KESSLER

Cyber Message 2023

Risk and Insurance

MIT SICHERHEIT VORAUS.

Unternehmen sind stärker denn je durch Cyber-Angriffe bedroht. Für die meisten gehören Cyber-Vorfälle zu den Top 3 der Geschäftsrisiken. Die Zunahme der Schadenfälle bei Unternehmen führt dazu, dass die Versicherer nachgelagert gleichermassen betroffen sind. Unsere Erfahrungen aus Schadenfällen und die «Lessons Learned» geben wir Ihnen in dieser Cyber Message weiter.

Rechtliche Veränderungen

NEUES DATENSCHUTZGESETZ

Am 1. September 2023 trat das neue Datenschutzgesetz (revDSG) in Kraft. Doch warum war es notwendig, das bestehende Gesetz anzupassen? Die Originalfassung stammt aus dem Jahr 1992. In 31 Jahren hat sich einiges verändert; wir sind im digitalen Zeitalter angekommen. Deshalb ist es zum Schutz der Privatinteressen jedes Einzelnen unerlässlich, auch den Datenschutz auf den neuesten Stand zu bringen. Die Korrelation von Informations- und Datensicherheit zeigt sich bei den bekannten Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.

Was gehört zu den hervorzuhebenden Anpassungen?

- Die Daten von natürlichen Personen sind betroffen, jedoch nicht mehr diejenigen von juristischen Personen.
- Dokumentationspflichten
- Stärkung der Rechte der betroffenen Personen
- Einführung der Grundsätze «Privacy by Design» und «Privacy by Default»
- Strafrechtliche Haftung der verantwortlichen Person

Eine Übergangsfrist gab es hierfür nicht. Was empfehlen wir unseren Kunden? Dies ist klar und einfach: Alle Aufgaben müssen eindeutig verteilt sein und die Verantwortlichen entsprechend sensibilisiert werden.

MELDEPFLICHT KRITISCHE INFRASTRUKTUR

Eine weitere regulatorische Anpassung wird in Form der Revision des Informationssicherheitsgesetzes (ISG) stattfinden, welche insbesondere für Behörden und Organisationen des Bundes neue Standards definiert. Diese sollen zukünftig die Informations- und Cyber-Sicherheit verbessern. Alle betroffenen Behörden und Unternehmen müssen beispielsweise ein Managementsystem für Informationssicherheit (ISMS) erstellen und über ein adäquates Risikomanagement verfügen.

Darüber hinaus gilt für Unternehmen im Bereich der kritischen Infrastruktur eine Meldepflicht an das National Cyber Security Centre NCSC für Cyber-Angriffe mit schwerwiegenden Auswirkungen innerhalb von 24 Stunden nach deren Entdeckung. Sollte dieser Meldepflicht nicht nachgekommen werden, kann dies mit einer Busse von bis zu CHF 100'000 bestraft werden.

Als kritische Infrastrukturen gelten u. a. Hochschulen, Behörden, Organisationen der Sicherheit und Rettung, Trink- und Abwasserversorgung, Abfallentsorgung, Energieversorgung, Banken, Versicherungen, Gesundheitseinrichtungen, Sozialversicherungen, Schweizerische Radio- und Fernsehgesellschaft etc. Das Inkrafttreten der neuen Gesetzgebung wird in Kürze erwartet.

Aktuelle Risiken

ENTWICKLUNG RANSOMWARE

Ransomware bleibt eines der Hauptrisiken für die meisten Kunden. Zudem werden gerade kleine bis mittelständische Unternehmen für Cyber-Kriminelle attraktiver. Diese haben meist nicht vergleichbar viele Ressourcen in ihre IT-Sicherheit investiert wie zum Beispiel Grossunternehmen. Generell lässt sich ein Trend feststellen, dass Ransomware-Angriffe weniger auf bestimmte Industriezweige abzielen. Seit Mitte 2022 sind die Ransomware-Attacken wieder deutlich häufiger geworden.

Interessant zu beobachten ist, dass sich die Vorgehensweise der Angreifer in einigen Fällen geändert hat. Gerade weil die Unternehmen vermehrt in «Detection and Response» investiert haben, steht bei diversen Hackergruppierung die Exfiltration von Daten inklusive der Androhung von deren Veröffentlichung im Vordergrund

und nicht mehr deren Verschlüsselung. Einige Gruppierungen treten bei einem erfolgreichen Angriff mit den betroffenen Unternehmen in Kontakt und versuchen, an die Deckungsinformationen von deren Cyber-Versicherungspolice zu gelangen.

In einem solchen Fall wird dringend von einer Kooperation mit den Angreifern ohne vorherige Zustimmung des Versicherers abgeraten. Eine solche Kooperation stellt eine Obliegenheitsverletzung im Sinn der Police dar und kann Leistungskürzungen im Schadenfall zur Folge haben.

ANGRIFFE DURCH KÜNSTLICHE INTELLIGENZ (KI)

Mit der rasanten Entwicklung von KI haben sich auch die digitalen Betrugsmöglichkeiten enorm erweitert. Im Besonderen sieht man dies in den neuesten Methoden zur Verwendung von Phishing E-Mails und sogenannte «Social Engineering Fraud» (SEF). Inzwischen bietet «Deep Fake» Möglichkeiten, Audio- und Bildaufnahmen derart zu manipulieren, dass Opfer auf virtuellen Meeting-Plattformen dazu überredet werden, Geld zu überweisen oder Informationen bekannt zu geben. Häufig geben sich Betrüger als leitende Angestellte aus, welche die Mitarbeitenden zu solchen Tätigkeiten veranlassen.

