Innovative Lösungen in Zeiten von Cloud Computing und Cyber-Risiken

IT-Haftplicht-versicherung 3.0

Die Gefahr, dass IT-Unternehmen aufgrund von Datenschutzverletzungen in Anspruch genommen werden, steigt. Auch die besten technischen oder organisatorischen Schutzmechanismen bieten keinen 100-prozentigen Schutz. Somit ist es notwendig, die verbleibenden Risiken zu versichern.

Hacker knacken 18 Millionen E-Mail-Konten«; »Hacker erbeuten Daten von 38 Millionen Adobe-Kunden«; »Web-Account geknackt – Rewe Chef wird erpresst«; Amazon, Vodafone, Sky oder Ebay – Schlagzeilen, die uns täglich begleiten.

Weniger bekannt aber von großer praktischer Relevanz sind die folgenden Tatsachen:

- Allein am Frankfurter Flughafen wurden 2013 zirka 3.300 Laptops als gestohlen gemeldet oder abgegeben – viele mit sensiblen Daten.
- DDOS-Attacken haben allein im Februar 2014 um 371 Prozent zugenommen.
- Häufigste Ursache für Datenpannen sind Unachtsamkeit oder Vorsatz eigener Mitarbeiter
- 25 Prozent aller Rechner weltweit sind infiziert
- Allein in Deutschland erfolgen 30.000 Angriffe pro Tag
- In einigen Ländern werden mittlerweile höhere Umsätze mit dem Handel von Daten erzielt als mit dem Handel von Drogen.

Wichtige Erkenntnisse. Eine KPMG-Cybercrime-Studie aus dem Jahr 2013 lieferte folgende interessante Erkenntnisse:

- Unternehmen müssen sich darauf einstellen, dass die Angriffe künftig gezielt, maßgeschneidert und unter Einsatz neuester Technologien ausgeführt werden. Dabei ist die Frage nicht mehr ob, sondern lediglich wann und wie die Attacke stattfindet.
- Die befragten Unternehmen unterschätzen die Gefahr für das eigene Unternehmen, das Risiko von E-Crime wird tendenziell eher bei den anderen Unternehmen gesehen.
- Die größte Schwachstelle, die E-Crime begünstigt, liegt in der Unachtsamkeit von Mitarbeitern
- Es gibt Unternehmen, die Schäden durch E-Crime-Delikte zwar detailliert erfassen, dies aber noch nicht ausreichend im (IT-)Risikomanagement berücksichtigen.

Rechtslage. Die Risiken sind hochkomplex, die Haftungsregelungen äußerst vielschichtig. Die Herausforderungen an Unternehmen, IT-Risk-Manager und Fachanwälte sind enorm.

Mit der Reform des BDSG zum 01.09.2009 hat der Gesetzgeber in Deutschland den Bußgeldrahmen für Datenschutzdelikte nach § 43 BDSG bereits auf maximal 300.000 Euro angehoben – für 2015 ist eine generelle Überarbeitung der europäischen Datenschutzverordnung geplant. Außerdem ist die Vereinheitlichung der unterschiedlichen Datenschutzgesetze innerhalb der EU im Gespräch sowie eine weitere deutliche Anhebung des Bußgeldrahmens bei Datenschutzverletzungen bis zu 100 Millionen Euro. Es wird mit einer Aufstockung des Betrages auf 0,5 bis 2 Prozent des Jahresumsatzes gerechnet.

> »**Die Risiken sind hochkomplex,** die Haftungsregelungen äußerst vielschichtig. Die Herausforderungen an Unternehmen, IT-Risk-Manager und Fachanwälte sind enorm. «

Lösungsansatz Versicherung? Vor diesem Hintergrund wird die Cyber Security immer mehr vom Schlagwort zum Alltagsthema in den Unternehmen. Doch neben dem technischen Sicherheitsmanagement stellt sich auch die Frage nach der Versicherbarkeit von Datenschutzvorfällen. Obwohl die Zahl der Anbieter für Cyber-Policen in Deutschland stark angestiegen ist, sind gerade einmal 5 Prozent aller europäischen Unternehmen gegen Cyber-Risiken versichert (Stand: 2012). Deutschland belegt dabei im europäischen Vergleich einen der hinteren Plätze. In den USA beträgt der Abdeckungsgrad bereits rund 30 Prozent.

