KESSLER

Cyber Message 2025

Risk and Insurance

MIT SICHERHEIT VORAUS.

Geopolitische Spannungen, hybride Kriegsführung und KI-getriebene Angriffe prägen 2025 das globale Cyber-Risikoumfeld. Diese Entwicklungen betreffen auch die Schweiz. Neue Meldepflichten sollen den Schutz von Unternehmen und Behörden proaktiv stärken. Doch in welchen Bereichen ist eine vertiefte Prüfung nötig? Kessler teilt Erfahrungswerte, um die Relevanz für die Unternehmenssicherheit zu verdeutlichen. Die Integration in das Risk Management ist zentral, um die Resilienz gezielt und nachhaltig zu erhöhen.

Rechtliche Veränderungen

MELDEPFLICHT FÜR BETREIBER KRITISCHER INFRASTRUKTUREN

Seit dem 1. April 2025 gilt in der Schweiz eine Meldepflicht für Cyber-Vorfälle bei Betreibern von kritischen Infrastrukturen. Betroffen sind unter anderem die Sektoren Energie, Transport, Gesundheitswesen, Finanzwirtschaft und öffentliche Verwaltungen. Cyber-Angriffe müssen innerhalb von 24 Stunden an das Bundesamt für Cybersicherheit (BACS) gemeldet werden, sobald die Funktionsfähigkeit der kritischen Infrastruktur eingeschränkt ist, Daten abfliessen oder Vorfälle mit Erpressung oder Nötigung einhergehen. Bleibt die Meldung aus, drohen meldepflichtigen Behörden und Organisationen seit dem 1. Oktober 2025 Bussen bis CHF 100'000. Grundlage ist die Änderung des Informationssicherheitsgesetzes (ISG), das die Resilienz kritischer Infrastrukturen erhöhen soll.

KÜNSTLICHE INTELLIGENZ

AI Agents beschleunigen Prozesse und optimieren Entscheidungen, bergen jedoch erhebliche Cyber-Risiken. Manipulierte Trainingsdaten, unklare Verantwortlichkeiten und unkontrollierte Aktionen erhöhen das Missbrauchspotenzial. Der 2024 beschlossene EU AI Act schafft klare Regeln: AI Agents in sensiblen Bereichen wie Bonitätsprüfung oder Personalwesen gelten als Hochrisikosysteme mit strengen Vorgaben zu Transparenz, Kontrolle und Risikomanagement. Für Anbieter generativer Basismodelle gelten zusätzliche Anforderungen an Robustheit und Dokumentation, auch für Schweizer Firmen mit EU-Bezug.

Kleine Anbieter sehen Innovationshürden, multinationale Firmen warnen vor regulatorischer Komplexität und hohen Kosten. Sie fordern präzisere Leitlinien und längere Übergangsfristen. Parallel entstehen freiwillige Verhaltenskodizes und Standards (z. B. CEN, ETSI). Auch die Schweiz plant bis 2026 einen eigenen Rechtsrahmen, angelehnt an denjenigen in der EU. Im Fokus stehen AI Agents, die autonom handeln oder mit Kunden interagieren. Wer sie produktiv nutzen will, braucht technisches Know-how und regulatorische Weitsicht: Risikomanagement, transparente Prozesse und interne Kontrollen werden Pflicht – und bieten gleichzeitig einen Wettbewerbsvorteil.

Aktuelle Risiken

CYBER-SICHERHEIT BEI M&A-TRANSAKTIONEN

Cyber-Sicherheit erhält bei M&A-Aktivitäten oft zu wenig Beachtung. Laut IBM prüfen über die Hälfte der Unternehmen Cyber-Risiken erst nach Abschluss der Due Diligence. Risiken müssen jedoch frühzeitig und gezielt durch eine Analyse der Infrastruktur des Targets sowie durch die fortlaufende Beurteilung der geschäftlichen Auswirkungen im Transaktionszyklus identifiziert und quantifiziert werden. Nur so lassen sich Renditen sichern und Werte nachhaltig schützen.

