KESSLER

Cyber Message 2026

Risk and Insurance



MIT SICHERHEIT VORAUS.

Cyber Message 2026

Cyber ist längst mehr als ein IT-Risiko. Angriffe treffen Unternehmen über Dienstleister, Schäden entstehen an der Schnittstelle von Täuschung und Technik und künstliche Intelligenz (KI) wirft neue Haftungsfragen auf. Der Umgang mit Cyber-Risiken hat sich über die Jahre erweitert: von der technischen Abwehr und Prävention hin zur Vorbereitung auf den Ernstfall. Zehn Jahre Cyber-Erfahrung bei Kessler zeigen: Anspruchsvoll wird es insbesondere dort, wo Unternehmensführung, Haftung und Versicherung zusammentreffen und Verantwortlichkeiten, Prozesse und Deckungen im Vorfeld nicht aufeinander abgestimmt wurden.

Rechtliche Veränderungen

CYBER-GOVERNANCE ALS FÜHRUNGSAUFGABE

Cyber-Sicherheit ist keine reine IT-Aufgabe mehr, sondern eine zentrale Führungsaufgabe, die zunehmend unter rechtlichem Druck steht. Verwaltungsrat und Geschäftsleitung müssen Cyber-Risiken im Rahmen ihrer gesetzlichen Sorgfalts- und Aufsichtspflichten berücksichtigen. Dazu gehört, Cyber-Risiken als festen Bestandteil der Unternehmensführung, des Risikomanagements und strategischer Entscheide wie bei Outsourcing oder M&A-Transaktionen zu verankern. Gefordert sind eindeutige Verantwortlichkeiten, regelmässiges Reporting, angemessene Aufsicht und ein bewusster Umgang mit Restrisiken. Auch ein allfälliger Transfer von Cyber-Risiken ist zu prüfen und Entscheide sind nachvollziehbar zu dokumentieren. Werden Sorgfaltspflichten verletzt und entsteht daraus ein Schaden, können Organpersonen persönlich haftbar gemacht werden. Eine Organhaftpflichtversicherung (D&O) entbindet sie dabei nicht von der Erfüllung ihrer gesetzlichen Organpflichten.

HAFTUNG ZWISCHEN VERTRAG UND KUNDENERWARTUNG

Kunden verlangen heute nicht nur funktionierende Produkte und Dienstleistungen, sondern auch vertragliche Zusagen, dass digitale Komponenten, Daten und Systeme geschützt sind und verfügbar bleiben. Für Anbieter entsteht daraus ein Spannungsfeld. Je konkreter die Service-Level-Agreements sind, desto eher werden sie im Streitfall zum Haftungsmassstab. Wer zu viel verspricht, übernimmt Risiken, die technisch und organisatorisch nicht vollständig kontrollierbar und oft nur eingeschränkt versicherbar sind. In der Praxis zeigt sich: Haftpflichtdeckungen greifen grundsätzlich bei gesetzlicher und nicht bei vertraglich übernommener Mehrhaftung. Wichtig sind deshalb eine klare Risikoverteilung, realistische Zusagen und präzise Haftungsgrenzen.

KI ALS RISIKOTREIBER

Ein KI-Agent löscht versehentlich Produktivdaten, ein Chatbot macht eine falsche Zusage, ein KI-Tool verarbeitet Personendaten unrechtmässig: KI verstärkt bestehende Risiken. Sie kann Cyber-Angriffe beschleunigen, Phishing glaubwürdiger machen, Datenschutzverletzungen begünstigen, fehlerhafte Outputs erzeugen oder Diskriminierungsfragen auslösen. Je nach Schadenmechanismus können verschiedene Deckungen betroffen sein: Cyber bei Sicherheits- oder Datenschutzereignissen, Berufshaftpflicht bei fehlerhaften Empfehlungen oder Technologieleistungen, Crime bei betrügerisch ausgelösten Zahlungen und D&O bei Aufsichtsthemen. Die zentrale Frage lautet nicht, ob KI versichert ist, sondern ob bestehende Policen die relevanten KI-Anwendungsfälle sauber abbilden.

Aktuelle Risiken

TECHNOLOGIE-RISIKEN FÜR INDUSTRIE-UNTERNEHMEN

Viele Industrieunternehmen sind heute auch Technologieunternehmen. Sie entwickeln Software, bieten digitale Plattformen an oder ergänzen Maschinen mit IT-Dienstleistungen wie Fernwartung oder Software-as-a-Service.

