten – insbesondere bei Angaben Dritter aus der IT – zu dokumentieren.

²⁵ Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV), Statistiken zur deutschen Versicherungswirtschaft 2026, Abschnitt Cyberversicherung, 2026

²⁶ LG Kiel, Urteil v. 23.05.2024 – 5 O 128/21; OLG Schleswig – 16 U 63/24 (Januar 2025); dazu ADVANT Beiten, 27.08.2024, und GÖRG, 25.04.2025

²⁷ LG Tübingen – 4 O 193/21

²⁸ LG Hagen, Urteil v. 15.10.2024 – 9 O 258/23

Aufklärungspflicht und Anzeigegenauigkeit bleiben das größte vermeidbare Risiko für Versicherungsnehmer.

Kapazitätsmanagement: Aus einer Hand sind bei den meisten Risikoträgern wieder 10 Mio. EUR erhältlich, teilweise bis 15 Mio. EUR Eigenkapazität; standardisierte Deckungen greifen bis etwa 50 Mio. EUR Umsatz. Im Exzedentenbereich ergeben sich durch die höhere Zahl der Marktteilnehmer weiter attraktive Möglichkeiten – auch wenn die Konsolidierung an der Spitze mittelfristig zu beobachten ist.

Pricing: Der Preisdruck ist unverändert nach unten gerichtet, aber die Versicherer beginnen zu differenzieren. Kunden mit guter IT-Sicherheit erhalten weiter Nachlässe; bei kritischen Risiken werden Konditionsanpassungen und Auflagen zur Risikoverbesserung eingesetzt, die eine mindestens gleichwertige Rolle wie Prämienanpassungen spielen. Angesichts der steigenden Schadenquoten – US-Schadenquote von 53 % im Jahr 2025 – ist damit zu rechnen, dass der Spielraum in den nächsten 12 bis 18 Monaten enger wird.

Für Kunden bleibt das Fazit mit Blick auf das Renewal zum 01.01.2027: Die aktuelle Marktlage bietet attraktive Möglichkeiten, um den Versicherungsschutz weiter auszubauen, in dem die Versicherungssumme zu attraktiven Konditionen erhöht wird, Verbesserungen auf Bedingungsseite (beispielsweise durch attraktivere Sublimate) genutzt und mögliche Deckungslücken, insbesondere im Bereich Cyber-Kriminalität und Social Engineering Betrug geschlossen werden – sei es über die Cyber-Versicherung oder eine eigenständige Vertrauensschadenversicherung. Hier ist auch die Maklerseite im Rahmen der Detailanalyse der Bedingungen sowie der umfassenden Beratung gefragt – die Finlex Expert:innen unterstützen hier jederzeit gerne.

Besonderheiten des österreichischen Marktes in Cyber

Der österreichische Cyber-Versicherungsmarkt befindet sich – insbesondere im vorherrschenden KMU-Segment – weiter in einer vergleichsweise frühen Entwicklungsphase, weist aber eine hohe Dynamik auf. Auffällig bleibt die Zurückhaltung heimischer Versicherer bei Cyber-Deckungen; viele österreichische Komposit-Versicherer zögern, eigenständige Cyber-Produkte anzubieten, oder tun es nur mit restriktiven Bedingungen. Der Markt wird daher stark von ausländischen Anbietern dominiert. Typische Deckungseinschränkungen betreffen die Deckung von Lösegeldzahlungen sowie die Betriebsunterbrechungs-Deckung, bei der einige österreichische Produkte kurze Haftzeiten oder Tages-Maximalentschädigungen vorsehen.

Cyber Österreich: Markt-Durchschnittsprämien in der Finlex-Plattform (Weichmarktpphase)

Unternehmensgröße	Umsatz	Markt-Durchschnittsprämie je 1 Mio. € Versicherungssumme
Kleinbetriebe	5 Mio. €	ca. 1,75 ‰
Mittelbetriebe	50 Mio. €	ca. 5 ‰

Quelle: Finlex-Plattform

Ein entscheidender Treiber der nächsten zwölf Monate ist regulatorisch: Das **NISG 2026** tritt am 01.10.2026 in Kraft und betrifft rund 4.000 Organisationen in 18 Sektoren; die Registrierung hat bis 31.12.2026 zu erfolgen, die Selbsterklärung bis 30.09.2027.²⁹ Damit wiederholt sich in Österreich mit rund zehnmonatiger Verzögerung, was in Deutschland Ende 2025 begonnen hat: Ein regulatorisch erzwungener Anstieg des Security-Niveaus, der das Risikoprofil verbessert – und gleichzeitig die Nachfrage nach Versicherungsschutz erhöht, weil die Geschäftsleitung persönlich in der Verantwortung steht.

²⁹Parlament Österreich, XXVIII/I/308 (BGBl. I Nr. 94/2025); WKO, NIS2-Übersicht, Abruf 08/2026

Handlungsempfehlungen für österreichische Makler: Aus der Kombination von günstiger Marktsituation und regulatorischem Handlungsdruck ergeben sich Chancen sowohl im Neugeschäft als auch in der Optimierung bestehender Verträge. Die Neukundenansprache lohnt sich 2026 besonders, weil das NISG-Inkrafttreten einen natürlichen Anlass bietet. Im Bestand ist vorrangig zu prüfen, ob Haftzeiten und Betriebsunterbrechungsdeckung noch zum tatsächlichen Risiko passen und ob Dienstleisterausfälle erfasst sind.