Gemeinsam mit Marsh identifiziert Kessler weltweit die Angriffsfläche des Targets und bewertet die finanziellen Folgen von Ausfällen, Datenschutzverletzungen und Ransomware-Angriffen. Die Resultate fliessen in einen strukturierten Bericht mit priorisierten Handlungsempfehlungen zu Massnahmen mit signifikantem Einfluss auf den Transaktionswert.

KRISENMANAGEMENT – SICHERHEIT IN SCHWIERIGEN ZEITEN

Cyber-Versicherungen bieten weit mehr als finanziellen Schutz: Sie stellen ein wirksames Krisenmanagement sicher, um schnell und effektiv auf Sicherheitsvorfälle zu reagieren. Dazu gehören Incident-Response-Verfahren zur Erkennung, Analyse und Eindämmung von Cyber-Angriffen, gesetzeskonforme Meldungen und ein Business Continuity Plan (BCP) zur Sicherung kritischer Prozesse. IT-Forensiker, PR-Berater und Anwälte arbeiten rund um die Uhr an Analyse, Eindämmung und Wiederherstellung. Kessler begleitet von der Schadenmeldung über die Koordination mit Dienstleistern bis hin zum Nachweis gegenüber Versicherern.

CYBER-RISIKEN BEI SPIN-OFFS

Bei der Abspaltung einer Gesellschaft (Spin-off) stellt der Verkäufer oft übergangsweise während 6 bis 36 Monaten die IT-Infrastruktur bereit und regelt dies durch ein Transition Service Agreement (TSA). Klassische Cyber-Versicherungen decken diese Phase nicht ab: Kommt es zu Ausfällen oder Angriffen, drohen erhebliche Haftungsansprüche. Abhilfe schafft eine Berufshaftpflichtversicherung (Professional Indemnity, PI), die Fehler oder Versäumnisse in der Leistungserbringung absichert und so die Deckungslücke der IT-Übergangsszenarien schliesst.

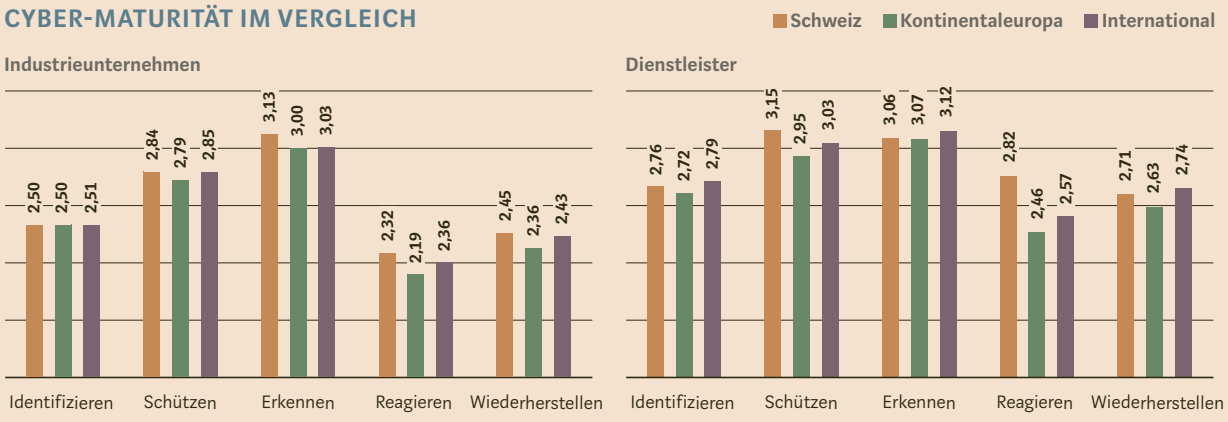
CYBER-MATURITÄT IM VERGLEICH: WO STEHEN SCHWEIZER UNTERNEHMEN?

