Liberty Specialty Markets

Cyber-Risiken

Cybercrime – eine wachsende Industrie

Cybercrime-Methoden sind vielfältig: Von Spionage und Sabotage über Erpressung und Datenabfluss bis zu Marktmanipulation oder Phishing. Auch haben die Fälle zugenommen, die ihren Ausgangspunkt innerhalb des Unternehmens haben, also Insidertaten oder unbeabsichtigtes Verhalten von Mitarbeitenden. Darüberhinaus werden vermehrt ganze IT-Geschäftsprozesse ausgelagert – damit verändern sich auch die Risiken, denen diese Unternehmen ausgesetzt sind.

Liberty schützt die immateriellen Vermögensgegenstände seiner Kunden mit einem innovativen, kreativen Ansatz und bietet schnelle und flexible Versicherungslösungen. Unsere Cyber Suite berücksichtigt alle Herausforderungen, mit denen Unternehmen angesichts der wachsenden Abhängigkeit von IT-Netzwerken, IT-Strukturen von Drittanbietern, digitalen Ressourcen oder auch personenbezogenen Speicherdaten konfrontiert sind.

Jedes Unternehmen ist Cyber-Risiken ausgesetzt

Wer Daten über Dritte oder über Mitarbeitende gespeichert hat, muss sich überlegen, wie sicher diese sind. Je umfangreicher und vertraulicher die Daten, desto kostspieliger ist eine eventuelle Haftung gegenüber Dritten oder Mitarbeitenden.

Je nach Gesetzgebung und aufsichtsbehördlichen Bestimmungen können Schadenersatzansprüche, Bussen (von Gesetzes wegen nicht immer versicherbar), Kosten für die Kundenbenachrichtigung oder das Kredit-Monitoring ein beachtliches Ausmass annehmen. In immer mehr Ländern besteht eine gesetzliche Informationspflicht gegenüber Personen, deren Datenschutzrechte verletzt wurden. Sollten vertrauliche Daten von EU-Bürgern betroffen sein, kommen auch für Schweizer Unternehmen die Datenschutzgrundverordnung DSGVO der EU zur Anwendung. Und wo keine entsprechenden Gesetze existieren, ist diese Informationspflicht oft Bestandteil von Vertragsbestimmungen oder Branchenrichtlinien.

Das Risiko eines Netzwerkausfalls, der einen Betriebsunterbruch verursacht und schliesslich zu entgangenen Einnahmen führt, besteht ebenfalls in jedem Unternehmen: Können beispielsweise Mitarbeitende nicht auf Verkaufs- oder Marketinglisten, CRM oder Beschaffungssysteme für die Lieferkette zugreifen, kommt die Arbeit schnell zum Stillstand. Auch Gebäude, Fabriken und Lager werden oft über Netzwerke gesteuert. Ihr Ausfall kann den Herstellungsprozess ebenfalls empfindlich stören.

Kapazitäten	Umfang
Cyber-Risiken	bis zu CHF/EUR/USD 10 Mio.

Szenarien von Cyberkriminalität

Erst standen Finanzinstitute im Fokus betrügerischer Handlungen. Nun sind auch Anwaltskanzleien, Beratungsunternehmen und insbesondere KMU aus den unterschiedlichsten Tätigkeitsbereichen Ziel professioneller Angriffe. Drei Beispiele:

Erpressung mit Folgeschäden

Eine mittelständische Schweizer Handelsfirma erfährt einen Hacker-Angriff aus dem Nichts. Erst unterschätzt, trifft es das Unternehmen mit voller Wucht: Kein Zugang mehr zum Intranet, zahlreiche Applikationen sind zerstört, Datenbanken gelöscht, Server nicht sichtbar oder auf Werkseinstellungen zurückgesetzt – das IT-System ist am Boden. Schnittstellen, über die Grosskunden ihre Bestellungen automatisch eingeben, sind gelöscht, das Arbeiten wird komplett verunmöglicht und das Unternehmen muss notfallmässig offline gehen.

Aufgrund dieser Situation drohen Kundenabgänge und Konventionalstrafen. Dann treffen Lösegeldforderungen über mehrere Hunderttausend Franken ein. Erst nach mehr als dreiwöchiger, aufwendigster Abwehr- und noch länger andauernder Rekonstruktionsarbeiten kann das Unternehmen wieder schrittweise zum Normalbetrieb zurückkehren.

