Bundesverband Deutscher Versicherungs-Makler e.V.

PRESSE-INFORMATION

Hamburg, 09. Oktober 2025

Cyber-Risiken und –versicherung

Aktuelle (Markt-) Entwicklungen und der Einfluss von KI auf Risiko und Risikoprüfung.

Inhalt

Stimmungsbild zum Renewal

Die Cyber-Versicherung in der DACH-Region setzt ihren Wachstumskurs fort. Versicherer wollen das **Neugeschäft fördern** und Marktdurchdringung erhöhen. Nachdem die letzten Jahre in großen Teilen durch den Anstieg von Ransomware-Fällen geprägt waren und die Prämien als Konsequenz daraus zeitweise stark angezogen haben, hat sich die Schadensituaion inzwischen stabilisiert. **2025 steht für eine weitere Normalisierung der Cyber-Sparte:** Cyber-Risiken werden von Unternehmen zunehmend als zentrales Managementthema angesehen, und Versicherer erkennen darin langfristige Geschäftschancen. Viele Versicherer – sowohl etablierte als auch neue – **bewerben ihr Cyber-Offering wieder prominenter**, da die Nachfrage hoch bleibt. **Medienwirksame Großschäden** (wie z.B. Hackerangriffe auf kritische Infrastruktur oder bekannte Konzerne) haben das **Risikobewusstsein** in den Chefetagen geschärft. Die Geschäftsführung eines Unternehmens –

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

egal ob klein oder groß – kann sich kaum noch erlauben, *keine* Cyber-Versicherung zu besitzen, ohne kritische Nachfragen zu erhalten oder sich Haftungsrisiken auszusetzen. Selbst im Mittelstand ist das Thema angekommen: Die Zahl der Cyber-Abschlüsse bei Finlex und anderen Marktplätzen steigt kontinuierlich.

Die Versicherer haben dementsprechend die in den Vorjahren reduzierten **Kapazitäten wieder erweitert** und ihre Angebote verbessert. Viele haben gelernt, mit Cyber-Risiken umzugehen, und konnten ihre Produkte auf Basis der Schadenerfahrung verfeinern. Die zuletzt so hohen Prämiensteigerungen (2020–2042 teils +100 % p.a.) liegen hinter; in einigen Fällen sind sogar **prämiensenkende Effekte** erkennbar – insbesondere, wenn ein Kunde in den vergangenen Jahren Sicherheitsstandards erhöht hat. Kurz: Die harte Marktphase 2021/2024 mit knappen Kapazitäten ist vorbei, 2025 ist die Cyber-Versicherung wieder **verfügbarer und bezahlbarer – zumindest für Unternehmen mit einer guten Risikoqualität**.

Allerdings bleibt der Markt noch vorsichtig. Die **Schadenlage** entspannte sich 2024/2025 leicht (dazu später mehr). Aber keiner der Akteure vergisst, dass Cyber ein hochvolatiles Risiko ist: Einzelne Extremevents (wie z.B. gerade die Schadenfälle LandRover Jaguer und Collins Aerospace) können viele Policen gleichzeitig treffen (Stichwort Kumul). Deshalb verfolgen Versicherer beim Expansionskurs ein wachsames Auge. Dennoch überwiegt Optimismus, dass man Cyber-Risiken beherrschbar machen kann, zumal das **Netzwerk der Schadendienstleister** (Incident Response, Forensik etc.) immer besser funktioniert.

Auswirkungen auf den Cyber-Markt: Schadentrends, Anbieterwechsel und Umfeld

Der Cyber-Versicherungsmarkt 2025/2026 steht an einem interessanten Punkt der Entwicklung: Einerseits treiben **technologische und kriminelle Entwicklungen** die Risikolandschaft ständig weiter, andererseits formen Marktereignisse und Umweltfaktoren die geschäftlichen Rahmenbedingungen.

Schadentrends & Bedrohungslage: Die letzten Jahre haben gezeigt, dass Cyber-Schäden zyklisch auftreten können. 2022 war vielerorts ein Tiefpunkt mit Rekordschäden, die Folgejahre hingegen etwas ruhiger, wenngleich nicht entspannt. Insbesondere blieb die Anzahl der Schadenmeldungen hoch. So warnen die Experten bereits: *„Ransomware is back with a vengeance in 2025.“* Tatsächlich ist seit Q4 2024 zu beobachten, dass neue **Ransomware-Gruppen** auftreten und die Angriffe wieder zunehmen. Insbesondere **“Crime-as-a-Service”** floriert:

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Fertige Hacker-Toolkits und *Ransomware-as-a-Service* ermöglichen auch weniger versierten Kriminellen Angriffe durchzuführen.