Damit steigt die Komplexität der Haftungsrisiken. Die Grenzen zwischen Produkthaftpflicht, Berufshaftpflicht und Cyber verschwimmen. Was früher ein Maschinenschaden war, kann heute Softwareversagen, Datenschutzverletzung oder reiner Vermögensschaden sein. Dies bilden klassische Betriebs- und Produkthaftpflichtlösungen nicht immer ausreichend ab. Industrieunternehmen sollten deshalb ihre digitalen Leistungen systematisch erheben und im Risikomanagement prüfen.

Für grenzüberschreitend tätige Unternehmen verschärft die neue EU-Produkthaftungsrichtlinie die Haftungsrisiken: Ab 9. Dezember 2026 kann Software unter bestimmten Voraussetzungen als Produkt gelten; Softwarefehler oder unzureichende Updates können Produkthaftungsansprüche auslösen.

CYBER-CRIME-SZENARIO

«Bitte überweisen Sie dringend CHF 500'000.» Diese Nachricht scheint vom CEO zu stammen, ein Mitarbeitender führt die Zahlung aus. Doch die Anweisung ist gefälscht und das Geld weg. Welche Versicherung deckt den Schaden?

In der Schadenbegleitung sehen wir, dass solche Betrugsfälle technisch verbreitet sind: durch ein kompromittiertes E-Mail-Konto, über Phishing erlangte Zugangsdaten oder eine Rechnung mit geänderter Bankverbindung. Für Unternehmen bleibt es ein Vorfall; versicherungstechnisch zählt der Schadenmechanismus. Folgekosten wie Forensik oder Wiederherstellung können unter die Cyber-Deckung fallen, die Fehlüberweisung eher unter die Crime-Versicherung – oft mit Sublimits und Verifizierungspflichten. Je nach Versicherung ist derselbe Vorfall vollständig, teilweise oder gar nicht gedeckt.

Entscheidend ist deshalb nicht nur, welche Police besteht, sondern ob die Cyber-Crime-Szenarien umfassend geprüft wurden. Wer sich auf einzelne Deckungsbausteine verlässt oder Prozesse nicht dokumentiert, kann trotz Schaden leer ausgehen.

Cyber-Vorfälle

DIE VERSTECKTEN KOSTENTREIBER

Cyber-Vorfälle sind teuer, in der Schweiz jedoch unserer Erfahrung nach selten aufgrund von Schadenersatzforderungen. Die rechtlichen Hürden sind hoch: Nachzuweisen sind Verschulden, Kausalität und konkreter Vermögensschaden. In unserem Cyber-Portfolio entfallen deutlich unter 5 Prozent der Zahlungen, einschliesslich der Abwehr unbegründeter Ansprüche, auf Schadenersatz. Die Kostentreiber liegen bei Incident Response, Forensik, Wiederherstellung, Betriebsunterbrüchen, Meldepflichten und regulatorischen Anforderungen mit finanziellen, operativen und reputativen Folgen.

Für international tätige Unternehmen greift dies zu kurz. Je nach Rechtsraum fällt das Haftungsrisiko höher aus: In der EU drohen unter der DSGVO Bussgelder und Schadenersatzansprüche, in den USA Sammelklagen und Strafschadenersatz. Entscheidend sind deshalb nicht nur Unternehmenssitz, sondern auch Standort von Kunden, Tochtergesellschaften oder personenbezogenen Daten.

CYBER-ANGRIFFE AUF IT-DIENSTLEISTER

IT-Dienstleister sichern den Geschäftsbetrieb ihrer Kunden. Wird ein Anbieter kompromittiert, treffen die Folgen oft viele Kunden gleichzeitig: Betriebsunterbrüche, Datenabfluss und Migrationskosten. Der Fall Unico Data zeigt die Tragweite: Nach einem Ransomware-Angriff 2023 waren zahlreiche Kunden gleichzeitig offline. Ende 2025 stellte das Unternehmen den Betrieb ein – nicht wegen Sofortkosten von über CHF 1 Mio., sondern wegen Reputationsschäden und Kundenverlusten.

Wer trägt einen solchen Schaden? Verträge begrenzen Ansprüche häufig auf direkte Schäden. Folgekosten und Umsatzausfälle sind oft nur eingeschränkt ersatzfähig. Fällt der Dienstleister aus oder gibt er den Betrieb auf, laufen vertragliche Ansprüche ins Leere. Seine Cyber-Versicherung deckt in der Regel den eigenen Schaden, nicht denjenigen der Kunden.