Um einen Konkurrenzeinbruch bei den Bestandsverträgen zu vermeiden, sollten die Makler das eigene Portfolio auf Marktkonformität überprüfen. Finlex hat dazu den Portfolio Health Check entwickelt und unterstützt seine Kooperationsmakler durch eine transparente Ist-Analyse und einfache Optimierungsvorschläge ohne neues Risikoassessment.



Claims

Schadenentwicklung und -ausblick Cyber

Die Finlex Claims-Abteilung begleitet als Ansprechpartner sowohl Kooperationsmakler als auch Versicherungsnehmer und versicherte Personen während des gesamten Schadenprozesses. Die Unterstützung reicht von der Ersteinschätzung über die Sichtung von Schadenunterlagen mitsamt deckungsrechtlicher Prüfung und der Abgabe von Handlungsempfehlungen bis hin zur Schadenmeldung und der Übernahme der gesamten Korrespondenz mit Versicherern und/oder Kunden. Darüber hinaus erarbeitet die Finlex Claims-Abteilung fundierte Stellungnahmen bei unberechtigten Deckungsablehnungen, unterstützt Kooperationsmakler sowie Kunden bei Vergleichsverhandlungen und vermittelt Spezialisten aus dem Finlex Expertennetzwerk.

In dieser Rolle hat Finlex Claims allein in den letzten zwölf Monaten eine mittlere dreistellige Anzahl Neuschäden begleitet.

Cyber – Schadenentwicklung

Die Zahl der Cyber-Schäden bleibt auf hohem Niveau. Neben klassischen Ransomware-Szenarien gewinnen Datenabfluss und Erpressung ohne Verschlüsselung an Bedeutung. Für die Schadenhöhe bleiben insbesondere Betriebsunterbrechungs-, Wiederherstellungs- und Incident-Response-Kosten relevant.

Frequenz: Cyber-Schäden nehmen weiter zu. Im Vergleich zum Vorjahr verzeichnete Finlex rund 17 % mehr Schadenmeldungen. Gleichzeitig ist der Anteil reiner Verdachtsfälle zurückgegangen. Die Meldungen betreffen damit häufiger bereits konkret eingetretene Cybervorfälle. Es zeigt sich allerdings auch, dass eine steigende Zahl von Cyber-Angriffen nicht zwangsläufig zu einer entsprechenden Zunahme schwerer Schäden führt. Investitionen in IT-Sicherheit, verbesserte Backup-Konzepte und professionellere Incident-Response-Strukturen tragen dazu bei, Angriffe früher einzudämmen und insbesondere Betriebsunterbrechungs- und Datenverlustschäden zu begrenzen.

+17 %

Cyber-Schadenmeldungen bei Finlex gegenüber dem Vorjahr

rund 25 %

der Fälle, in denen Erstmaßnahmen Schlimmeres verhindern konnten

Quelle: Finlex Claims

Schadenarten: Ransomware-Angriffe bleiben prägend für die Großschäden, insbesondere wenn Verschlüsselung, Datenabfluss und längere Betriebsunterbrechungen zusammentreffen. Dabei verändert sich das Angriffsmuster zunehmend: Neben der klassischen Verschlüsselung von Systemen setzen Angreifer auch auf den Abfluss sensibler Daten und die Drohung mit deren Veröffentlichung. Teilweise verzichten die Täter mittlerweile vollständig auf eine Verschlüsselung und nutzen allein die mögliche Veröffentlichung der erbeuteten Daten als Druckmittel für ihre Lösegeldforderung. Die Schadenfrequenz wird allerdings stärker durch **kleinere Sicherheitsvorfälle wie Phishing-Angriffe oder kompromittierte E-Mail-Accounts** geprägt. Insgesamt bleibt das Cyber-Schadengeschehen damit durch eine hohe Frequenz kleinerer Vorfälle bei gleichzeitig erheblichem Großschadenpotenzial gekennzeichnet.

Schadenfälle an der Schnittstelle zwischen Cyber- und Vertrauensschadenversicherung: Zugenommen haben Schadenmeldungen zu Fake-Rechnungs-, Fake-President- und Payment-Diversion-Fällen, bei denen Täter durch Social Engineering oder die Kompromittierung von Kommunikationswegen Zahlungen manipulieren oder umleiten. Diese Entwicklung gewinnt nicht nur aufgrund der steigenden Fallzahlen an Bedeutung, sondern auch mit Blick auf die Deckungszuordnung: Je nach konkretem Tathergang kann entscheidend sein, ob dem Vermögensschaden eine Netzwerksicherheitsverletzung vorausgegangen ist und damit die Cyberversicherung betroffen sein kann. Um dies zu klären ist meist eine forensische Untersuchung – und damit auch eine Meldung an den Versicherer bzw. die Notfallhotline – erforderlich.