Die Folge sind zahlreiche Attacken, oft gegen mittelständische Ziele, die sich in der Summe bemerkbar machen.

Auch der stetig zunehmende Einsatz von Künstlicher Intelligenz stellt die Cyber-Versicherung vor teils große Herausforderungen – vor allem Angriffsszenarien rund um Cyber-Kriminalität, inklusive der sog. „Fake President"-Angriffe – einer Form des Social Engineerings, bei der Angreifer versuchen, sich als eine vertraute oder hochrangige Führungsperson auszugeben, um Mitarbeiter dazu zu bringen, Geldüberweisungen zu tätigen oder sonstige vertraulichen Informationen preiszugeben – sind dadurch immer schwieriger zu umgehen. Waren beispielsweise Phishing-Mails in ihren Anfangstagen noch geprägt von schlechter Sprache und wenig Kontext, so haben sich diese mit Hilfe von KI zu gut getarnten Mails mit persönlicher Ansprache und Kontext entwickelt. Künstliche Intelligenz ermöglicht mittlerweile sogar täuschend echte Telefon- oder Videocalls, bei denen Stimmen und Gesichter der Angreifer so manipuliert werden, dass sie kaum von den imitierten Personen zu unterscheiden sind. KI sucht inzwischen automatisiert nach Schwachstellen und führt autonom die ersten Angriffsschritte durch.

Die Sensibilisierung und kontinuierliche Schulung der Mitarbeiter sind damit wichtiger denn je!

Marktveränderungen durch Anbieter

Der Ausstieg einzelner Player – sei es aus Gründen des Risikoappetits oder der finanziellen Lage – sorgte in der zweiten Jahreshälfte 2024 kurzfristig für Unruhe im deutschen Cyber-Versicherungsmarkt und hat sowohl bei Maklern als auch bei Versicherern zu großem Umdeckungsbedarf und Portfolioverschiebungen geführt. Das insgesamt positive Stimmungsbild des Marktes – auch bedingt durch den Eintritt von weiteren Playern im Markt und der damit einhergehende Anstieg von zur Verfügung stehenden Kapazitäten – ermöglichte es Maklern aber, vergleichsweise einfach alternative Lösungen für betroffene Kunden zu finden und die Verträge entsprechend mit stabilen Konditionen zu anderen Marktteilnehmern umzudecken.

Dem gegenüber steht der bereits erwähnte Markteintritt mehrerer **neuer Player** im deutschen Markt. Hierzu zählen sowohl MGAs, die sich v.a. über den Einsatz hauseigener Scanning-Technologie und präventiver Service-Tools von den klassischen Anbietern

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

differenzieren, als auch der Einstieg bzw. Ausbau des Risikoappetits von etablierten Versicherern in der Cyber-Sparte.

Zu den noch neueren und am stärksten vertretenen MGAs am Markt zählen beispielsweise Coalition (US-Anbieter, der in Kooperation mit Allianz als Risikoträger nun auch im deutschen Markt Kapazitäten für Unternehmen bis 1 Mrd. EUR Umsatz anbietet), Stoik (französisches Start-up mit Fokus auf Cyber-Versicherung für KMUs), sowie Baobab (ebenfalls mit Fokus auf KMUs). Seit Anfang 2025 ist auch CFC (etablierte MGA aus dem Londoner Markt) als Teil ihrer Wachstumsstrategie in Europa auf dem deutschen Cyber-Markt vertreten.

Unter den traditionellen Versicherern mit deutlich gestiegenem Risikoappetit in der Cyber-Sparte im Vergleich zu den Vorjahren sind HDI Global, Liberty oder Generali zu nennen. Für Kunden bedeuten diese neuen Anbieter **mehr Auswahl und oft innovative Leistungen**.

Auch die Grundlage der Risikobewertung unterscheidet sich zunehmend – während der traditionellen Versicherer die Risikosituation weiterhin im Kern auf Basis von Risikofragebögen oder -dialogen bewerten, nutzt der Großteil der neuen Marktteilnehmer überwiegend die eigens entwickelte Scan-Technologie, um sich ein eigenes Bild über die IT-Sicherheit des Kunden zu verschaffen und so die Anzahl der seitens des Kunden zu beantwortenden Fragen teils deutlich zu reduzieren. Aber auch die etablierten Player greifen inzwischen auf die Scan-Technologie zur kontinuierlichen Bewertung ihres Portfolios zurück.