Schwachstelle Mensch

Die gesamte IT-Infrastruktur eines Schweizer Gebäudetechnik-Unternehmens wurde lahmgelegt: Mitarbeitende ermöglichten den Zugang via einem Phishing-E-Mail. Betroffen waren das zentrale ERP- und das Lagerleitsystem, die Website, sämtliche E-Mail-Adressen und die Festnetz-Telefonie.

Die Lager- und Lieferlogistik war besonders stark betroffen, Auslieferungen erfolgten keine mehr. Forensische IT-Spezialisten wurden beauftragt, Ermittlungen aufzunehmen. Betroffen waren sämtliche Schweizer Standorte des Unternehmens mit über 1000 Angestellten.

Gezielte Attacken

Bei einem Provider, der gegen 50 Mitarbeitende beschäftigt, beginnt der Tag hektisch: Ein Cyber-Angriff hatte einen Cloud-Service zum Erliegen gebracht. Zwar konnten die Ransomware-Attacke mehrheitlich abgewehrt, die Applikationsserver und Daten nach und nach wieder hergestellt werden. Doch musste das Unternehmen zahlreiche Kunden noch Wochen später um Geduld bitten, da betroffene Systeme nur nach und nach wieder in Betrieb genommen, die zum Teil sehr grossen Datenmengen nur zeitaufwändig wieder hergestellt werden konnten.

Was diesen Fall bemerkenswert macht, ist die gezielte Cyber-Erpressung: Zu Ransomware mittels Massenangriffen kommen immer mehr gezielte Erpressungen von einzelnen Unternehmen hinzu. Merkmal dieser Angriffe: Es können viel höhere Summen verlangt werden, denn die Angegriffenen sind bekannt, es kann in etwa abgeschätzt werden, was diese zu zahlen bereit sind.

Was umfassen denn nun genau Cyber-Risiken?

Der Begriff beschreibt eine Reihe von Risiken für Eigen- und Drittschäden im Zusammenhang mit der Nutzung von Informationstechnologien. Die Cyber Suite von Liberty bietet folgende Deckungsarten:

Eigenschäden

- **Verlust oder Beschädigung von Daten oder Programmen**
  Kosten für Instandsetzung, Aktualisierung, Wiederherstellung oder Ersatz beschädigter Daten und/oder Programme, um den Zustand vor dem Schadenfall wiederherzustellen.
- **Bei Betriebsunterbruch**
  Einnahmenverlust durch Unterbruch, Beeinträchtigung oder Ausfall Ihres Netzwerks, auch unterbrechungsbedingte Aufwendungen für Minderung und Untersuchung des Schadens.
- **Cyber-Erpressung**
  Bei Erpressung unter der Androhung, Ihr Netzwerk lahmzulegen oder zu beeinträchtigen, unberechtigt Daten aus Ihrem Netzwerk zu veröffentlichen oder unter Vorspiegelung falscher Tatsachen mit Ihren Kunden zu kommunizieren, behandeln wir die Forderungen und bezahlen das Lösegeld.
- **Reputationsverlust**
  Bei Nachricht einer Datenschutzverletzung erleiden Sie einen Reputationsverlust, Ihnen entgehen durch Kundenverluste Einnahmen: Wir erstatten die entgangenen Einnahmen sowie die erhöhten Arbeitskosten und Aufwendungen für Öffentlichkeitsarbeit.

Drittschäden

- **Cyber-Haftpflicht**
  Aufwendungen für Haftung und rechtliche Verteidigung, die aus Ansprüchen einer realen oder behaupteten unrechtmässigen Handlung entstehen können.
- **Aufsichtsbehördliches Verfahren**
  Kosten für Untersuchung, Verteidigung und – soweit gemäss anwendbaren Recht versicherbar – auch Geldbussen und Geldstrafen.
- **Benachrichtigungskosten und Krisenmanagement**
  Rechtskosten sowie Kosten für Unterstützung von Personen, die von Datenschutzverletzungen betroffen sind, beispielsweise durch das Monitoring von Kreditakten oder durch Beratung bei Identitätsdiebstahl, auch für Schutz oder Wiederherstellung der Reputation.
- **Multimedia-Haftpflicht**
  Untersuchungs- und Verteidigungskosten sowie Schadenersatzansprüche, wenn Sie Immaterialgüter- oder Datenschutzrechte Dritter verletzen, wenn Ihnen Verleumdung vorgeworfen wird oder wenn Sie fahrlässig Inhalte online oder offline veröffentlichen.