Schadenausmaß: Die Durchschnittskosten pro Cyber-Schaden variieren zumeist nach der Größe des betroffenen Unternehmens. In rund 25% aller von Finlex begleiteten Cyber-Versicherungsfälle konnte durch die sofortigen Erstmaßnahmen (Incident Response Team, Forensiker) Schlimmeres verhindert werden. Die 24/7-Notfallhotlines und eine schnelle Intervention zahlen sich hier aus.

Regulierungspraxis: Die Cyber-Schadenregulierung hat ihren Rhythmus gefunden, ist aber weiterhin komplex. Zu Beginn steht fast immer die Schadenhotline: Der Versicherer entsendet in Abstimmung mit dem Kunden und dem Makler Forensiker und IT-Dienstleister. Viele Versicherer steuern den gesamten Prozess, was zumeist als sehr hilfreich empfunden wird und wertvolle Zeitvorteile bringt. Zugleich gewinnen die Kosten der Schadenbewältigung an Bedeutung. Insbesondere spezialisierte Forensik- und Incident-Response-Leistungen können bei komplexen Cybervorfällen erhebliche Kosten verursachen. Hinzu kommt die Herausforderung, bei parallelen Großschäden kurzfristig ausreichende Kapazitäten qualifizierter Spezialisten verfügbar zu haben.

Deckungsablehnungen: Deckungsstreitigkeiten bleiben auch in der Cyberversicherung Teil der Regulierungspraxis. Im Mittelpunkt stehen dabei häufig Obliegenheitsverletzungen oder die Frage, ob Angaben des Versicherungsnehmers bei Vertragsschluss zutreffend und vollständig waren. Nicht jede Deckungsablehnung führt jedoch zu einer endgültigen Leistungsverweigerung. Gerade bei rechtlich oder tatsächlich nicht eindeutigen Sachverhalten besteht häufig Raum für Vergleichslösungen. Deutlich konsequenter reagieren Versicherer dagegen, wenn sie von einer arglistigen Täuschung bei Vertragsschluss ausgehen. In diesen Fällen werden regelmäßig die entsprechenden Gestaltungsrechte geltend gemacht und Versicherungsleistungen verweigert.

Cyber – Schadenausblick

Auch für 2026/2027 ist mit einer gleichbleibend hohen Anzahl an Cyber-Schadenfällen zu rechnen. Die Bedrohungslage bleibt angespannt und Cyber-Angriffe werden sich auch künftig nicht vollständig verhindern lassen. Umso entscheidender ist die Cyber-Resilienz der Unternehmen: Wie gut sie auf einen Angriff vorbereitet sind und wie schnell und effektiv sie reagieren können, bestimmt maßgeblich das mögliche Schadenausmaß.

Erpressungsmodelle verändern sich: Ransomware bleibt ein wesentlicher Treiber von Cyber-Großschäden. Gleichzeitig verändern die Täter ihre Vorgehensweise. Neben der klassischen Verschlüsselung gewinnen Datendiebstahl und die Drohung mit der Veröffentlichung sensibler Informationen als eigenständiges Erpressungsmittel an Bedeutung. Verbesserte Backup- und Recovery-Konzepte reduzieren damit zwar das Risiko erheblicher Schäden durch eine Verschlüsselung, bieten jedoch keinen Schutz vor den finanziellen,

regulatorischen und reputativen Folgen eines Datenabflusses. Für Unternehmen wird daher neben der Wiederherstellungsfähigkeit insbesondere der Schutz sensibler Daten weiter an Bedeutung gewinnen.

KI verstärkt Cyber- und Betrugsrisiken: Künstliche Intelligenz dürfte die Cyber-Bedrohungslage weiter verändern. KI ermöglicht es Angreifern, Phishing und Social Engineering schneller, skalierbarer und zielgerichteter einzusetzen. Gleichzeitig können Deepfake-Technologien die täuschend echte Imitation von Stimmen, Personen und Kommunikationsinhalten erleichtern. KI schafft damit nicht zwingend völlig neue Angriffsszenarien, erhöht aber die Qualität und Skalierbarkeit bereits bekannter Angriffsmethoden erheblich. Besonders relevant dürfte KI im Bereich des Social Engineering und damit an der **Schnittstelle zwischen Cyber- und Vertrauensschadenversicherung** werden. Fake-President-, Fake-Rechnungs- oder Payment-Diversion-Szenarien können durch KI-generierte E-Mails sowie täuschend echte Sprach- oder Videonachrichten erheblich überzeugender gestaltet werden. Versicherungstechnisch kann dies die Abgrenzung zwischen Cyber- und VSV-Deckung weiter in den Fokus rücken, da ein digital initiiertter Betrug nicht zwangsläufig einen unter der Cyberversicherung gedeckten Vermögensschaden darstellt. Angesichts des bereits beobachteten Anstiegs von Schadenfällen mit VSV-Bezug dürfte dieser Bereich für die Schadenpraxis weiter an Bedeutung gewinnen.