Regulatorische Treiber gibt es auch im Cyber-Umfeld: NIS-2 (oben erwähnt) zwingt viele Mittelständler zur Verbesserung ihrer IT-Security, was tendenziell das Risikoprofil verbessert und die Nachfrage nach geeignetem Versicherungsschutz erhöht.

Zusammengefasst: Das Marktumfeld 2025/2026 ist für Cyber-Versicherungen von **positiver Dynamik** geprägt (Nachfrage, neue Anbieter) und gleichzeitig weiterhin großen **Unsicherheiten** (neue Angriffsarten, Großschäden möglich) unterworfen.

Zeichnungsverhalten der Cyber-Versicherer

Die Underwriter in der Cyber-Versicherung haben in den letzten Jahren eine steile Lernkurve durchlaufen. 2025 zeigt sich das Zeichnungsverhalten einerseits **offener** für neue Risiken, andererseits weiterhin **diszipliniert** bei Mindeststandards.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Risikoselektion und -bewertung: Dreh- und Angelpunkt für die Zeichnungsbereitschaft der Versicherer ist weiterhin die Risikoerfassung und -bewertung – ohne die Umsetzung und Befolgung solider Cyber-Hygiene-Standards ist ein Zugang zur Cyber-Deckung für Unternehmen nicht mehr möglich.

Auch die ansonsten weichere Marktphase ändert hieran im Grundsatz nichts, die konkreten Anforderungen unterscheiden sich je Versicherer allerdings in den Details. **Sogenannte „Outside-In-Scans“** der IT-Systeme gehören dabei mittlerweile zum Standard: Versicherer nutzen Tools, um z.B. offene Ports, auslaufende Zertifikate oder bekannte Schwachstellen eines Antragstellers aufzuspüren. Diese automatisierten Scans fließen in die Risikobewertung ein – ein hoher Befund kann zu Rückfragen oder sogar Ablehnung führen. Während die technologisch orientierteren MGAs dabei eigene Technologie nutzen, greifen traditionelle Versicherer hier in der Regel auf Drittanbieter, v.a. Cysmo, zurück. Darüber hinaus werden weiterhin **detaillierte Fragebögen** eingesetzt, die sich im Laufe der Jahre stetig weiterentwickelt haben.

Die zu bearbeitenden Themenfelder der IT- sicherheitstechnischen Mindestanforderungen inzwischen weitgehend einheitlich: Datensicherung, Patch-Management, Berechtigungskonzepte, Multi-Faktor-Authentifizierung (MFA), Altsysteme etc. Anbieter unterscheiden sich jedoch teils drastisch in dem Detaillierungsgrad, mit dem sie ihre Anforderungen formulieren und vorgeben und in der Praxis auch darin, ob und ggfs. wie sie mit (noch) nicht optimalen Verhältnissen umgehen können.

Die gute Nachricht: Viele Unternehmen haben diese Security-Basics mittlerweile implementiert – oft getrieben durch die Forderungen der Versicherer selbst in den letzten Renewals. **Die Qualität der versicherten IT-Risiken hat sich verbessert.** Dies trägt mit zur Entspannung des Marktes und der Schadensituation bei.

Zeichnungspraxis: Versicherer segmentieren weiterhin stark nach Unternehmensgröße und Branche. Für **Kleinunternehmen** (< 50 Mio. EUR Jahresumsatz) gibt es meist standardisierte Deckungen mit vereinfachter Zeichnung – oft voll digital über Plattformen, wie beispielsweise auch über die **Finlex Cyber Fast Lane**. Hier ist der Abschluss einer Police binnen Minuten anhand weniger Datenpunkte (Branche, Umsatz, IT-Mindestanforderungen) möglich. Für **größere Mittelständler und Konzerne** bleibt das Underwriting zwar individueller, auch hier sind Underwriter aber kooperativer geworden: War 2021 noch häufig ein rigoroses „Checkliste nicht 100 % erfüllt = kein Angebot“ zu erleben, so geht man 2025 öfter ins Gespräch und versucht gemeinsam mit Maklern und Endkunden Lösungen zu finden.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Mindestanforderungen werden als Vorbehalte für die Eindeckung aufgegeben, bei weniger kritischen Themenfeldern sind Versicherer auch bereit, den Kunden mittels Auflagen im Versicherungsvertrag eine realistische Übergangsfrist zu gewähren. Allerdings gibt es rote Linien: Wer **kritische Schwachstellen** nicht behebt oder die Basics weiterhin nicht erfüllt, hat es weiterhin schwer, Versicherungsschutz zu finden.

