KESSLER

Cyber Message 2024

Risk and Insurance

MIT SICHERHEIT VORAUS.

Im Jahr 2024 stehen Unternehmen vor einer immer komplexeren Cyber-Bedrohungslandschaft. Neben den bereits bekannten Angriffsformen wird deutlich, welche Abhängigkeiten vor allem von externen Dienstleistern bestehen. Wie sich der allgemeine Cyber-Markt in diesem Jahr entwickelt hat, welche Rolle der Mensch im Unternehmen spielt und wie wir den Prozess der Risikobewertung optimieren, erfahren Sie in der zweiten Ausgabe der Kessler Cyber Message.

Rechtliche Veränderungen

revDSG

Die rasant fortschreitende Technologie erfordert kontinuierliche Anpassungen der Gesetzgebung. Seit dem 1. September 2023 ist das revidierte Datenschutzgesetz (revDSG) in Kraft, das die schweizerischen Datenschutzbestimmungen enger an die europäische Datenschutz-Grundverordnung (DSGVO) anlehnt. Diese Reform soll den Schutz personenbezogener Daten verbessern.

Wesentliche Neuerungen sind die erweiterten Auskunfts-, Melde- und Informationspflichten. Unternehmen müssen Betroffene umfassend über die Erhebung und Verarbeitung ihrer Daten informieren und Datenschutzverletzungen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden. Bisher sind über 200 Meldungen beim EDÖB eingegangen – aus verschiedenen Branchen. Das revDSG bringt grössere Verantwortung, Anpassungsbedarf bei den Unternehmen sowie höhere Compliance-Kosten und mögliche Änderungen der Geschäftspraktiken.

Am 14. August 2024 wurde ein neuer Datenschutzrahmen bestimmt, der einen sicheren Austausch von Personendaten zwischen der Schweiz und zertifizierten US-Unternehmen ermöglichen soll – ohne zusätzliche Garantien. Das «Swiss – U.S. Data Privacy Framework» soll sicherstellen, dass die Datenschutzmassnahmen eingehalten werden. Die offizielle Liste https://www.dataprivacyframework.gov/list führt alle zertifizierten Unternehmen auf.

GESETZMÄSSIGKEIT VON RANSOMWARE PAYMENTS

Während der Schweizer Bundesrat und weitere Regierungen nach effektiven Wegen suchen, um das Ransomware-Problem zu bewältigen, bieten die gesetzlichen Rahmenbedingungen bereits relevante Regelungen. Auch ohne spezifisches Verbot bestehen für Lösegeld zahlende Organisationen erhebliche rechtliche Risiken. Eine Zahlung könnte gegen Art. 260ter Abs. 1 lit. b StGB verstossen, wenn sie an eine kriminelle Gruppierung erfolgt.

Daher ist es essenziell, einen Entscheid zur Lösegeldzahlung sorgfältig und fundiert zu treffen. In der Schweiz zeigt die Praxis bisher eine opferfreundliche Handhabung der gesetzlichen Bestimmungen. Unternehmen, die sich mit Lösegeldzahlungen zu helfen versuchten, wurden bislang nicht mit zusätzlichen behördlichen Strafen konfrontiert.

KÜNSTLICHE INTELLIGENZ

Die Bedrohungen, die aus KI-generierten Angriffsformen entstehen, sind nach wie vor sehr aktuell. Dass es weiteren Schutz durch Regulatorien bedarf, beweist das Inkrafttreten des EU AI Act am 1. August 2024. Dieser wurde zur Wahrung der ethischen Werte und Grundrechte als Verordnung von der EU entwickelt und soll ein sicheres Umfeld schaffen – sowohl für die User als auch für die Wirtschaft.

