Cyberversicherung

Cyberdeckung als Selbstverständlichkeit

Die Absicherung von Cyberrisiken spielt eine ganz zentrale Rolle beim Schutz der Firmendaten. Unzureichende Maßnahmen oder Verstöße können zu einer persönlich unbegrenzten Haftung des Geschäftsführers oder Vorstands führen.

»manage it« sprach mit Christian Hörtkorn, Geschäftsführer der Dr. Hörtkorn Unternehmensgruppe, über die Notwendigkeit einer umfassenden und dennoch individuellen Abdeckung der Cyberrisiken für Unternehmen und deren Organe.

Die Cyberversicherung ist ein relativ junges Geschäftsfeld. Das Bewusstsein für den Bedarf an einer Cyberschutzversicherung ist bei den Kunden und bei den Versicherungsunternehmen erst in den letzten Jahren deutlich gestiegen. Welche Risiken deckt die Cyberversicherung ab?

Die Cyberversicherung ist in der Tat ein noch relativ neues Produkt auf dem deutschen Versicherungsmarkt. Allerdings beschäftigen sich zwischenzeitlich so gut wie alle Versicherungsgesellschaften mit diesem Thema und bieten entsprechende Lösungen an. Ein wirklicher »Bedingungsstandard« hat sich, trotz der GDV-Musterbedingungen, noch nicht wirklich entwickelt.

Generell ist die Cyberversicherung ein Produkt, welches mehrere Versicherungselemente vereint. So werden neben der Komponente »Eigenschaden«, etwa Betriebsunterbrechungsschäden oder Wiederherstellungskosten der Systeme, ein Baustein Haftpflicht für Drittschäden auch die elementar wichtige Unterstützung im Schadenfall durch hoch spezialisierte Dienstleister wie Krisenhotline, Forensik, etc., zusammengefasst.

Cyberrisiken sind begrifflich nicht eindeutig definiert. Zwar ist für viele Unternehmen eine Versicherung gegen Hacker sehr bedeutsam wegen der zielgerichteten Angriffe auf IT-Systeme und Daten, doch ein Datenverlust entsteht auch durch nachlässiges Verhalten eigener Mitarbeiter und durch Strom- und Internetausfälle, zu seltene Backups und weitere Organisationsmängel. Welche sind die häufigsten Cyberrisiken?

Allein von der Anzahl her betrachtet, sind die häufigsten Cyberrisiken nach unserer Einschätzung klar Schäden durch Ransomware. Allerdings mit einer extrem breiten Auswirkung hinsichtlich der Schadenhöhe – diese reicht von »Kleinschäden« mit weniger als 10.000 Euro bis hin zu kompletten Produktionsstillständen mit Schadenpotenzial von mehreren Millionen Euro.

Es gibt Firmen, die eher selten Hackerangriffe, wohl aber Datenverlust durch Fehlbedienungen fürchten. Ein Beispiel wäre das nur im Stundentakt durchgeführte Backup, weil das Unternehmen nicht in der Cloud mit ihren sekündlichen Backups arbeiten will. Wenn vor dem Backup am Tagesende eine Festplatte ausfällt, ist der Schaden groß. Des Weiteren können extern gelagerte Datenträger durch Unfälle wie Brand, Wasser etc., unbrauchbar werden.

Sind in der Cyberversicherung von Dr. Hörtkorn die Datenschutzversicherung und die Internetschutzversicherung enthalten?

Bei der Datenversicherung gibt es zwei Modelle. Zum einen die »einfache« Datenversicherung, die einen Schutz gegen die Sachgefahren wie Feuer, Diebstahl, Explosion oder Wasser bietet. Das zweite Modell ist die »erweiterte« Datenversicherung. Hier werden die Sachgefahren erweitert um Schäden durch Viren oder Bedienfehler. Beide Lösungen können eine vollwertige Cyberversicherung nicht ersetzen. Unsere Versicherungslösung Cyber

» **Allein von der Anzahl her betrachtet,** sind die häufigsten Cyberrisiken nach unserer Einschätzung klar Schäden durch Ransomware. «

Fotos: © Anne-Kathrin Kabitzke

Protection Plus unterscheidet in puncto der Datenwiederherstellung nicht, ob diese durch einen Sachschaden oder durch einen Cybervorfall erforderlich wird.

Welche wirtschaftliche Bedeutung hat die Cyberdeckung?