Kaum ein anderes Thema hat die Assekuranz in den letzten Jahren vor solche Herausforderungen gestellt – zu komplex sind die technischen und juristischen Fragestellungen. Cyber-Risiken lassen sich einfach nicht mit den üblichen Versicherungstechniken greifen. In diesem versicherungstechnischen Neuland mangelt es an Transparenz, Vergleichbarkeit und Klarheit.

Da es im Bereich der Risikoabsicherung von Cyber-Risiken bislang keine standardisierten Verbandsbedingungen gibt, entwickelt jeder Versicherer ein anderes Vertragskonzept – ganz nach eigenem Gusto. Das ist ein Alptraum für jeden Kunden und Versicherungsmakler, die sich einen objektiven Überblick zu Leistungen, Ausschlüssen und Prämien verschaffen möchten.

»Versicherung von Cyber-Risiken« – entscheidend ist die Herangehensweise. Die meisten Diskussionen zum Thema »Cyber-Versicherung« scheitern bereits bei der banalen Frage: »Um was geht es eigentlich?« Es zeichnet sich eine Einteilung in drei Themenkomplexe ab:

Cyber-Haftpflicht:
Versicherungsschutz bei Inanspruchnahme wegen Datenschutzverletzungen durch Dritte.

Cyber-Eigenschadenversicherung (Datenkasko):
Versicherungsschutz bei Eigenschäden infolge von Datenpannen.

Cyber-Kostenschäden:
Übernahme von Kosten für die Umsetzung von Sofortmaßnahmen (Stichwort: Forensik), Meldeverpflichtungen gegenüber betroffenen Personen, Kreditkarten-Monitoring etc. Da diese Kostenschäden sowohl bei Haftungs- wie auch bei Eigenschäden anfallen können, muss eine adäquate Versiche-

rungslösung so aufgebaut sein, dass beide Fälle unter die Deckung fallen.

Deckt die IT-Haftpflicht auch Schäden in Zusammenhang mit der Inanspruchnahme bei Cyber-Risiken?

Kurze Antwort: Ja, Aber...! Sofern Sie eine Betriebs- und Vermögensschadenhaftpflicht für Ihr Unternehmen abgeschlossen haben, ist die Cyber-Haftpflicht integrierter Bestandteil Ihres Versicherungsschutzes.

Ob im konkreten Schadensfall Ihr IT-Haftpflichtversicherer auch wirklich die Deckung bejaht, hängt sehr stark von der Qualität der Versicherungsbedingungen ab. Bei den heute am Markt etablierten IT-Haftpflichtpolicen ist eine adäquate Absicherung in den allermeisten Fällen nicht gegeben. Spezialanbieter für IT-Versicherungen wie beispielsweise der Versicherungsmakler SCHUNCK GROUP, bieten bereits heute Haftpflichtpolicen, bei denen alle relevanten Cyber-Haftungsrisiken mitversichert sind.

Welche Fälle könnten mit der IT-Haftpflicht versichert werden? Worauf kommt es an?

Priorität 1:

Beim Verdacht auf eine **Datenschutzpanne** müssen die gesetzlichen Melde- beziehungsweise Benachrichtigungspflichten eingehalten werden:

Für besonders sensible Daten sind diese heute u.a. im § 42a BDSG geregelt. Mit der für 2015 erwarteten EU-Gesetzesvorlage werden die Anforderungen deutlich verschärft. So entfällt nach heutiger Entwurfsfassung insbesondere die Begrenzung auf Risikodaten (wie beispielsweise im § 42a BDSG). Auch hinsichtlich der Informations- und Dokumentationspflichten wird es Neuregelungen geben (beispielsweise Informationspflicht binnen 24 Stunden, gesetzlich geregelter Mindestinhalt der Meldung, Dokumentationspflichten).

Ist Ihr IT-Risk Management auf diese Situation vorbereitet?