Ähnlich bietet die Plattform WormGPT die Möglichkeit, eine hohe Anzahl an raffinierten Phishing E-Mails zu erstellen, welche in Business Email Compromise (BEC) und Phishing-Angriffen resultieren. Wichtig ist zu erwähnen, dass für einen klassischen «Social Engineering Fraud» (SEF), wo es zu keiner Manipulation des Computersystems des Versicherten kommt, üblicherweise die Vertrauensschaden- und nicht die Cyber-Versicherung zur Anwendung kommt.

Versicherer im Cyber-Markt

12 KEY CONTROLS

Die Mindestanforderungen für den Abschluss einer Cyber-Versicherung lassen sich in «12 Key Controls» unterteilen. Deren Einhaltung hat gemäss einer Studie unseres Netzwerkpartners Marsh einen massgeblichen Einfluss auf die Schadenprävention. Allerdings ist die Effektivität der einzelnen Key Controls sehr unterschiedlich.

Die Gegenüberstellung der Mindestanforderungen mit der Schadendatenbank hat gezeigt, dass vor allem Härtungsmassnahmen die Wahrscheinlichkeit eines erfolgreichen Cyber-Angriffs reduzieren. Härtungsmassnahmen sind jene Sicherheitsvorkehrungen und -konfigurationen, die ergriffen werden, um Systeme, Netzwerke oder Software widerstandsfähiger gegen potenzielle Bedrohungen und Angriffe zu machen.

Bemerkenswert ist, dass der bisherige Fokus der meisten Versicherer jedoch auf den Key Controls «Multi-Faktor-Authentifizierung (MFA)», «Endpoint Detection and Response (EDR)» und «Privileged Access Management (PAM)» lag. Die Studie hat auch gezeigt, dass MFA nur dann eine starke Wirkung hat, wenn sie vollständig umgesetzt wird.

OBLIEGENHEITSVERLETZUNGEN

Für den Versicherungsnehmer bestehen zahlreiche Obliegenheiten in den Allgemeinen Geschäftsbedingungen (AVB) – so auch in zunehmendem Mass für die Sparte Cyber. Angemessene technische Schutzmassnahmen und Verfahren werden vorgeschrieben und reichen bis hin zu Verpflichtungen der Versicherungsnehmer, die fachliche Prüfung der Eignung ihrer Computersysteme und ihrer IT-Prozesse sicherzustellen. Hierbei sollen die Integrität, Verfügbarkeit und Vertraulichkeit der sich darauf befindenden Daten gewährleistet werden.

Bei schuldhafter Verletzung der Obliegenheiten durch den Versicherungsnehmer droht eine Kürzung der Entschädigungsleistung durch den Versicherer. Der Versicherer trägt die Beweislast für das Vorliegen einer Obliegenheitsverletzung. Ein Nachteil tritt für den Versicherungsnehmer nicht ein, wenn die Obliegenheitsverletzung den Umständen nach als unverschuldet anzusehen ist oder die Obliegenheitsverletzung keinen Einfluss auf den Eintritt des befürchteten Ereignisses und auf den Umfang der vom Versicherungsunternehmen geschuldeten Leistungen gehabt hat (seit VVG-Revision). Diese Neufassung stellt eine Verbesserung der Rechtsstellung des Versicherungsnehmers dar.

Cyber-Versicherungsmarkt

MARKET-UPDATE

Der Cyber-Versicherungsmarkt steuert 2023 weiterhin auf eine Stabilisierung zu. Die Versicherer können die Kapazitäten und Deckungen in aller Regel aufrechterhalten. Die Prämien stiegen durchschnittlich im einstelligen Prozentbereich, was gegenüber den Vorjahren eine massive Verbesserung darstellt.

Bei besonders exponierten Kunden, wie beispielsweise Spitälern oder Dienstleistern im Bereich der kritischen Infrastruktur, waren teilweise grössere Anpassungen nötig. Der Abschluss einer Cyber-Versicherung soll als Qualitätsmerkmal für einen hohen IT-Security-Reifegrad verstanden werden. Daher werden die «12 Key Controls» konsequent eingefordert. Dies zeigt Wirkung: Während seit Mitte 2022 weltweit ein deutlicher Anstieg an «Cyber Incidents», allen voran Ransomware-Angriffe, verzeichnet wird, sank während derselben Periode die Anzahl der von Kessler und Marsh rapportierten Cyber-Fälle.

KESSLER BLUE LINE FACILITY

Um den Prozess rund um die Submission einer Cyber-Versicherung effizienter zu gestalten, haben wir nach einer Lösung gesucht – und sie gefunden. Mit unserer Kessler blue line Facility schlagen kleine und mittelgrosse Unternehmungen eine neue Richtung ein. Sofern Sie sich qualifizieren, können wir auf den jährlichen Erneuerungsprozess verzichten und Sie profitieren von einem exklusiv verhandelten Vertragswerk zu attraktiver Prämie.

CYBER-ATTACKE? SICHERE KOMMUNIKATION MIT THREEMA

In der aktuellen sowie auch zukünftigen Cyber-Welt ist die Kommunikation im Krisenfall essenziell. Viele Unternehmen – ob Grossunternehmen oder KMUs – haben für den effektiven Krisenfall keine sichere Plattform, um sich auszutauschen und die relevanten Personen, den sogenannten Krisenstab, sicher und schnell zu erreichen.

Wir haben daher eine Lösung für einen zukünftigen Krisenfall erarbeitet: dank der Zusammenarbeit mit Threema. Per 1. Januar 2024 offerieren wir dem Krisenstab unserer Kunden die Kommunikations-App Threema Work kostenfrei zur Cyber-Versicherung. Damit können wir unseren Kunden eine sichere Plattform anbieten, um auch im Krisenfall korrekt kommunizieren zu können.

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 330 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