Der Schutz muss deshalb beim eigenen Unternehmen ansetzen: Outsourcing-Verträge, Haftungslimiten, eigene Cyber-Deckung und Business-Continuity-Pläne sind regelmässig zu prüfen. Denn wer IT-Leistungen auslagert, gibt Systeme ab, nicht aber das Risiko.

LEBENSZYKLUS EINES CYBER-SCHADENS



01 **Meldung und Triage**
Verdacht prüfen, Krisenstab
Tipp: rasche Meldung und klar definierter Krisenstab

02 **Sofortmassnahmen**
Systeme isolieren
Tipp: Notfallplan vorab testen

03 **Forensik und Analyse**
Ursache und Umfang klären
Tipp: klare vertragliche Regelung mit IR-Anbieter

04 **Recht und Kommunikation**
Meldepflichten wahren
Tipp: OFAC-Check der Täter-gruppe vor Zahlung

05 **Wiederherstellung**
Systeme, Ertragsausfall
Tipp: keine Eigenversuche, damit Beweise gesichert werden

06 **Deckung und Regulierung**
Nachweis, Abrechnung
Tipp: Nachweis lückenlos von Beginn weg führen

Cyber-Versicherungsmarkt: 10 Jahre Cyber bei Kessler

Seit Kessler 2016 die erste Cyber-Police platziert hat, hat sich der Markt stark verändert. Ab 2020 folgte eine Phase der Verhärtung mit hohen Schäden, knappen Kapazitäten und steigenden Anforderungen an die Cyber-Sicherheit. Inzwischen hat sich der Markt entspannt. Zusätzliche Kapazitäten und ein intensiver Wettbewerb schaffen neue Spielräume bei der Platzierung. Gleichzeitig bleibt das Umfeld wegen KI-gestützter Angriffe, Lieferkettenrisiken und zunehmender Regulierung anspruchsvoll. Gute Sicherheitsstandards, klare Risikoangaben und belastbare Schadenprävention bleiben für die Versicherbarkeit entscheidend.

Heute begleiten wir Sie ganzheitlich mit einem spezialisierten Cyber-Team, bei Bedarf gemeinsam mit unserem Partner Marsh – von Self-Assessments und Reifegradanalysen bis zur Schadenbegleitung. Zudem haben wir für kleinere und mittlere Unternehmen eine auf ihre Bedürfnisse zugeschnittene Rahmenvertragslösung zu attraktiven Konditionen entwickelt. 2026 konnten wir die Cyber blue line für weitere drei Jahre platzieren. Unser Anspruch bleibt: Risiken frühzeitig erkennen, Resilienz stärken und Kunden im Ernstfall verlässlich begleiten.

ÜBER KESSLER

Kessler ist das führende Schweizer Unternehmen für ganzheitliche Risiko-, Versicherungs- und Vorsorgeberatung. Wir betreuen über 1'600 mittlere und grosse Schweizer Unternehmen aus Dienstleistung, Handel und Industrie sowie der öffentlichen Hand. Dank unserer Expertise in den einzelnen Wirtschaftsbranchen, unseren qualifizierten Mitarbeitenden und unserer führenden Marktstellung leisten wir einen wesentlichen Beitrag zum nachhaltigen Erfolg unserer Kunden. Als verlässlicher Partner begeistern wir sie und eröffnen ihnen durch den sicheren Umgang mit Risiken neue Perspektiven. Gegründet 1915, beschäftigt Kessler heute 390 Mitarbeitende am Sitz in Zürich und an den Standorten Basel, Bern, Genf, Lausanne, Luzern, Neuenburg, St. Gallen, Sion und Vaduz. Als Schweizer Partner von Marsh sind wir seit 1998 Teil eines Netzwerks mit Spezialistinnen und Spezialisten aus allen Gebieten des Risk Managements und mit grosser Erfahrung in der Betreuung globaler Versicherungsprogramme. Marsh ist ein weltweit führender Anbieter in den Bereichen Risiko, Rückversicherung und Kapital, People and Investments sowie Management Consulting und berät mit über 90'000 Kolleginnen und Kollegen Kunden in 130 Ländern (NYSE: MRSH).

Weitere Informationen finden Sie unter www.kessler.ch, www.marsh.com und www.corporate.marsh.com.

KESSLER & CO AG
Forchstrasse 95
Postfach
CH-8032 Zürich
T +41 44 387 87 11
www.kessler.ch

MARSH Network