Aktuelle Risiken

FAKTOR MENSCH

Cyber-Kriminelle greifen häufig gezielt Mitarbeitende an, um über sie die Sicherheitsvorkehrungen von Unternehmen zu umgehen und in IT-Systeme einzudringen, was erhebliche Schäden verursachen kann. Das Verhalten der Mitarbeitenden hat direkten Einfluss auf die Cyber-Sicherheit und auch auf die Minderung der Folgen eines Angriffs. Schutz und Schadensbegrenzung sind zentrale Elemente der Cyber-Resilienz.

Die aktuelle Forschung besagt, dass die Einstellung der Mitarbeitenden gegenüber Cyber-Risiken entscheidend ist. Verstehen Mitarbeitende, dass sie täglich mit sensiblen Informationen arbeiten, stärkt dies ihre Sensibilisierung und erhöht die Sicherheit. Es ist wichtig, den Einfluss jedes Einzelnen auf die Cyber-Resilienz zu verdeutlichen. Konkrete Beispiele, branchenspezifische Bezüge sowie regelmässige Weiterbildungen fördern nachhaltige Awareness und führen zu einer sicherheitsorientierten Haltung.

BERUFSHAFTPFLICHTRISIKEN FÜR TECHNOLOGIEUNTERNEHMEN

Technologieunternehmen hängen stark von komplexen IT-Systemen ab, gleichzeitig nehmen technische Risiken stetig zu. Diese können je nach Unternehmensart und den angebotenen Dienstleistungen schwerwiegende Folgen haben. Pflichtverletzungen, Versäumnisse, Systemausfälle und Softwarefehler führen zu erheblichen Problemen und Haftungsansprüchen. Eine Berufshaftpflichtversicherung (PI) ist daher eine sinnvolle Massnahme, um sich gegen berufliche Risiken abzusichern.

Das Risiko für Cyber-Vorfälle steigt bei Technologieunternehmen, die vermehrt externen Angriffen ausgesetzt sind. Während die «PI Tech-Versicherung» Risiken abdeckt, die durch Fehler oder Versäumnisse bei der Erbringung von Dienstleistungen oder durch technische Produkte entstehen, schützt die «Cyber-Versicherung» vor externen Bedrohungen wie Hackerangriffen, Datenlecks oder Betriebsunterbrechungen. Die Kombination beider Versicherungen bietet Technologieunternehmen umfassenden Schutz.

Cyber-Versicherungsmarkt

MARKET UPDATE

Der Cyber-Versicherungsmarkt zeigt sich seit Ende 2023 dynamisch und wettbewerbsintensiv. Er wird zunehmend durch neue Anbieter belebt. Der Trend zu flexibleren Zeichnungsrichtlinien, höheren Versicherungssummen und oft auch Prämiensenkungen bei gleichbleibendem Deckungsumfang setzt sich fort. Gleichzeitig bleiben strenge Mindestanforderungen an die IT-Maturität der Versicherten, wie die «12 Key Controls», eine Konstante. Diese Anforderungen sind für den Abschluss einer Cyber-Versicherung entscheidend. Die Marktentwicklung zeigt, dass die Schweizer Versicherer zunehmend risikobereiter werden, wobei sie eine Balance zwischen Vorsicht und Innovationsfreude anstreben.

ALLGEMEINE ENTWICKLUNG IM SCHADENUMFELD

Ransomware-Angriffe bleiben nach wie vor das grösste Risiko und verursachen die höchsten finanziellen Schäden. Oftmals werden die vielfältigen Positionen des Eigenschadens unterschätzt. Die Kosten für das Krisenmanagement, die Wiederherstellung der Systeme sowie die Auswirkungen eines Betriebsunterbruchs können schnell stark ansteigen.

Lösegeldforderungen bleiben ein ernstes Problem. Bei einer Erpressung empfiehlt sich die Aufnahme von Verhandlungen, um Informationen zu sammeln und Zeit zu gewinnen. Statistiken von Kessler zeigen, dass dadurch Lösegeldforderungen im Median um 59 Prozent gesenkt werden können.