Die Mitversicherung von Cyber-Kostenschäden kann hier äußerst hilfreich sein. Hierzu gehören beispielsweise forensische Untersuchungen, Übernahme von Meldeverpflichtungen an Regulierungsbehörden oder betroffene Personen, Kreditüberwachungskosten, Öffentlichkeitsarbeit oder sogenannte Reputationskosten. Doch dieser Vertragsbaustein ist nur dann effektiv, wenn im Rahmen Ihrer Versicherungspolice zugleich die Einschaltung eines passenden Risk Consultants mit einer **24/365-Krisenhotline** inkludiert ist.

> **Bei begründetem Verdacht** auf das Vorliegen einer Datenschutzverletzung zählt nur eines: Zeit und schnelles, organisiertes Handeln um datenschutzrechtliche Konsequenzen im Vorfeld zu vermeiden. «

Bei einem begründeten Verdacht auf das Vorliegen einer Datenschutzverletzung zählt nur eines: Zeit und schnelles, organisiertes Handeln um datenschutzrechtliche Konsequenzen (Einhaltung von Informationspflichten gem. § 42a BDSG, Schadensersatzpflichten gem. § 7 BDSG oder Bußgelder gem. § 43 Abs. 1 Nr. 7 BDSG) im Vorfeld zu vermeiden. Einige der großen Versicherer von Cyber-Policen bieten bereits heute entsprechende Krisenmanager an.

Im Rahmen der IT-Haftpflicht ist der Baustein »Cyber-Kostenschäden« bis heute jedoch nicht oder zumindest nur unzureichend versichert. Allein die Verpflichtung zum Ergreifen von Datenschutzmaßnahmen, wie beispielsweise durch das BDSG, stellt noch keinen gesetzlichen Schadensersatzanspruch eines Betroffenen dar. Daraus resultiert, dass reine Kostenschäden als Eigenschäden nicht unter die übliche IT-Haftpflichtdeckung fallen.

Einige Spezialanbieter denken hier bereits um und bieten Versicherungsschutz inklusive Krisenmanagement im Rahmen der Haftpflichtpolice mit an. Ein Vergleich lohnt sich!

Priorität 2:

Gesetzliche Haftpflicht bei **Datenschutzverletzungen,** auch bei Vorsatz oder wissentlicher Pflichtverletzung eigener Mitarbeiter.

Die gesetzliche Haftpflicht bei Datenschutzverletzungen ist in den gängigen IT-Haftpflichtpolicen geregelt. Beruht die Ursache für den Schadensersatzanspruch jedoch auf Vorsatz oder wissentlicher Pflichtverletzung eines Mitarbeiters, greifen häufig Deckungsausschlüsse.

Fallbeispiele für die gesetzliche Haftpflicht:

Eine neue Mitarbeiterin eines IT-Unternehmens speichert versehentlich sensible Daten auf einem falschen Laufwerk. Im Rahmen einer Schulungsveranstaltung werden von einem externen Teilnehmer die Daten zufällig entdeckt und weiter verschickt.

Ein Mitarbeiter lässt seinen Firmen-Laptop am Flughafen für Sekunden aus den Augen. Der Laptop mit vertraulichen Konstruktionsdaten eines Kunden wird gestohlen.

Fallbeispiele für die gesetzliche Haftpflicht bei Vorsatz oder wissentlicher Pflichtverletzung durch eigene Mitarbeiter:

Ein frustrierter Mitarbeiter eines IT-Unternehmens löscht absichtlich Datenbestände von Kunden und verursacht so einen Haftpflichtanspruch.

Ein Mitarbeiter führt vereinbarte Programmtests nicht durch, da »es bisher auch immer geklappt hat«. Schließlich ist gleich Feierabend und am Abend steht Fußball auf dem Programm. Durch eine Fehlfunktion entsteht ein Haftpflichtschaden.

Priorität 3:
Vertragliche Haftung und/oder »verschuldensunabhängige Haftung«
Neben der »gesetzlichen Haftung« ist gerade für IT-Unternehmen die »vertragliche Haftung« von Bedeutung.