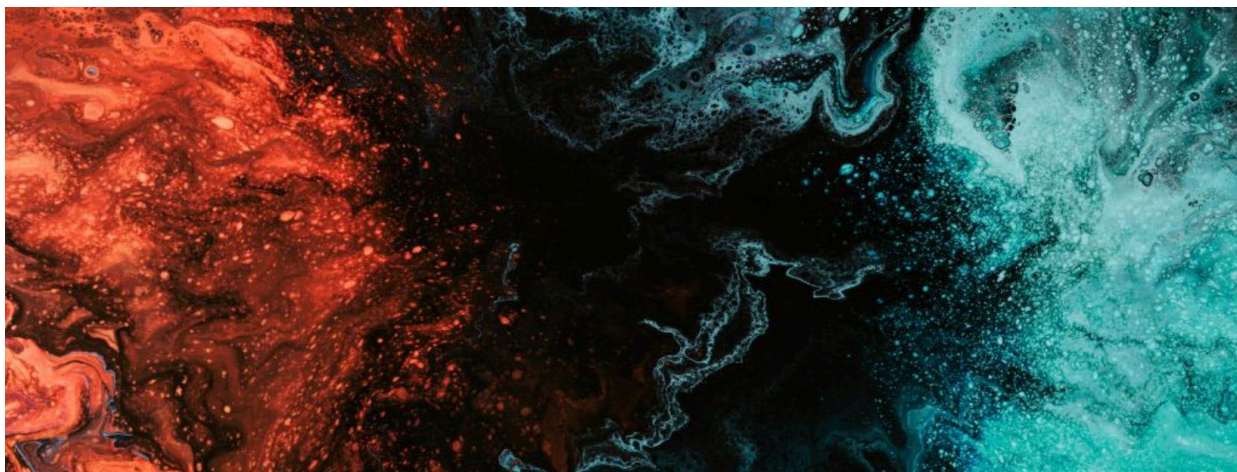
Empfehlung

Für einen möglichst umfassenden Versicherungsschutz empfiehlt es sich daher, die Cyberversicherung durch eine eigenständige Vertrauensschadenversicherung zu ergänzen und beide Deckungen aufeinander abzustimmen. Gerade bei Social-Engineering- und Zahlungsbetrugsfällen können so Deckungslücken an der Schnittstelle zwischen Cyber- und Vertrauensschadenversicherung vermieden werden – **die Finlex Expert:innen unterstützen Sie dabei gerne.**

Positiv bleibt, dass Unternehmen und Versicherer zunehmend professioneller auf Cybervorfälle vorbereitet sind. Neben klassischen Präventionsmaßnahmen gewinnen Incident-Response-Pläne, regelmäßige Übungen, Threat Intelligence und eine möglichst frühzeitige Erkennung von Angriffen an Bedeutung. Diese Investitionen zeigen Wirkung: Verbesserte Detection- und Response-Fähigkeiten sind ein wesentlicher Grund dafür, dass die Auswirkungen bestimmter Cyber-Großschäden begrenzt werden können. Der Schwerpunkt verschiebt sich damit zunehmend von der Vorstellung, jeden Angriff verhindern zu können, hin zur Frage, wie schnell ein Angriff erkannt, eingedämmt und der Geschäftsbetrieb wiederhergestellt werden kann. Die Empfehlung sowohl für Versicherer als auch Unternehmen lautet unverändert: **Wachsam bleiben und in Prävention investieren.**

Die Empfehlung sowohl für Versicherer als auch Unternehmen lautet unverändert: Wachsam bleiben und in Prävention investieren.

Fazit: Der Versicherungsmarkt für D&O und Cyber präsentiert sich auch 2026/2027 weiterhin stabil und leistungsfähig. Das Risikoumfeld wird allerdings zunehmend komplex, da sowohl bekannte als auch neue Risiken das Schadengeschehen prägen. Damit wird ein ganzheitlicher Blick auf Risiko und Versicherungsschutz wichtiger denn je. Entscheidend ist nicht allein, neue Risiken frühzeitig zu erkennen, sondern Versicherungsschutz, Prävention und Krisenmanagement sinnvoll aufeinander abzustimmen. D&O- und Cyberversicherung bleiben dabei zentrale Bausteine des unternehmerischen Risikomanagements. Ein umfassender Risikotransfer sollte jedoch auch mögliche Deckungslücken an der Schnittstelle zur Vertrauensschadenversicherung berücksichtigen. Genau diese Entwicklungen und ihre Auswirkungen auf den Versicherungsmarkt und die Schadenpraxis soll der vorliegende Market Report einordnen.



Künstliche Intelligenz

Auswirkungen auf die Versicherungsbranche und Bedarf nach neuen Versicherungslösungen

Im Markt Report des Vorjahres war Künstliche Intelligenz ein Exkurs. Diese Einordnung trägt nicht mehr. KI ist innerhalb eines Jahres von einem Technologiethema zu einem Risikothema mit eigener Deckungsfrage geworden – und zwar auf drei Ebenen gleichzeitig: als Werkzeug der Angreifer, als Haftungsquelle für Unternehmen und ihre Organe, und als Gegenstand einer neuen, noch jungen Produktkategorie in der Versicherungswirtschaft. Dieses Kapitel ordnet die drei Ebenen und benennt, was daraus für Makler und Versicherungseinkäufer folgt.