Ein wichtiges Thema im Underwriting ist auch die **Aufklärungspflicht und Anzeigegenauigkeit** der Versicherungsnehmer. Mehrere Gerichtsentscheidungen in Deutschland 2023/2024 haben verdeutlicht, wie kritisch falsche oder unvollständige Antworten im Cyber-Antrag sein können.

So entschied das LG Kiel (bestätigt durch OLG Schleswig 2025), dass ein Versicherer den Vertrag wegen **arglistiger Täuschung anfechten** kann, wenn der Versicherungsnehmer IT-Sicherheitsfragen „ins Blaue hinein“ beantwortet und diese Angaben tatsächlich falsch sind. Im konkreten Fall hatte ein IT-Leiter im Antrag bestätigt, alle Systeme seien up-to-date geschützt, obwohl veraltete ungeschützte Server liefen – nach einem Schaden verweigerte der Versicherer die Leistung zu Recht aufgrund dieser Falschangaben. Demgegenüber hat das LG Tübingen 2023 klargestellt, dass nicht **jede** falsche Antwort automatisch zum Verlust des Schutzes führt – es komme auf Verschulden und Kausalität an.

Dennoch: Versicherer sind sensibilisiert und pochen darauf, dass Kunden **sorgfältig und wahrheitsgemäß** antworten. Viele integrieren Warnhinweise in die Anträge.

Für Makler heißt das, ihre Kunden zur Genauigkeit anzuhalten, um im Schadenfall nicht den Schutz zu gefährden.

Kapazitätsmanagement: Kapazitäten der Versicherer haben sich im Vergleich zur Hartmarktphase wieder deutlich erhöht. Waren zwischenzeitlich nicht mehr als 5 Mio. EUR Kapazität aus einer Hand zu bekommen, so sind einige Versicherer mittlerweile wieder bereit, 10 Mio. EUR, teilweise sogar bis zu 15 Mio. EUR Eigenkapazität bereitzustellen. Vor allem im Bereich der Exzedenten ergeben sich durch die erhöhte Anzahl der Marktteilnehmer wieder attraktive Möglichkeiten für Versicherungsnehmer.

Pricing: Im letztjährigen Renewal waren nur noch in wenigen Fällen Prämiensteigerungen zu verzeichnen. Im eigenen Bestand haben Versicherer sich darauf konzentriert, Konditionsanpassungen vor allem bei aus ihrer Sicht kritischen Risiken vorzunehmen; in diesen Einzelfällen spielten Prämienanpassungen sowie Auflagen zur Risikoverbesserung eine durchaus gleichwertige Rolle.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Insgesamt hat sich der Preisdruck der vergangenen Jahre mittlerweile deutlich entspannt und Kunden können Cyber-Versicherungsschutz zu attraktiven Konditionen einkaufen – vorausgesetzt das IT-Sicherheitsniveau passt.

Zusammenfassend: Das Zeichnungsverhalten 2025 ist geprägt von **positivem Aufschwung**. Versicherer haben klare Anforderungen, arbeiten aber konstruktiv mit den Kunden zusammen und geben Zeit und Unterstützung, die Anforderungen umzusetzen.

Neue Analysetechniken (Scans, Scores) erhöhen die Transparenz.

Wichtig für Kunden ist, die **Spielregeln** einzuhalten – dann steht einer Cyber-Deckung in den meisten Fällen nichts im Weg. Die „Ablehnungsquote“ im Markt sinkt, weil sich Versicherer und Versicherungsnehmer in der Mitte treffen: Unternehmen verbessern ihre Sicherheit, Versicherer willigen dafür in Deckung und fairere Preise ein.

Schadenentwicklung Cyber

Die Schadenentwicklung in der Cyber-Versicherung kann für 2024/2025 als **durchwachsen, aber nicht dramatisch** beschrieben werden. Es zeigen sich einerseits erfreuliche Tendenzen, andererseits auch klare Warnsignale.

