HÖHERE RISIKEN FÜR UNTERNEHMER AB 2015

Cyberrisiken – Gefahren aus dem Netz

IT-Attacken stellen die betriebliche Haftungssicherung vor immer neue Herausforderungen. Das Competence Center IT bei Schunck bereitet Unternehmen auf die neue Europäische Datenschutzrichtlinie 2015 vor.

Unabhängig von Größe oder Branche ist heute jedes Unternehmen mit Informationstechnologie konfrontiert. Kritisch wird es, wenn sensible Daten Teil der Geschäftsabläufe sind. Hackerangriffe, Unachtsamkeit oder auch vorsätzliche Schäden durch Mitarbeiter treffen Unternehmen empfindlich. Die Schäden erreichen schnell ungeahnte Höhen, doch sind nur wenige Unternehmen gegen solche Verluste abgesichert.

EUROPÄISCHE DATENSCHUTZVERORDNUNG VERSCHÄRFT HAFTUNGSRISIKEN

„Die Berücksichtigung der IT-Risiken gehört für jedes Unternehmen zum Risikomanagement. Ein funktionierendes Sicherheitsmanagement im Datenschutz liegt in der Managerverantwortung. Trifft ein Unternehmen ein entsprechender Schaden, kann der verantwortliche Geschäftsführer persönlich und unbeschränkt mit seinem Privatvermögen in die Haftung genommen werden“, verdeutlicht Peter Janson, Kundenberater Industrie und Leiter des Competence Centers Informationstechnologie bei SCHUNCK. 2015 werde die neue Europäische Datenschutzverordnung mit weitreichenden Konsequenzen für Unternehmen aller Branchen verabschiedet. „Laut einer KPMG-Cybercrime-Studie von 2013 sind in der Risikowahrnehmung der befragten Geschäftsführer eher andere Unternehmen und nicht das eigene von E-Crime betroffen. Hier haben sehr viele Betriebe deutlichen Nachbesserungsbedarf, insbesondere im Hinblick auf die gesetzlichen Neuerungen ab 2015“, so Janson.

Foto: MHJ/iStock,SCHUNCK

IT-Unternehmen sollten die neue EU-Verordnung zum Datenschutz im Blick haben.

WENIG TRANSPARENZ, VIEL OPTIMIERUNGSBEDARF

Das Competence Center IT konzentriert sich auf Softwareentwickler, Systemhäuser und IT-Dienstleister. „Als wir uns mit dem Thema IT befassten, stellten wir große Defizite und Optimierungsmöglichkeiten bei den vorhandenen Versicherungslösungen fest“, erinnert sich Janson. Heute sei die Risikosituation ungleich gravierender und der Beratungsbedarf für IT-Unternehmen immens. Die Cyber-Bedrohung hat die Versicherungswelt vor neue große Herausforderungen gestellt. Das Thema Cyberrisiken lässt sich nicht mit den üblichen Versicherungstechniken greifen – zu komplex sind die technischen und juristischen Frage-

stellungen. Im Ergebnis mangelt es in diesem versicherungstechnischen Neuland an Transparenz, Vergleichbarkeit und Klarheit“, umreißt Janson die Situation.

Angriffe werden unter Einsatz der neuesten Technologien durchgeführt. Für Janson ist der Handlungsbedarf klar vorgegeben: „Unternehmer müssen sich darauf einstellen, eines Tages Opfer einer IT-Attacke zu werden. Bisher sind nur etwa 5 Prozent der Unternehmen in Deutschland gegen IT-Risiken abgesichert. Das ist ein extrem schlechter Wert.“

KERNTHEMEN DER IT-VERSICHERUNGEN

Im Jahr 2000 führte das Competence Center IT mit der SCHUNCK Net Risk eine spartenübergreifende und branchenspezifische Versicherungslösung für IT-Firmen ein. Gemeinsam mit namhaften IT-Versicherern entwickelte das Competence Center ein exklusives Bedingungswerk für die Versicherungsbelange von Softwareentwicklern, IT-Dienstleistern und EDV-Systemhäusern. „Viele Schäden, die wir in den letzten Jahren für Kunden abgewickelt haben, haben zu Modifizierungen der SCHUNCK Net Risk geführt. Dadurch entwickelt sich das Bedingungswerk immer weiter und hält mit den aktuellen Entwicklungen Schritt“, erläutert Janson. Aus Sicht des Competence Centers IT lässt sich die komplexe Struktur der Cyberrisiken derzeit in drei Themenkomplexe einteilen.