Wie schnell die Verschiebung erfolgt ist, zeigt das Allianz Risk Barometer 2026: KI springt von Rang 10 (2025) auf Rang 2 (2026) mit 32 % der Nennungen – der größte Sprung des Rankings; Cyber bleibt mit 42 % auf Rang 1. Bemerkenswert ist die Ambivalenz: 44 % der Befragten sehen mehr Chancen als Risiken, 19 % mehr Risiken als Chancen.³⁰

Allianz Risk Barometer 2026: Anteil der Nennungen (Top Unternehmensrisiko)



Quelle: Allianz Risk Barometer 2026

KI in der Versicherungswirtschaft: breite Adoption, dünne Wertschöpfung

Versicherer, Makler und Versicherungsnehmer stehen unter Wettbewerbs- und Effizienzdruck und führen KI-Tools ein. In der Versicherungsbranche wird dies zugleich als eine Antwort auf den absehbaren Fachkräftemangel gesehen. Der Stand der Dinge ist allerdings differenzierter, als die öffentliche Diskussion vermuten lässt.

Die EIOPA-Erhebung vom Februar 2026 – Basis 347 Unternehmen aus 25 Ländern – zeigt, dass knapp zwei Drittel der europäischen Versicherer generative KI aktiv nutzen. 64 % der Anwendungsfälle liegen im Back-

³⁰Allianz Risk Barometer 2026, Pressemitteilung v. 14.01.2026 – Basis 3.338 Risikoexperten aus 97 Ländern, 15. Ausgabe

End (Datenextraktion, Textgenerierung, Coding-Assistenten), 36 % im Kundenkontakt (Chatbots, Voice). 49 % verfügen inzwischen über dedizierte KI-Richtlinien, gegenüber 25 % im Jahr 2023. Die Mehrheit der Anwendungen befindet sich jedoch noch im Proof-of-Concept-Stadium.³¹

knapp 2/3

der europäischen Versicherer nutzen generative KI aktiv

64 %

der Anwendungsfälle liegen im Back-End

49 %

verfügen über dedizierte KI-Richtlinien (2023: 25 %)

Quelle: EIOPA, 02.02.2026

Capgemini kommt in seinem World Property and Casualty Insurance Report 2026 zu einem ähnlichen Befund. Dazu kommt, dass 72 % der KI-Investitionen in Technologie und Infrastruktur fließen, aber nur 28 % in Change Management und Schulung.³² Swiss Re formuliert es am deutlichsten: Weniger als 5 % der analysierten Versicherer berichten über einen (bisher) messbaren finanziellen Nutzen aus KI.³³

Weniger als 5 % der analysierten Versicherer berichten über einen (bisher) messbaren finanziellen Nutzen aus KI.

Dort, wo Anwendungen produktiv sind, sind die Effekte allerdings erheblich. Zwei deutsche Beispiele aus einer GDV-Veröffentlichung: Bei ERGO prüft KI Zahn- und Laborrechnungen mit 90 bis 95 % Treffgenauigkeit und reduziert die Bearbeitungszeit von rund 90 Minuten auf etwa 10 Minuten. Bei Signal Iduna senkte der Wissensassistent „COSI“ die Weiterleitungsquote im Kundenservice von 27 % auf 3 %; 96 % der Mitarbeitenden nutzen das System.³⁴

Was das für Makler bedeutet: Die Effizienzgewinne der Versicherer schlagen zuerst dort durch, wo Prozesse standardisierbar sind – in der Antragsverarbeitung, in der Erstprüfung von Schadenmeldungen, in der Dokumentenauswertung. Für die Zusammenarbeit heißt das: Vollständige, strukturierte Antrags- und Schadenunterlagen werden schneller verarbeitet als bisher, unvollständige fallen häufiger in manuelle Klärungsschleifen. Gleichzeitig steigt die Bedeutung der fachlichen Einordnung durch den Makler dort, wo Automatisierung an ihre Grenzen kommt: bei Bedingungsauslegung, Deckungsstreit und individueller Risikodarstellung.

Aufsichtsrechtliche Erwartungen: KI-Governance ist prüfbar geworden

Der aufsichtsrechtliche Rahmen hat sich 2025/2026 von allgemeinen Erwartungen zu konkret prüfbaren Anforderungen verdichtet.

EIOPA hat am 06.08.2025 eine Opinion zu KI-Governance und Risikomanagement veröffentlicht.³⁵ Sie ist an die nationalen Aufsichtsbehörden adressiert, richtet sich inhaltlich aber an Versicherungsunternehmen **und** **Versicherungsvermittler**. Der Ansatz ist verhältnismäßig und risikoorientiert: zuerst eine KI-Risikoeinschätzung, dann eine daran abgestufte Governance. Verbotene und Hochrisiko-KI im Sinne der KI-

³¹EIOPA, Survey on Generative AI shows swift but cautious adoption among Europe's insurers, 02.02.2026

³²Capgemini, World Property and Casualty Insurance Report 2026, 05.05.2026 – Basis 344 P&C-Führungskräfte, 809 Mitarbeitende, 1.113 Versicherungsnehmer

³³Swiss Re Institute, sigma insights 01/2026: AI adoption is reshaping the risk landscape, 13.01.2026

³⁴GDV, Versicherungsstandort Deutschland: Der Weg zum KI-Champion, 09.07.2026

³⁵EIOPA-BoS-25-360, Opinion on Artificial Intelligence governance and risk management, 06.08.2025

Verordnung deckt die Opinion ausdrücklich nicht ab, um Doppelregulierung zu vermeiden. Verlangt werden unter anderem dokumentierte Policies über den gesamten KI-Lebenszyklus, klare Rollen (z.B. Compliance, Interne Revision, Aktuarfunktion, Datenschutzbeauftragter), Schulungen, Datenqualität und Erkennung, Bewertung und Minderung von Verzerrungen (Bias).