DER CYBERBEDINGTE BETRIEBSUNTERBRUCH

Die Berechnung von Umsatzausfällen nach Cyber-Vorfällen ist herausfordernd, da sie von saisonalen und konjunkturellen Schwankungen beeinflusst werden. Dazu müssen die Umsätze mit den Budgetzahlen und dem Vorjahr verglichen werden. Lösungsansätze wie eine Business Impact Analysis sind zeit- und kostenintensiv. Auch die Dokumentation von Mehrkosten ist problematisch. Kessler empfiehlt, Überstunden und zusätzliche Massnahmen zu dokumentieren, um die Nachweisbarkeit und Krisenbewältigung zu verbessern. Neben den Arbeitsstunden sollten die in dieser Zeit ausgeführten Tätigkeiten erfasst werden, um später nachvollziehen zu können, was geleistet wurde.

CROWDSTRIKE-VORFALL

Der CrowdStrike-Vorfall im Juli 2024 hat verdeutlicht, wie kritisch ein fehlerhaftes Update eines Drittanbieters sein kann. Ein Fehler im Falcon-Content-Update löste weltweite Ausfälle für Windows User aus. So etwas kann die Integrität der gesamten Lieferkette gefährden. Die Prüfung der Lieferanten sollte daher nicht nur einmalig, sondern als kontinuierlicher Prozess umgesetzt werden. In Verträgen mit Drittanbietern braucht es klare Sicherheitsstandards sowie regelmässige Audits. Diese Massnahmen helfen, die Datenintegrität zu schützen und Auswirkungen solcher Vorfälle zu minimieren.

CYBER SELF-ASSESSMENT TOOL (CSA)

Seit Anfang 2024 bietet Kessler seinen Kunden das Cyber Self-Assessment Tool (CSA) des Netzwerkpartners Marsh an. Der webbasierte Fragebogen erleichtert die Erfassung von Risikoinformationen, wobei der Umfang der Fragen auf Unternehmensgrösse und Tätigkeit abgestimmt ist. Die Wiederverwendbarkeit der Daten für Folgejahre und die breite Akzeptanz bei Versicherern vereinfachen den Ausschreibungs- und Erneuerungsprozess erheblich.

Das CSA bietet jedoch noch mehr: Es liefert Reports, die die Einschätzung der Versicherer zur IT-Maturität des Unternehmens aufzeigen, zeigt, wie die Controls im Vergleich zu internationalen Frameworks einzuordnen sind und wie das Unternehmen im Peer-Vergleich aufgestellt ist. Zusätzlich modelliert das Analysetool Blue[i] mögliche Schadensszenarien, einschliesslich Eintrittswahrscheinlichkeiten und erwarteten Schadensausmasses. Diese Einblicke unterstützen die Risikotransfer-Evaluation und verfeinern die Ausschreibungsstrategie. Sie zeigen auch auf, mit welchen Massnahmen die Cyber-Sicherheit gezielt verbessert werden kann.

CYBER BLUE LINE

Nach der Einführung der Cyber blue line 2023 ziehen wir durchweg positive Bilanz. Die Cyber blue line vereinfacht den Cyber-Submissionsprozess erheblich. Sind die 12 Mindestanforderungen erfüllt, beschliessen über 98 Prozent unserer Kunden, zur Cyber blue line zu wechseln. Zusätzlich profitieren unsere Kunden über den Rahmenvertrag von Services wie Phishing-Simulationen oder Mitarbeiterschulungen.

THREEMA

Um auch in einer Krise die sichere Kommunikation zu gewährleisten, setzen wir auf die Zusammenarbeit mit Threema. Das Marktforschungsunternehmen Forrester anerkannte 2024 Threema als führendes Unternehmen für sichere Kommunikation. Häufig wird in den Unternehmen nicht verifiziert, auf welche Art ein Austausch im Krisenfall stattfinden soll – unsere Kunden sind dankbar für den Hinweis auf diesen Fakt und nutzen den sicheren Kommunikationskanal über Threema.

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 350 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