Frequenz: Nach wie vor beobachten wir eine hohe Anzahl an Cyber-Angriffen und entsprechend auch eine unverändert **hohe Schadenquote**. Wir beobachten aber auch, dass viele Unternehmen ihre Cyber-Sicherheit deutlich ernster nehmen und z.B. durch Investitionen das Sicherheitsniveau erhöht und Backups verbessert haben. Dadurch führen viele Angriffe nicht mehr zwangsläufig zu hohen Schäden durch Datenverluste und/oder Betriebsunterbrechungsschäden.

Schadenarten: Das **typische Schadenbild** bei Großschäden in Cyber ist weiterhin von **Ransomware-Angriffen** geprägt, inklusive **Datenverschlüsselung** und oft **Datenabfluss**. Diese Fälle machen wertmäßig den größten Teil der Schadenzahlungen aus. In der Anzahl dominieren jedoch **kleinere Vorfälle** wie Phishing-Angriffe oder kompromittierte E-Mail-Accounts. Viele verbleiben im Stadium der Verdachtsebene und verursachen keine hohen Kosten. Zu beobachten sind zudem vermehrt **Vertrauensschaden**-Fälle (z.B. Fake President oder Payment Diversion Fraud), die sich zumeist im fünf- bis niedrigen sechsstelligen Bereich bewegen. Sie können dennoch die Frequenz treiben.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Schadenausmaß: Die **Durchschnittskosten pro Cyber-Schaden** variieren zumeist nach der Größe des betroffenen Unternehmens. Bei größeren Unternehmen kann ein Ransomware-Angriff oft mehrere Millionen Euro kosten – Forensik, Datenwiederherstellung, Produktionsausfall, Lösegelder und PR-Kosten summieren sich schnell. 2024/2025 gingen viele Fälle jedoch „glimpflich“ aus. In rund **25 % aller Cyber-Versicherungsfällen**, die Finlex begleitet hat, konnte bereits durch die **sofortigen Erstmaßnahmen** (Incident Response Team, Forensiker) Schlimmeres verhindert werden. Die **24/7-Notfallhotlines** und eine schnelle Intervention zahlen sich hier aus.

Die Versicherer haben dedizierte Panels von IT-Security-Firmen, die sofort eingreifen. Die Finlex Statistik legt nahe: Ein Viertel der gemeldeten Fälle konnte durch solche **Erstmaßnahmen gelöst** werden, ohne dass der Schaden eskalierte. Das ist eine positive Entwicklung und zeigt, wie wichtig die Service-Komponente ist.

Regulierungspraxis: Die Cyber-Schadenregulierung hat nach unserem Empfinden 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.

Konflikte entstehen manchmal, wenn der Versicherer versucht, Entscheidungen zu diktieren – etwa ob Lösegeld gezahlt wird oder nicht. Hier zeigt sich die Tendenz, dass einige Versicherer restriktiver beim **Thema Lösegeldzahlung** wurden. Zwar sehen fast alle Policen solche Zahlungen vor, doch einige Versicherer verfolgen zunehmend eine restriktive Linie und setzen auf Wiederherstellung aus Backups. Entschädigt werden die Kosten in jedem Fall, aber der Weg unterscheidet sich – und soll das Signal vermeiden, dass Lösegeld eine Standardlösung ist. Dieser **Policy-Shift** (weg vom „Einfach bezahlen“) wird 2025/2026 wohl weitergehen.

Deckungsablehnungen: Einige Cyber-Schäden führten zu **Deckungsstreitigkeiten**, meist wegen Obliegenheitsverletzungen. Urteile wie jene des LG Tübingen (pro Versicherungsnehmer) oder LG Kiel (pro Versicherer) zeigen, dass im Einzelfall genau geprüft wird, ob z.B. ein Rücktritt gerechtfertigt ist. Für die Praxis heißt das: Ablehnungen geschehen, sind aber oft ein Schritt hin zu Vergleichsverhandlungen. Die Versicherer sind sich bewusst, dass eine harte Regulierungspraxis dem Markt schadet. Daher versucht man eher, auch bei Obliegenheitsverletzungen Kulanzlösungen zu finden (z.B. Quotelungen),

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

sofern kein hochgradiges Fehlverhalten vorliegt. Dennoch: Gab es arglistige Falschangaben, scheuen Versicherer nicht, konsequent zu kündigen und keine Leistungen zu zahlen – gedeckt von der Rechtsprechung.