Erklärbarkeit der Ergebnisse, menschliche Aufsicht mit Eskalationsverfahren – und, für die Praxis besonders wichtig: Bei Auslagerung an KI-Anbieter bleibt die Verantwortung beim Unternehmen; wo der Anbieter sein geistiges Eigentum schützt, sind kompensierend Vertragsklauseln, externe Audits und Due-Diligence-Tests einzusetzen.

Die BaFin hat am 18.12.2025 eine unverbindliche Orientierungshilfe zu IKT-Risiken beim Einsatz von KI-Systemen veröffentlicht. Sie unterstützt insbesondere CRR-Institute und Solvency-II-Versicherer bei der Anwendung der DORA-Anforderungen auf KI-Systeme.³⁶ Sie erwartet, dass Ergebnisse „je nach Einsatzzweck und Risikogehalt erklärbar und überprüfbar“ sind, adressiert Bias sowie Drittanbieter- und Cloud-Konzentrationsrisiken.³⁷ Seit dem 29.07.2026 ist das deutsche Durchführungsgesetz zur KI-Verordnung in Kraft; die BaFin ist damit **Marktüberwachungsbehörde** für KI-Systeme in direktem Zusammenhang mit regulierten Finanztätigkeiten und verfügt über Bußgeldkompetenz.³⁸

Der EU AI Act wurde durch den „Digital Omnibus“ (Verordnung (EU) 2026/1744, in Kraft seit 27.07.2026) bei den Hochrisiko-Pflichten entzerrt: Anhang III gilt nun ab 02.12.2027, Anhang I ab 02.08.2028. Nicht verschoben wurden die Transparenzpflichten nach Art. 50, die seit dem 02.08.2026 anwendbar sind, die Verbote (seit 02.02.2025), die KI-Kompetenzpflicht und die GPAI-Pflichten (seit 02.08.2025).³⁹ Für Versicherer ist zu beachten, dass Anhang III die Risikobewertung und Preisbildung gegenüber natürlichen Personen in der **Lebens- und Krankenversicherung** als Hochrisiko einordnet – Financial Lines und Sachversicherung fallen nicht darunter.⁴⁰

Praxishinweis für Makler

Die KI-Förderungspflicht **nach Art. 4 KI-VO gilt seit dem 02.02.2025 bzw. 27.07.2026 auch für Versicherungsmakler und deren Mitarbeitende**.⁴¹ Wer KI-Tools in Beratung, Angebotsvergleich oder Dokumentenerstellung einsetzt, sollte als Best Practice drei Dinge belegen können: eine schriftliche KI-Richtlinie, Schulungsnachweise für die betroffenen Mitarbeitenden – und eine Regelung, wie KI-generierte Ergebnisse vor Verwendung gegenüber dem Kunden geprüft werden.

Hinzu kommt seit dem 02.08.2026 die Transparenzpflicht nach Art. 50: Wer mit einer KI interagiert, muss dies erkennen können. Für Chatbots und automatisierte Kundenkommunikation im Maklerbetrieb ist das unmittelbar relevant.

Neue Haftungsrisiken – und warum sie in der D&O ankommen

Die Haftungsdiskussion um KI hat sich 2026 von der Frage „Wer haftet für die Maschine?“ zur Frage „Wer haftet für die Governance?“ verschoben. Diese zweite Frage führt direkt zur D&O-Versicherung.

³⁶BaFin, Orientierungshilfe zu IKT-Risiken bei dem Einsatz von KI-Systemen in Finanzunternehmen, 18.12.2025

³⁷BaFin, Risiken im Fokus 2026 – Digitalisierung

³⁸BaFin, Pressemitteilung Überwachung von KI: BaFin erhält neue Kompetenzen, 29.07.2026

³⁹Verordnung (EU) 2026/1744; Rat der EU, Pressemitteilung v. 29.06.2026; Gibson Dunn, EU AI Act Omnibus Agreement, 2026

⁴⁰EIOPA-BoS-25-360, Abschnitt 2.4; BaFin, Pressemitteilung v. 29.07.2026

⁴¹Deutsche Versicherungsbörse, EU-KI-Verordnung: Was Versicherungsmakler beachten müssen, 07.07.2026

Die Haftungsdiskussion um KI hat sich 2026 von der Frage „Wer haftet für die Maschine?“ zur Frage „Wer haftet für die Governance?“ verschoben.

Rechtsgrundlage sind in Deutschland die allgemeinen Sorgfaltspflichten aus **§ 93 AktG** und **§ 43 GmbHG** – mit unbeschränkter persönlicher Haftung bereits bei einfacher Fahrlässigkeit. Drei Haftungsauslöser sind bereits identifiziert: erstens der unterlassene KI-Kompetenzaufbau bzw. die Untätigkeit der Geschäftsleitung – auch das **Nicht-Befassen** mit KI kann eine Pflichtverletzung sein, wenn Wettbewerbsvorteile verkannt oder Risiken nicht erkannt werden; zweitens KI-gestützte Entscheidungen ohne Plausibilitätsprüfung; drittens Compliance-Verstöße durch fehlende KI-Richtlinien, fehlende Schulungen oder Verstöße gegen Datenschutz-, Urheber- und Aufsichtsrecht.