Für unser Verständnis spielt die Absicherung von Cyberrisiken eine ganz zentrale Rolle. Die Erkenntnis, dass diese Bedrohungsszenarien leicht existenzbedrohende Folgen haben können, setzt sich mehr und mehr durch. Wir sind der Auffassung, dass spätestens in fünf Jahren die Cyberdeckung eine Selbstverständlichkeit im Versicherungsportfolio jeder Firma sein wird.

Welche Anwendungsbereiche der Cyberversicherung sind für das Kundenklientel besonders wichtig und müssen hervorgehoben werden?

Eine Cyberversicherung ist für nahezu alle Branchen relevant. Insbesondere für solche Unternehmen, die stark von der IT abhängig sind und/oder über zu schützende Datenbestände verfügen, seien es personenbezogene, sensible, vertrauliche Daten oder Daten, die der Geheimhaltung unterliegen.

Wie gestaltet sich die Regulierungspraxis in der Cyberversicherung?

Nahezu alle Anbieter von Cyberversicherungen haben eine Krisenhotline 24/7 hinterlegt. Bereits im Verdachtsfall ist diese Hotline vorrangig zu kontaktieren. Die Experten entscheiden dann, in der Regel unter Einbindung der jeweiligen IT-Abteilung, welche Maßnahmen zu treffen sind und welche Partner im Netzwerk erforderlich werden, etwa spezialisierte Rechtsanwälte, PR-Berater, etc.

Welche Ausschlüsse und Grenzen des Deckungsschutzes gibt es bei der Cyberversicherung?

Da sich, wie bereits erwähnt, noch kein einheitlicher Standard entwickelt hat, ist eine pauschale Aussage nicht möglich. Hier lohnt ein intensiver Vergleich. Teilweise finden sich in Bedingungswerken noch Klauseln wie »Stand der Technik«, welche den Versicherern im Schadenfall erheblichen Interpretationsspielraum bieten. Gute Cyberpolicen sollten sich auf wenige klar definierte Tatbestände wie Krieg, Vorsatztaten durch Repräsentanten, etc., beschränken.

Wie hat sich die Cyberversicherung entwickelt, insbesondere im Zusammenhang mit der DSGVO?

Der Cyberversicherungsmarkt entwickelt sich ganz unabhängig von der DSGVO ständig. Die Geschwindigkeit in welcher neue beziehungsweise aktualisierte Versicherungsbedingungen der einzelnen Anbieter auf den Markt kommen, ist beachtlich.

Die DSGVO hat sicherlich dazu beigetragen, dass Unternehmen den eigenen Datenschutz und Datensicherheit kritisch hinterfragen. Hierzu zählt als ein Element natürlich auch die Absicherung der Risiken, zumal das Thema beziehungsweise die Verantwortung für IT-Sicherheit ganz klar im Bereich der Unternehmensführung angesiedelt ist. Unzureichende Maßnahmen oder Verstöße können zu einer persönlich unbegrenzten Haftung des Organs führen und ziehen neben der finanziellen Inanspruchnahme auch die Kündigung des Arbeitsplatzes nach sich.

Welche USPs haben Ihre Versicherungsangebote?

Unser exklusives, eigens auf die Bedürfnisse unserer Kunden entwickeltes Bedingungswerk sowie unsere starken und renommierten Partner, also Risikoträger und Dienstleister. Für ganz entscheidend halten wir die Spezialisierung unserer Münchner Einheit. Die Dr. Hörtkorn München GmbH befasst sich seit vielen Jahren mit der Absicherung von IT- und Cyberrisiken.

Ganz aktuell wurde zudem die Schnittstelle zur Vertrauensschadenversicherung geschlossen. Immer wieder kommt es auf Seiten der Kundschaft bei den Fällen von CEO Fraud oder Fake President zu Unklarheiten, ob hier die Cyber- oder Vertrauensschadenversicherung betroffen ist. Da es in der Tat Konstellationen geben kann, in denen beide Policen getriggert wären, haben wir ein auf unsere Cyber Protection Plus abgestimmtes Bedingungswerk verabschiedet, welches zum einen Überschneidungen vermeidet und zum anderen speziell auf Schadenfälle aus dem Bereich der Wirtschaftskriminalität abzielt.

Herr Hörtkorn, vielen Dank für dieses Gespräch.