Fallbeispiele:
Ein IT-Unternehmen als Betreiber eines Rechenzentrums wird durch eine DoS-Attacke vorübergehend lahm gelegt. Als Folge dieser Betriebsunterbrechung können vertraglich zugesicherte Service Levels nicht eingehalten werden.

Hacker erbeuten Kreditkarteninformationen von Kunden des IT-Unternehmens. Die betroffenen Kreditkartenunternehmen stellen Schadenersatzansprüche für die gesonderte Überwachung der Kreditkarten sowie den entstandenen Schaden durch den Missbrauch der Kartendaten.

Sonderfall: Cloud Computing
Grundsatz: Bedient sich ein IT-Unternehmen eines externen Cloud-Anbieters, verbleibt die volle Verantwortung und damit Haftung beim Cloud-Nutzer (§ 11 Abs. 1 BDSG).

Neben den offensichtlichen Vorteilen einer Cloud-Lösung, bietet das Cloud-Computing eine Fülle von Risiken, insbesondere im Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit von Daten. Beim Kunden können hohe Vermögensschäden entstehen, beispielsweise aufgrund Wiederherstellung von Daten oder Gewinnausfällen, weil das IT-Unternehmen als Cloud-Nutzer haftet. Das Risiko wird noch größer, wenn die Datenverarbeitung außerhalb des EU-Raumes geschieht. So könnten Daten in Ländern gespeichert oder verarbeitet werden, die über keine ausreichende Datenschutzgesetzgebung verfügen oder in denen Behörden oder Gerichte den Zugriff verlangen können. Der Speicherort ist insbesondere bei Public Clouds oft nicht erkennbar.

Nach dem Gesetz haftet das IT-Unternehmen gegenüber seinem Kunden auch für das Verschulden des Cloud-Anbieters, soweit dieser als Erfüllungsgehilfe angesehen wird. Ob der Haftpflichtversicherer in einem solchen Schadenfall eintritt, hängt maßgeblich davon ab, ob eine gesetzliche Haftungsgrundlage gegeben ist und ob der Cloud-Nutzer nicht bereits im Vorfeld vertraglich jegliche Regressmöglichkeit gegenüber dem Cloud-Anbieter abbedungen hat.

Schwierig wird es, wenn der Cloud-Anbieter bei einem Datenverlust die gesetzlichen Verpflichtungen in Sachen Datenschutz und Informationssicherheit seines Landes nachweislich erfüllt hat und das IT-Unternehmen als Cloud-Nutzer gegenüber seinem Kunden verschuldensunabhängig haftet. In einem solchen Fall kann der Cloud-Anbieter nicht in die Verantwortung gezogen werden. Nur eine umfassende Versicherungspolice, welche auch den Drittanbietern in eine verschuldensunabhängige Haftung bei Datenverlusten als Erfüllungsgehilfen einbindet, kann hier das Unternehmen vor finanziellen Verlusten schützen.

> **Neben den offensichtlichen Vorteilen** bietet das Cloud-Computing eine Fülle von Risiken, insbesondere im Hinblick auf die Verfügbarkeit, Integrität und Vertraulichkeit von Daten. «

Zusammenfassung. Der Markt für reine Cyber-Policen steckt noch in den Kinderschuhen. Es gibt zwar bereits vielversprechende Produkte, von einer Markttransparenz kann bislang jedoch keinesfalls die Rede sein.

IT-Unternehmen haben die Möglichkeit im Rahmen ihrer Betriebs- und Vermögensschadenhaftpflicht zumindest die Cyber-Haftpflicht und Cyber-Kostenschäden (inklusive 24 h Krisenhotline) kostengünstig oder sogar ohne Zusatzkosten zu versichern. Die Qualität der Versicherungsbedingungen muss im Hinblick auf die genannten Kostenschäden sowie die vertragliche und verschuldensunabhängige Haftung geprüft werden. Versicherungsmakler wie die SCHUNCK GROUP, die sich auf die Bedürfnisse der IT-Branche spezialisiert haben, können Unternehmern helfen, die erheblichen Risiken versicherungstechnisch bestmöglich in den Griff zu bekommen.

Peter Janson

Peter Janson,
Competence Center IT,
Schunck

www.schunck.de