Seit Anfang 2024 nutzt Kessler das Cyber Self-Assessment Tool (CSA) von Marsh, kombiniert mit dem NIST Cybersecurity Framework, um die Cyber-Resilienz der Kunden einzuordnen (Level 1 = teilweise umgesetzt bis Level 4 = adaptiv). Industrieunternehmen in der Schweiz erreichen durchschnittlich 2,71, Dienstleister wie IT-, Finanz- und Beratungsfirmen 2,91 – beide liegen damit über dem EU- und dem internationalen Mittel. Der Vorsprung der Dienstleister zeigt sich besonders in den Bereichen «Schützen» (+0,20) und «Reagieren» (+0,36). Eine schnelle Reaktion auf Vorfälle hat sich dabei als entscheidend für die Schadensbegrenzung erwiesen.

SUPPLY CHAIN – ERKENNTNISSE

IT-Dienstleister sind für die meisten Unternehmen zentral, gleichzeitig aber ein bevorzugtes Angriffsziel. Rund ein Drittel aller Cyber-Zwischenfälle geht auf sie zurück, vor allem durch fehlerhafte Konfigurationen, ungeschützte Konten oder verzögerte Sicherheitsupdates. Jedes Unternehmen sollte deshalb die IT-Dienstleister systematisch ins Risikomanagement einbinden, regelmässig überprüfen und sicherstellen, dass Cyber-Versicherungen auch Outsourcing-Vorfälle abdecken. Verantwortung lässt sich nicht auslagern, Risiken schon.

CYBER-MATURITÄT IM VERGLEICH



Cyber-Versicherungsmarkt

LÖSEGELDVERHANDLUNGEN

Erpressung ist ein zentrales Element des Geschäftsmodells «Ransomware-as-a-service» und zielt auf die Freigabe verschlüsselter Daten oder die Verhinderung ihrer Veröffentlichung. Unternehmen zahlen oft mangels Alternativen. Cyber-Versicherungen decken Lösegeld teilweise als Ultima Ratio. Verhandlungen laufen idealerweise über spezialisierte Krisenberater, welche die Kommunikation und die Verhandlungen steuern, die Glaubwürdigkeit der Forderungen prüfen und versuchen, die Lösegeldsumme zu reduzieren. Ziel ist die Wiederherstellung der Daten, die Zusicherung, dass kein erneuter Angriff erfolgt, sowie eine Offenlegung der Angriffsmethode. Zusätzlich sprechen sie Empfehlungen aus, um künftige Angriffe zu verhindern.

CYBER-ANGRIFFE 2024: MEHR MELDUNGEN, WENIGER SCHÄDEN

Gemäss Marsh Claims Report stiegen 2024 die Schadenmeldungen bei Cyber-Versicherungskunden in Europa um 61 Prozent. Gleichzeitig begrenzen wachsende Resilienz und schnellere Reaktion auf Bedrohungen die Auswirkungen. Treiber waren unter anderem digitale Lieferkettenstörungen wie der globale CrowdStrike-Ausfall. Der Anteil an Ransomware-Fällen sank von Spitzenwerten von über 40 Prozent im Jahr 2021 auf 18 Prozent im Jahr 2024, während KI-gestützte Phishing-Angriffe zunahmen. Auffällig bleibt: Die Multi-Faktor-Authentifizierung (MFA) ist weiterhin die am häufigsten kompromittierte Sicherheitskontrolle.

ÜBER KESSLER

Kessler ist das führende Schweizer Unternehmen für ganzheitliche Risiko-, Versicherungs- und Vorsorgeberatung. Wir betreuen über 1'500 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 370 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 Spezialisten aus allen Gebieten des Risk Management und mit grosser Erfahrung in der Betreuung globaler Versicherungsprogramme. Marsh ist in über 130 Ländern vertreten und der weltweit führende Versicherungsbroker und Risikoberater und Teil von Marsh McLennan (NYSE: MMC).

Weitere Informationen finden Sie unter:
www.kessler.ch, www.marsh.com, www.mmc.com.

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

Marsh Network