Gute Frage: Ist der Verlust von Daten nicht schon durch andere Versicherungen gedeckt?

Berufshaftpflicht

Wenn Sie über eine Berufshaftpflichtversicherung verfügen, deckt diese möglicherweise bereits Drittschäden aufgrund von Datenverlusten – in der Regel allerdings nur dann, wenn der Schaden durch die Ausübung der beruflichen Tätigkeit entsteht.

Eine Berufshaftpflicht deckt meist keine Forderungen von Angestellten, auch eine böswillige oder unautorisierte Nutzung des Netzwerks des Versicherten, die Kundendaten beschädigt, missbraucht oder zerstört oder die Denial-of-Service-Attacken auslöst.

Weiter sind Schäden durch die Übertragung von Computerviren oft ausgeschlossen und die Deckung beschränkt sich auf Forderungen von Kunden des Versicherten, wobei aufsichtsrechtliche Verfahren ausgeschlossen sind. Zudem bieten die meisten Berufshaftpflichtversicherungen bei Eigenschäden wie entgangenen Einnahmen, Verlust oder Beschädigung von Daten/Programmen, Cyber-Erpressung oder Reputationsverlust keine Deckung.

Allgemeine Haftpflicht

Eine allgemeine Haftpflichtversicherung deckt nur Personen- und Sachschäden. Da die Gerichte Daten als immaterielle Vermögensgegenstände betrachten, ist eine Verletzung von Datenschutzrechten üblicherweise nicht gedeckt.

Sachversicherung

Eine Sachversicherung deckt in der Regel nur Schäden an physischem Eigentum. Die Gerichte betrachten Daten als immaterielle Vermögensgegenstände. Deshalb werden Verluste oder Beschädigungen von Daten/Programmen meist nicht übernommen. Selbst wenn Sie über eine Betriebsunterbruch-Versicherung aufgrund von Sachschäden verfügen, besteht vermutlich keine Deckung bei einem Betriebsunterbruch als Folge immaterieller Schäden an Ihrem Netzwerk. Computerviren und Netzwerk-Risiken sind bei Sachversicherungen oft ausgeschlossen.

All-Risk-Computerversicherung

Die All-Risk-Computerversicherung deckt die Kosten für die Reparatur beschädigter Hardware (physisches Eigentum), anders als bei einer Cyber Suite-Versicherung jedoch keine Forderungen im Zusammenhang mit dem Verlust von Daten oder Folgekosten.

Unser Anspruch ist auch ein langfristiger

Die Zusammenarbeit mit unseren Kunden gestalten wir innovativ und entscheidungsfreudig. Wir sind schnell und wir sind am Puls der Zeit. Gleichzeitig stellen wir eine nachhaltige Entwicklung über alles: In der Beziehung zu unseren Kunden und erst recht hinsichtlich Ihrer Unternehmung.

Denn nur was gut ist für Sie, ist auch gut für uns. Also handeln wir immer auch langfristig: Mit unserer Fachkompetenz im Underwriting und Kenntnis der lokalen und internationalen Märkte, unseren starken Beziehungen zu den unterschiedlichen Geschäftspartnern oder mit unserer unkomplizierten Art der Schadenbehandlung. So schaffen wir Vertrauen und Verlässlichkeit in einer sich wandelnden Zeit. Auch auf lange Sicht.

Sie möchten mehr über Liberty in der Schweiz und über unsere Versicherungsprodukte erfahren?

Kontaktieren Sie uns:

Liberty Specialty Markets
Lintheschergasse 19, 8001 Zürich

+41 44 285 10 00
lsmzurich@libertyglobalgroup.com
www.libertyspecialtymarkets.com

Liberty Specialty Markets

For Mutual Advantage