Die Cyber-Haftpflicht ist Teilbereich der klassischen IT-Haftpflicht. Sie regelt den Versicherungsschutz eines Unternehmens, wenn es wegen Datenschutzverletzungen Dritter belangt wird. Da werden zum Beispiel vertrauliche Daten, die der Geheimhaltung unterliegen, „gehackt“ und an direkte Mitbewerber übermittelt. Ein klassischer Schadenfall, bei dem die konventionelle Haftpflichtpolice mangels ausreichender Deckung für „vertragliche Haftung“ schnell an ihre Grenzen stößt.

Die Europäische Datenschutzverordnung: Ausblick auf die neue EU-Gesetzesvorlage

Spätestens 2015 wird die Inkraftsetzung der harmonisierten Europäischen Datenschutzrichtlinie mit deutlichen Verschärfungen für den Datenschutz erwartet. Dies sind die wesentlichen Eckdaten der Gesetzesvorlage:

- Wegfall der Begrenzung auf besonders sensible Daten – damit fallen deutlich mehr Datenpannen unter die Datenschutzverordnung als bisher
- Verschärfung der Informationspflichten mit materiellen und zeitlichen Vorgaben:
  - Informationspflicht gegenüber Dritten und Behörden innerhalb von 24 Stunden
  - gesetzlich geregelter Mindestinhalt der Mitteilung
  - Dokumentationspflichten
- Erweiterung des Bußgeldrahmens von 300.000 Euro auf bis zu 100 Mio. Euro.
- Die Möglichkeit von Schadensersatzverpflichtungen außerhalb des BDSG nach nationalem Recht bleibt bestehen
- Verschärfung der Datenschutzbestimmungen beim Informationsaustausch mit Drittländern

HÖCHSTER ANTEIL ENTFÄLLT AUF EIGENKOSTEN

Ebenso wichtig ist die Absicherung gegen externe Zugriffe auf das Firmennetz wie Viren oder Hackerangriffe. „Hier kommt es auf schnelles und organisiertes Handeln an, um der Meldepflicht Genüge zu tun und zugleich Schadenersatzpflichten oder Bußgeldforderungen zu begrenzen beziehungsweise zu verhindern“, verdeutlicht Janson die Prioritäten. Einige Versicherer bieten hier eine 24-Stunden-Hotline über externe Dienstleister an, die im Verdachtsfall sofort die notwendigen Maßnahmen einleiten. Diese Deckung beinhaltet insbesondere Kosten für forensische Untersuchungen, Meldungen bei betroffenen Dritten oder Regulierungsbehörden, Kreditüberwachungskosten oder Öffentlichkeitsarbeit.

Neben den reinen Kostenschäden drohen darüber hinaus weitergehende Eigenschäden. „Hierfür bieten wir Deckung im Rahmen eines Cyber-Eigenschadenbausteins an“, erläutert Janson. Dieser deckt zum Beispiel Gewinnverluste ab, wenn das Computersystem nicht zugänglich ist oder durch einen Virus Daten verloren gehen. Auch Kosten für die Wiederherstellung der Daten oder Netzwerke sind versicherbar.

Gerade Unternehmen, die sensible Kreditkartendaten verwalten, können bei einer Datenpanne gleich mehrfach getroffen werden. So drohen neben Schadenersatzansprüchen oder Bußgeldern von Kunden zusätzliche hohe Forderungen oder Vertragsstrafen aus Kreditkartenverarbeitungsvereinbarungen mit Kreditkartenunternehmen. Das Unternehmen erleidet darüber hinaus sicherlich massive Umsatzeinbußen. Zugleich muss es aber auch viel Geld in kriminaltechnische Untersuchungen und PR-Maßnahmen investieren, um seinen beschädigten Ruf wiederherzustellen“, beschreibt Janson den Extremfall.

Alles ist versicherbar, selbst reine Vertragsstrafen bei Verletzung von vertraglichen Geheimhaltungsvereinbarungen sind inzwischen kein versicherungstechnisches Tabu mehr.

Die Frage, welche Bausteine im Einzelfall benötigt werden und wie hoch das jeweilige Risiko ist, sollte Bestandteil der gemeinsamen Risikoanalyse von Unternehmensleitung und IT-Risikomanager sein. Die Individualität und Komplexität der Risiken macht eine intensive Beratung erforderlich. Aus Sicht von Peter Janson erweist sich kaum ein Versicherungsthema derzeit als so individuell wie die Absicherung von Cyberrisiken. ■

Peter Janson, Leiter des Competence Centers IT bei SCHUNCK