Dass dies nicht theoretisch ist, zeigt der US-Kapitalmarkt. Im ersten Halbjahr 2026 wurden 121 Securities Class Actions eingereicht (+30 % gegenüber dem zweiten Halbjahr 2025), davon 15 mit KI-Bezug. Diese 15 Klagen machten rund 12 % der Filings aus, aber **73 % des Disclosure Dollar Loss** (385 von 529 Mrd. USD) und 73 % des Maximum Dollar Loss; zwei KI-Klagen allein stehen für 1,2 Bio. USD MDL.⁴² Der Klagegrund ist meist nicht ein technisches Versagen, sondern „**AI-Washing**“ – also unzutreffende oder überzeichnete Aussagen über die eigenen KI-Fähigkeiten. Über alle Klagearten hinweg sind KI-bezogene Verfahren zwischen 2021 und 2025 um 978 % gestiegen, allein von 2024 auf 2025 um 137 %.⁴³

US-Securities-Class-Actions mit KI-Bezug im ersten Halbjahr 2026



Quelle: Cornerstone Research, 29.07.2026

Für deutsche und österreichische Mittelständler sind daraus keine Aktionärsklagen zu erwarten. Die relevanten Konstellationen sind andere: Innenhaftungsansprüche der Gesellschaft nach einem KI-verursachten Schaden, Ansprüche nach fehlerhafter automatisierter Entscheidung gegenüber Kunden oder Bewerbern, Bußgelder wegen Verstößen gegen die KI-Verordnung oder die DSGVO – und, in Deutschland besonders relevant, **Urheberrechtsverletzungen durch generative KI**.

Neue Versicherungslösungen für KI-Risiken

Parallel zur Ausschlussdiskussion entsteht eine eigene Produktkategorie. Sie ist noch klein, aber sie ist real – und sie sollte in der Beratung bekannt sein, weil erste Kunden danach fragen.

In Deutschland wird eine entsprechende Absicherung aktuell primär durch das Produkt „aiSure“ von Munich Re zusammen mit Mosaic Insurance angeboten. Im Kern bietet das Produkt KI-Anbietern eine Absicherung von Performance-Garantien gegenüber seinen Kunden, also für den Fall, dass die KI die zugesagten Leistungsparameter nicht erfüllt.

Auch wenn es international noch vereinzelt weitere Beispiele für derartige Produkte gibt befindet sich das Segment grundsätzlich noch in der Testphase. Die Kapazitäten sind überschaubar, entsprechende Prämienvolumina sind bisher nicht kommuniziert. Die weiteren Entwicklungen sollten sicherlich mit Spannung beobachtet werden, für die überwiegende Zahl der mittelständischen Kunden ist der pragmatischere Weg aber sicherlich zunächst ein anderer – nämlich sicherzustellen, dass die **bestehenden** Policen in D&O, Cyber und VSH KI nicht ausschließen und Deepfake-Betrug erfassen.

⁴²Cornerstone Research, Securities Class Action Filings Surge in the First Half of 2026, 29.07.2026; dazu Cooley, 10.08.2026

⁴³Gallagher-Studie, März 2026, zitiert nach Claims Journal, 20.07.2026

Wie schnell sich hier ein Markt entwickelt, ist offen. Deloitte prognostiziert globale KI-bezogene Jahresprämien von 4,7 bis 4,8 Mrd. USD im Jahr 2032 bei einer durchschnittlichen jährlichen Wachstumsrate von rund 80 %.⁴⁴ Die Nachfrageseite ist jedenfalls vorhanden: Über 90 % von 600 befragten Versicherungsentscheidern in Unternehmen zeigen Interesse an einer Deckung für GenAI-Risiken, zwei Drittel würden dafür mindestens 10 % höhere Prämien zahlen; 71 % haben generative KI in mindestens einer Funktion implementiert. Als Top-Risiken nennen sie Cybersicherheit, Drittparteien-Haftung und Betriebsunterbrechung.⁴⁵

**4,7–4,8 Mrd.
USD**

globale KI-bezogene Jahresprämien
2032 (Prognose)

rund 80 %

durchschnittliche jährliche
Wachstumsrate

über 90 %

der befragten
Versicherungsentscheider zeigen
Interesse an GenAI-Deckung

Quelle: Deloitte; The Geneva Association

KI in der Verteidigung – und was Unternehmen jetzt tun sollten

KI ist nicht nur ein Risiko: Sie hebt auch die Cyber-Sicherheit auf eine neue Ebene, indem sie eine schnellere und automatisierte Erkennung von und Reaktion auf Bedrohungen ermöglicht. Der IBM Cost of a Data Breach Report 2026 quantifiziert beides. Auf der Angriffsseite: **Mehr als jede vierte böswillige Attacke war KI-gestützt**; diese Angriffe kosteten durchschnittlich rund 6 Mio. USD, etwa 1 Mio. USD über dem Durchschnitt, und stiegen um 56 % gegenüber dem Vorjahr. Knapp die Hälfte davon waren Deepfake-Impersonationen, rund ein Fünftel KI-generierte Malware. Auf der Verteidigungsseite: **KI und Automatisierung im Sicherheitsbetrieb sparten knapp 2 Mio. USD je Datenleck** und verkürzten die Bewältigung um etwa zwei Monate.⁴⁶

