Nur mit einem ganzheitlichen präventiven Risikomanagement lassen sich Risiken wie Cyberkriminalität auf ein Minimum reduzieren.

DIGITALISIERUNG VON GESCHÄFTSPROZESSEN:

Risiken gezielt angehen

Die zunehmende Digitalisierung und Vernetzung von Geschäftsprozessen stellt Unternehmen branchenübergreifend vor immer größere Herausforderungen. Vor allem Datenschutz und Cyberkriminalität machen ein professionelles Risikomanagement unumgänglich.

VON MICHAEL EICHNER

Michael Eichner ist bei der Südvers GmbH im Bereich Produkt- und Servicemanagement für die Haftpflicht-, Unfall- und Rechtsschutzversicherung tätig.

Während die Speicherung und Verarbeitung von personenbezogenen Daten, der Abschluss von Verträgen via Internet oder die Nutzung von Cloud-Dienstleistungen längst zum Alltag geworden sind, nehmen auch kriminelle Handlungen in diesem Bereich dramatisch zu. Aktuelle Studien sowie die täglichen Berichte in den Medien belegen diese Tendenz eindrucksvoll. Doch auch ohne die zahlreichen finanziell oder ethisch motivierten Hackerangriffe steigen rechtliche und regulatorische Risiken für die Unternehmen: Datenschutzrichtlinien und -gesetze werden immer umfassender und gleichzeitig schärfer in der Sanktionierung. So sind beispielsweise im Rahmen der von EU-Digitalkommissar Günther Oettinger für das Jahr 2015 auf EU-Ebene angekündigten EU-Datenschutz-Grundverordnung Bußgelder in einer Höhe bis zu fünf Prozent des weltweiten Jahresumsatzes vorgesehen.

ABSICHERN MIT CYBER-VERSICHERUNGEN

Das IT-Sicherheits- und das Datenschutzrisiko eines Unternehmens sind heute untrennbar miteinander verbunden. Das so genannte Cyberrisiko ist bei jedem Unternehmen unterschiedlich und tangiert dabei nahezu alle betrieblichen Funktionen. Diese Tatsache stellt hohe Anforderungen an ein präventives und ganzheitliches Risikomanagement. Nicht ohne Grund rücken Cyberrisiken bei Risikomanagern und Unternehmensleitern immer mehr in den Fokus. Für die Fälle, in denen präventives Risikomanagement das Unternehmen nicht mehr schützen kann, bieten so genannte Cyber-Versicherungen Schutz für derartige Risiken, die über konventionelle Versicherungssparten nur unzureichend abgesichert sind. Die Deckung folgt dabei üblicherweise einem modularen Aufbau mit folgenden Elementen:

Cyber-/Datenschutz-Haftpflichtversicherung
Versicherungsschutz besteht für die Fälle, in denen das Unternehmen wegen eines Vermögensschadens von Dritten in Anspruch genommen wird. Hierbei geht es in erster Linie um die fahrlässige Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten und sonstigen vertraulichen Daten und Informationen Dritter. Dazu zählen zum Beispiel Geschäftsgeheimnisse.
Darüber hinaus besteht Versicherungsschutz bei einer vom versicherten Unternehmen zu verantwortenden IT-Sicherheitsverletzung, zum Beispiel bei einer fahrlässigen Weitergabe von Viren an Geschäftspartner.

Kostenschutz
Versicherungsschutz besteht für Kostentatbestände. Dazu gehören insbesondere

- Kosten, die auf Grund der gesetzlich vorgeschriebenen Benachrichtigung von Behörden und Betroffenen nach einem Datenschutzvorfall entstehen, etwa beim Abhandenkommen beziehungsweise bei unberechtigtem Kopieren von Kreditkartendaten.
- Kosten für Krisenmanagement-/PR-Berater.
- Kosten für IT-forensische Tätigkeiten nach einem Cyber-Angriff.
- Kosten für die Wiederherstellung von Daten und Systemen des Unternehmens nach Cyber-Angriffen.

Betriebsunterbrechung
Versicherungsschutz besteht für den entgangenen Betriebsgewinn und die fortlaufenden Kosten, wenn der Betrieb des Unternehmens aufgrund eines Cybervorfalls unterbrochen oder erheblich beeinträchtigt wurde.

Bedrohung/Erpressung
Versicherungsschutz besteht für die Zahlung von Erpressungsgeldern, die zur Beendigung einer Bedrohung/Erpressung durch Hacker von dem Unternehmen aufgewendet werden.

DAS CYBER-RISIKO-MANAGEMENT

Die Absicherung von Risiken aus dem Cyberbereich ist ein Baustein im ganzheitlichen, unternehmensspezifischen Risiko- und Versicherungsmanagement. Vorgelagert bestehen die Aufgaben in der Identifikation und Bewertung der bestehenden Cyberrisiken sowie der Überprüfung des derzeit schon vorhandenen Versicherungsschutzes. Erst im Anschluss erfolgt die Konzeption einer stets maßgeschneiderten Cyber-Versicherungslösung. Die Kosten für eine wirksame Risikoabsicherung sind dabei nicht nur von der aktuellen Geschäftstätigkeit des Unternehmens, sondern darüber hinaus auch in hohem Maße vom individuellen Stand der vorgehaltenen IT-Sicherheitstechnik abhängig. Die IT-Risikobewertung stellt daher eine zentrale Aufgabe dar, die oftmals nur unter Hinzuziehung von Spezialisten erfolgen kann. ■

► WWW.SUEDVERS.DE