Versicherungsbetrug ist in Cyber zum Glück bislang kein großes Thema. Vereinzelt prüften Versicherer kritisch, ob ein „Angriff" vielleicht nur vorgetäuscht war oder ob der etwaige geltend gemachte Betriebsunterbrechungsschaden zu hoch angesetzt wurde. Relevant in diesem Zusammenhang ist jedoch eher, ob **Überschneidungen mit anderen Versicherungen** vorliegen.

Z.B., wenn die oben bereits beschriebenen Vertrauensschaden-Fälle (z.B. Fake President oder Payment Diversion Fraud) auftreten. Hier stellt sich die Frage, ob Versicherungsschutz primär über einen etwaigen Crime-Baustein in der Cyber-Police oder über eine vorhandene Vertrauensschadenversicherung besteht.

Die bisherigen Schadenerfahrungen sind etwas **besser als befürchtet**. Kein massiver Anstieg, viele abgefangene kleine Schäden, größere systemische Events blieben aus. Doch angesichts der sprunghaften Natur von Cyber-Risiken wäre es trügerisch, daraus Entwarnung abzuleiten.

Schadenausblick Cyber

Für 2025/2026 ist mit einer gleichbleibend hohen Anzahl an Cyber-Schadenfällen zu rechnen, denn die Sicherheitslage bleibt angespannt. Cyber-Angriffe sind unausweichlich und es bleibt entscheidend, wie vorbereitet ein Unternehmen den Angriff bewältigt. Dies zeigen auch die beiden Großschäden aus den letzten Wochen (Jaguar LandRover und Collins…)

Insbesondere in Bezug auf die Zahlung von Lösegeldern und die Prüfung von Antragsfragen sowie die Erfüllung von technischen Obliegenheiten ist damit zu rechnen, dass die Versicherer deutlich strenger bei der Regulierung hinschauen und versuchen werden, die Deckung teilweise abzulehnen.

Zu befürchten ist, dass wieder vermehrt **State-sponsored Attacks** auftreten. Insbesondere wenn geopolitische Konflikte eskalieren (etwa Cyber-Operationen im Kontext Ukraine oder Taiwan), könnten auch deutsche/europäische Firmen Kollateralschäden erleiden oder direkt angegriffen werden.

Neuartige Schadenszenarien könnten zudem auftreten, wenn ein **Angriff auf einen Cloud-Dienstleister** oder große Software-as-a-Service-Anbieter erfolgreich wäre, der Tausende Unternehmen gleichzeitig lahmlegt.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Insbesondere die Konzentration von Cloud-Diensten ist mit Sorge zu betrachten. Auch wenn die großen Anbieter wie AWS äußerst sichere Systeme haben, stellt ein erfolgreicher Angriff ein Kumulrisiko dar, das sowohl die Verfügbarkeit von Forensikern und IT-Dienstleistern als auch die Schadenabteilungen von Versicherern an ihre Kapazitätsgrenzen bringen würde.

Auch im Hinblick auf die **Regulatorik** wird 2025/2026 interessant. Insbesondere bleibt abzuwarten, wie die Behörden ihre Befugnisse nutzen, ob es z.B. zu mehr Bußgeldern nach der DSGVO kommen wird und wie NIS-2 Anwendung findet.

Positiv ist, dass immer mehr Unternehmen Incident Response trainieren und vorbereiten. Das dürfte auch 2025/2026 die **Schadenminderung** verbessern. Zudem wird der Markt für die **Bekämpfung und Verhinderung von Cyber-Kriminalität** professioneller. Z.B. investieren immer mehr Versicherer in Threat Intelligence und externe Schwachstellenscans. Die gewonnen Informationen werden mit den Versicherungsnehmern geteilt, so dass Angriffe erkannt und verhindert werden, bevor sie eintreten oder große Wellen schlagen. Dies gilt umso mehr, je größer ein Unternehmen ist. Wir vermuten daher, dass sich Ransomware-Angriffen auf mittelgroße und weniger gut geschützte Unternehmen verlagern werden.

Ein Aspekt, der stetig wichtiger wird, sind die **Cyber-Claim-Handling-Kapazitäten**. Bereits jetzt ist es herausfordernd, genug qualifizierte Forensiker und Spezialisten für parallele Großschäden zu finden. Sollte eine Großschadenwelle kommen oder sich ein Kumulrisiko verwirklichen, wird der Engpass an Experten ein zentrales Problem.