Der bemerkenswerteste Befund des Reports betrifft jedoch ein Risiko, das viele Unternehmen unterschätzen: **Shadow AI**. Der Anteil von Shadow AI an Sicherheitsvorfällen hat sich auf 43 % verdoppelt; in rund der Hälfte dieser Fälle kam es zu Datenverlust oder -kompromittierung, in 40 % zu Betriebsstörungen. Knapp 70 % der betroffenen Organisationen hatten **keine** KI-Governance-Richtlinien, und 92 % der KI-Sicherheitsvorfälle gingen mit fehlenden Zugriffskontrollen einher. Über 20 % der Organisationen meldeten Angriffe direkt gegen KI-Modelle oder -Anwendungen.⁴⁷

Damit schließt sich der Kreis zur Haftungsfrage: Der unkontrollierte Einsatz von KI-Tools durch Mitarbeitende ist gleichzeitig ein Cyber-Risiko, ein Datenschutzrisiko und – über die Organisationspflichten – ein D&O-Risiko. Und er ist der Punkt, an dem Prävention am günstigsten ist.

Der unkontrollierte Einsatz von KI-Tools durch Mitarbeitende ist gleichzeitig ein Cyber-Risiko, ein Datenschutzrisiko und – über die Organisationspflichten – ein D&O-Risiko.

Ihr Finlex Team

⁴⁴Deloitte Center for Financial Services, zitiert nach Digital Insurance, 11.08.2025

⁴⁵The Geneva Association, Pressemitteilung v. 02.10.2025, sowie Report Oktober 2025 – Befragung in China, Frankreich, Deutschland, Japan, UK und USA

⁴⁶IBM, Cost of a Data Breach Report 2026, veröffentlicht 29.07.2026 – Basis über 600 Organisationen, Zeitraum März 2025 bis Februar 2026

⁴⁷IBM, Cost of a Data Breach Report 2026, 29.07.2026

Autorenprofile



Andrea Schmidbauer

Andrea Schmidbauer ist Chief Broking Officer (CBO) bei Finlex und verantwortet damit die Bereiche Management Liability und Cyber spartenübergreifend. Sie verfügt über 16 Jahre Berufserfahrung in der (Rück-)Versicherungsbranche und umfassende und langjährige Expertise vor allem im Bereich der Cyber-Versicherung. Als Chief Broking Officer hat sie es sich zur Aufgabe gemacht, fachliche Expertise mit den technologischen Lösungen von Finlex zu kombinieren.



Dr. Sven Erichsen

Dr. Sven Erichsen begleitet als Non-Executive Director bei Finlex vor allem die Großkundenbetreuung, sowie komplexe Cyber-Ausschreibungen. Zudem hat er sich in seiner aktuellen Rolle als AI Officer bei Finlex der sicheren Anwendung von KI-Systemen verschrieben. Er ist seit Markteinführung der Cyber-Versicherung (2011) auf die Beratung von Kunden und Kooperationsmaklern spezialisiert und blickt auf insgesamt 35 Jahre Berufserfahrung als Versicherungsmakler bei Großmaklern, im eigenen Unternehmen und bei Finlex zurück.



Patrick Maier

Patrick Maier ist seit dem 01.01.2025 bei Finlex. Zum 01.10.2026 hat er die Rolle als Vice President Cyber übernommen und verantwortet somit die Weiterentwicklung und den Ausbau der Cyber-Sparte. Durch seine 7-jährige Tätigkeit bei verschiedenen Versicherern konnte er umfassende Erfahrungen in der Kundenberatung, der Umsetzung von IT-Projekten sowie in der fachlichen Betreuung von Cyber-Risiken sammeln. Neben der Fachlichkeit stehen für ihn die hochwertige Beratung und Betreuung der Kunden und Makler im Fokus.



Yannick Berkemeier

Yannick Berkemeier ist bereits seit vier Jahren teils des Cyber Broking Teams bei Finlex und hat zum 01.10.2026 in der Funktion als Head of Broking Cyber die Leitung des Teams übernommen. Er verfügt über fundiertes Fachwissen im Bereich IT-Security und Cyber-Versicherung und wird durch sein verbindliches und professionelles Auftreten in der Anbahnung und dem Abschluss von Cyber-Verträgen für Großkunden von Geschäftspartnern sehr geschätzt.



Elke Seiz

Elke Seiz ist Head of Claims & Insurance Legal bei Finlex. Sie verfügt über fundierte Erfahrung in der Bearbeitung komplexer Financial-Lines-Schadenfälle. Vor ihrer Tätigkeit bei Finlex war sie in der Schadenbearbeitung eines globalen Industrierversicherers tätig und kennt die Schadenregulierung damit auch aus der Perspektive des Versicherers.



Pressekontakt:

Finlex GmbH

E-Mail: marketing@finlex.io

Telefon: +49 (0) 69/8700 142-00

finlex.io