Risikoprüfungen bei Cyber-Versicherungen

Kein gläserner Kunde zu befürchten

Vor dem Hintergrund jüngster Cyber-Angriffe auf namhafte Unternehmen stellt sich die Frage nach der Gefährdungslage und Möglichkeiten der Absicherung. Studien zeigen, dass der Diebstahl von Daten, die digitale Ausspähung von Informationen und die Sabotage von Computern nicht nur Risiken gewisser Betriebsgrößen sind. Es gibt kaum noch eine Branche, die keine digitalen Infrastrukturen betreibt. Mit der Abhängigkeit von der IT steigt die Gefahr, Cyberattacken und Systemausfälle zu erleben. Die Schäden können ganz gravierend sein.

Dr. Mark Wilhelm

Schadenpotentiale und Risikoanalyse ▸ Verliert beispielsweise ein Online-Händler, der Millionen Datensätze verwaltet, persönliche Daten seiner Kunden durch einen Hackerangriff, muss er jeden Betroffenen informieren – ein kostspieliges Unterfangen. Außerdem sind Schadenersatzansprüche möglich. Prominenter Fall eines (teilweise von einer Cyberversicherung getragenen) Schadens ist der US-Einzelhändler Target, der Anfang 2014 rund 71 Millionen Kundendaten verlor. Der Hackerangriff verursachte nicht nur einen Schaden von rund 61 Millionen US-D, sondern auch einen Reputationsverlust sowie den Abgang des CEO.

Für produzierende Unternehmen haben Betriebsunterbrechungen infolge von Cybervorfällen große Relevanz. Das Schadenpotential zeigt ein Hackerangriff auf ein deutsches Stahlwerk, der einen längeren Betriebsausfall und einen erheblichen Vermögensschaden zur Folge hatte. Aber auch Logistiker, die nur für zwei, drei Tage keine Sendungen abwickeln könnten, hätten nennenswerte Schäden.

Die Risikoanalyse im Unternehmen selbst ist der Ausgangspunkt für alle späteren Maßnahmen zur Absicherung. Sie erfasst technische Aspekte: Welche Systeme werden eingesetzt? Erfolgt die Steuerung des Schweißroboters in der Produktion autark oder besteht eine anfällige Verbindung mit dem Netzwerk des Unternehmens oder mit dem Internet? Wie wird die IT-Infrastruktur betrieben (Redundanzen und Interdependenzen)? Wie wird gesichert, stets mit Software auf dem letzten Stand zu arbeiten, und wie finden welche Datensicherungen statt? Hinzu kommen organisatorische Aspekte: Wie sind die Zugriffsrechte von Mitarbeitern geregelt? Gibt es (restriktive) Vorgaben zur Nutzung des Internets und ein Passwort-Management? Schließlich geht es um rechtliche Aspekte, etwa um den Punkt, wem gegenüber und in welchem Umfang Unternehmen bei Datenverlust haften.

Zur Risikoanalyse gehört aber auch die Prüfung, inwieweit andere bestehende Policen Risiken schon decken, die auch in der Cyberversicherung gedeckt würden. So kann ein Datendiebstahl durch einen eigenen Mitarbeiter unter den Schutz der Vertrauensschadenversicherung fallen. Eine Mehrfachversicherung desselben Risikos, die nur teuer ist und im Schadenfall Konflikte mit dem Versicherer oder unter den Versicherern hervorrufen kann, ist zu vermeiden. Im Übrigen können Unternehmen in der Risikoanalyse erkennen, gegen welche Cyber-Risiken sie sich nicht versichern müssen, obwohl Versicherer die Werbetrommel für Rund-um-sorglos-Pakete rühren.

Christian Drave

Volle Informationstransparenz? ▸ Wer Versicherungsschutz gegen Cyberrisiken und ihre Folgen einkaufen will, hat seine Risiken voll transparent zu machen. Diesbezüglich befürchten Unternehmen, dass sie dem Versicherer (oder von diesem eingeschalteten Dritten) Einblicke in hoch sensible Daten und Prozesse geben müssten, etwa in Forschungs- und Entwicklungsdaten. Versicherer sind tatsächlich darauf angewiesen, zutreffende, vollständige Informationen über zu versichernde Risiken zu erhalten. Auf Grund dieser Informationen wird die Prämie kalkuliert und Versicherungsschutz geboten. Das ist bei Cyberpolicen nicht anders. Gleichwohl wird niemand Zugriff auf hoch sensible Entwicklungsdaten seines Industriekunden verlangen. Geprüft wird aber, wie der Versicherungsnehmer seine Daten schützt.

Diese Datensicherheit im Unternehmen bestimmt das Risiko für den Versicherer, der bei einem Datenverlust die Kosten der Wiederherstellung der Daten trägt. Unternehmen sollten also schon in der Risikoanalyse sowie beim Vertragsabschluss auf Datenschutzvereinbarungen mit dem Versicherer und eventuell eingeschalteten Dienstleistern achten. Die Schlüsselfragen lauten: Wer hat Zugriff auf welche Daten des Unternehmens? Wie verwendet der Versicherer die Daten, die er kennenlernt, und wie garantiert er deren Sicherheit? Werden sie zuverlässig gelöscht, falls dann kein Vertrag zustande kommt?

Der gläserne Versicherungsnehmer steht nicht auf der Agenda. Bei Abschluss einer Cyberversicherung sind nur Angaben zu den wirtschaftlichen, technischen und organisatorischen Aspekten zu machen, nach denen der Versicherer fragt. Im Schadensfall ist ihm allerdings jede Auskunft zu erteilen, die zur Feststellung des Versicherungsfalls oder zum Umfang der Leistungspflicht erforderlich ist. Insoweit gilt für die Cyberversicherung nichts anderes als auch sonst.

Dabei ist aus Sicht von Unternehmen nicht auszuschließen, dass der Cyber-Versicherungsschutz im Schadensfall ausgehöhlt wird, da Versicherer in der Vertragsanbahnung verschieden agieren. Im Normalfall sind die Fragebögen noch überschaubar. Bei großen Cyberrisiken und hohen angefragten Deckungssummen verlangen Versicherer jedoch umfangreiche Risikoprüfungen, die durch sie selbst oder durch IT-Dienstleister erfolgen können, mit denen sie kooperieren.

▸ *Fortsetzung auf Seite 39*

▸ *Fortsetzung von Seite 36*

Ein solcher Vorgang könnte Versicherern Informationen aus dem Unternehmen verschaffen, die sie ohne die Risikoprüfung gar nicht hätten. Will sich etwa ein Versicherer im Schadensfall auf eine Obliegenheitsverletzung des Unternehmens berufen und die Versicherungsleistung kürzen, muss er das Fehlverhalten nachweisen, zum Beispiel als grobe Fahrlässigkeit. Dieser Beweis wäre ohne tiefen Einblick des Versicherers in die IT des Unternehmens nur schwer zu führen, weil Industriekunden nicht alles, was ihren Versicherungsschutz mindern könnte, mitteilen müssen, also auch nicht alle (temporären) Umstände, die für grobe Fahrlässigkeit sprächen. Unternehmen bleiben also für Versicherer ein nicht ganz offenes Buch. ■

RA Dr. Mark Wilhelm, LL.M., Partner und Fachanwalt für Versicherungsrecht, und RA Christian Drave, LL.M., Wilhelm Rechtsanwälte, Düsseldorf