Die Empfehlung sowohl für Versicherer als auch Unternehmen lautet: **Wachsam bleiben und in Prävention investieren.** Ransomware, systemische Risiken und staatlich gestützte Angriffe sind reale Bedrohungen, doch Prävention und Incident Response gewinnen an Wirkung. Unternehmen sollten ihre Investitionen in die IT-Infrastruktur weiter steigern. Nicht zuletzt sollten auch die Versicherer ihre Schadenabteilungen, Notfallhotlines und Dienstleister-Netzwerke aufrüsten, sodass die Assistance-Leistungen im Schadenfall noch besser und schneller greifen.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Fazit

Der Versicherungsmarkt für Cyber in 2025/2026 präsentiert sich insgesamt deutlich **aufgehellt und stabilisiert**, mit erweitertem Angebot und professionellerem Handling. Beide Sparten profitieren vom gestiegenen Risikobewusstsein der Unternehmen und von technischen sowie versicherungstechnischen Innovationen. Dennoch sind die Herausforderungen – seien es ökonomische Risiken, neue Haftungsfelder oder die unberechenbare Kreativität von Cyber-Kriminellen – nicht zu unterschätzen. Ein sachlich-analytischer, ganzheitlicher Blick auf Risiko und Versicherungsschutz ist wichtiger denn je.

Exkurs zum Einsatz von Künstlicher Intelligenz

Versicherungsnehmer und Versicherer (und auch Versicherungsmakler) sind in einem sich wandelnden regulatorischen Umfeld unter Wettbewerbsdruck stehend gezwungen, KI-Tools einzuführen. In der Versicherungsbranche wird es nur so möglich sein, dem sich abzeichnenden Fachkräftemangel wirksam zu begegnen.

Auch die Angreifer setzen bereits in erheblichem Umfang KI ein, um Ransomware-Attacken zu automatisieren und zu skalieren, ausgeklügelte Schadsoftware zu entwickeln und überzeugende Phishing-Kampagnen zu konzipieren. Insbesondere die Suche nach IT-Systemen mit exponierten Schwachstellen geht mit der Unterstützung von KI schneller und effizienter.

Gleichzeitig hebt KI die Cyber-Sicherheit auf eine neue Ebene, indem sie eine schnellere und automatisierte Erkennung von und Reaktion auf Bedrohungen ermöglicht und die Cyber-Resilienz von Unternehmen stärkt. IBM zufolge (BM, Cost of a Data Breach Report 2024) waren die Kosten durch Datensicherheitsverletzungen bei Unternehmen, die KI-basierte Sicherheits- und Automatisierungslösungen nutzen, zuletzt um durchschnittlich 2,2 Millionen US-Dollar niedriger als bei Unternehmen, die keine derartigen Lösungen einsetzen. KI verschafft Unternehmen in der Verteidigung gegen Angriffe also einen Vorteil. Sie müssen kontinuierlich in KI-gestützte Erkennungstools investieren. Tun sie das nicht, liegt der KI-Vorteil bei den Angreifern, die dieses tun.

Auch die fortschreitende Regulierung erhöht Anforderungen an Cyber-Resilienz und fördert den Einsatz von KI. Neue Regelwerke wie die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) und die EU-Richtlinie zur Sicherung von Netzwerk- und Informationssystemen (NIS-2) sollen die Cyber-Sicherheitsstandards in kritischen Sektoren einschließlich der zugehörigen Lieferketten anheben.

Bundesverband Deutscher Versicherungsmakler e.V. (BDVM)
Admiralitätstr. 58, 20459 Hamburg
Tel.: +49 (0) 40/36 98 20-0
Fax: +49 (0) 40/22 81 70 569
E-Mail: bdvm@bdvm.de
www.bdvm.de

Sie enthalten Vorgaben für ein verbessertes Risikomanagement, Vorfallmeldungen und Resilienz Tests. Damit werden sie vor allem mittelgroßen Unternehmen mit ihrer derzeit noch unterentwickelten Cyber-Sicherheitsinfrastruktur zugutekommen.

Ansprechpartner:
Dr. Sven Erichsen
Non-Executive Director Finlex GmbH
Telefon: 0151 6494 1213
E-Mail: sven.erichsen@finlex.de