AUSWIRKUNGEN VON CYBER-RISIKEN

auf den D&O-Versicherungsschutz und Handlungsempfehlungen für Geschäftsführer

Michael Hendricks,
Rechtsanwalt,
Hendricks + Partner Rechtsanwälte mbB
und

Theodoros Bitis,
Syndikusrechtsanwalt,
Howden Germany GmbH

Cyber-Attacken und Datensicherheitsverletzungen zählen heutzutage zu den größten Risiken für mittelständische Unternehmen in Deutschland. Mit der wachsenden Cyber-Bedrohung hat auch das breite Spektrum der potenziellen Haftungsquellen für Manager eine erhebliche Erweiterung erfahren. Für Geschäftsführer wird es daher immer wichtiger, sich über den genauen Umfang ihrer Haftungsrisiken und auch ihres Versicherungsschutzes Gedanken zu machen.

Geschäftsführerhaftung im Rahmen von IT-Sicherheitsverletzungen

Der Geschäftsführer trägt die Verantwortung für die ordnungsgemäße Leitung des Unternehmens. Dazu gehören auch die interne IT-Organisation und die IT-Sicherheit. Er haftet im Zusammenhang mit seiner beruflichen Tätigkeit grundsätzlich unbeschränkt mit seinem gesamten Privatvermögen.

Dies gilt auch dann, wenn eine Pflichtenübertragung auf internes oder externes IT-Personal erfolgt. Bei der Pflichtenübertragung ist nicht nur auf eine sorgfältige Auswahl der beauftragten Personen, sondern auch darauf zu achten, dass diese der übertragenen Verantwortung nachkommen. Begeht der Geschäftsführer schuldhaft einen Pflichtverstoß bei der Auswahl oder Überwachung des Personals, so haftet dieser für die daraus resultierenden Vermögensschäden.

Mit dem Eintritt eines Cyber-Schadenfalls werden auch die getroffenen Maßnahmen auf den Prüfstand gestellt. Daraus ergeben sich sehr häufig die folgenden Fragen:

Wurde für die IT-Sicherheit ein angemessenes Budget bereitgestellt? Wurden ausreichende Maßnahmen im Rahmen des IT-Risikomanagements getroffen? Wurden die Maßstäbe für ein funktionierendes Krisenmanagement insbesondere durch die Schaffung eines effektiven IT-Notfallplans gesetzt?

Wurden keine Maßnahmen angestoßen oder erweisen sich diese als lückenhaft, kann den Geschäftsleitern ein Organisationsverschulden zum Vorwurf gemacht werden.

Da Cyber-Risiken sehr vielfältig sind […], sollten die Geschäftsführer ein speziell auf die Bedürfnisse des Unternehmens abgestimmtes IT-Risikomanagement einrichten, kontinuierlich aufrechterhalten und bei Bedarf den neuen Gegebenheiten anpassen.

Einrichtung und Aufrechterhaltung eines ordnungsgemäßen IT-Risikomanagements

Da Cyber-Risiken sehr vielfältig sind und in schwerwiegenden Fällen sogar eine Bestandsgefährdung für die Unternehmen darstellen, sollten die Geschäftsführer ein speziell auf die Bedürfnisse des Unternehmens abgestimmtes IT-Risikomanagement einrichten, kontinuierlich aufrechterhalten und bei Bedarf den neuen Gegebenheiten anpassen.

Die IT-Risikoorganisation sollte dabei ein breites Spektrum an Maßnahmen zur Sicherstellung eines ordnungsgemäßen Betriebsablaufs erfassen. Dazu gehören insbesondere die zeitgemäße Fortentwicklung der unternehmensinternen Richtlinien, turnusmäßige Schulungen von Mitarbeitern, eine einwandfreie IT-Compliance, eine maßgeschneiderte Strategie für die Öffentlichkeitsarbeit sowie ein funktionierendes Lieferantenmanagement.

Darüber hinaus stellt eine sorgfältige Dokumentation für den Geschäftsführer eine wichtige Vorgehensweise dar, um mit den entsprechenden Nachweisen den möglichen Vorwurf einer Pflichtverletzung in einem Haftungsprozess oder behördlichen Verfahren entkräften zu können.

Schutzbereich und Zweck der D&O-Versicherung

Wird der Geschäftsführer aufgrund des Vorwurfs eines schuldhaften Verhaltens auf Ersatz eines Vermögensschadens in Anspruch genommen, springt für ihn die sog. D&O-Versicherung ein (D&O steht als Abkürzung für Directors & Officers). Diese steht ihm nicht nur bei Ansprüchen der eigenen Gesellschaft (Innenhaftung), sondern auch bei Drittansprüchen (Außenhaftung) zur Verfügung.

Die D&O-Versicherung verfolgt in erster Linie den Zweck, das private Vermögen des Unternehmensleiters, der bereits bei leichtester Fahrlässigkeit einer unbeschränkten Haftung ausgesetzt ist, zu schützen. Darüber hinaus dient die D&O-Versicherung auch dem Fortbestand der Gesellschaft, da die private Haftungsmasse von Verantwortlichen zum Ausgleich von Schadenersatzansprüchen in Innenhaftungsfällen in der Regel nicht genügt.

Herausforderungen für die D&O-Versicherung im Digitalisierungszeitalter

Der D&O Versicherer bietet – angesichts der sehr oft streitigen Haftungslage – zunächst Deckung für die Abwehr von Schadensersatzansprüchen. Der Haftungsprozess nimmt dann sehr viel Zeit in Anspruch und endet nach langwierigen Verhandlungen sehr häufig in Vergleichen, deren Beträge erfahrungsgemäß nur einen sehr geringen Teil des Gesamtschadens darstellen.

In Cyber-Schadenfällen benötigen Geschäftsführer jedoch eine sofortige Unterstützung, um nicht die Liquidität des Unternehmens zu gefährden.

In Cyber-Schadenfällen benötigen Geschäftsführer jedoch eine sofortige Unterstützung, um nicht die Liquidität des Unternehmens zu gefährden. Unternehmen können bei ungeplanten Geschäftsausfällen bereits nach kürzester Zeit in ernsthafte finanzielle Schwierigkeiten geraten.

Kommen anlässlich des Schadenfalls auch interne IT-Sicherheitsmängel zum Vorschein, besteht zudem die Gefahr, dass der D&O-Versicherer den Deckungsschutz für die Geschäftsführer mit gravierenden Einschränkungen, etwa durch Bedingungsausschlüsse oder Deckungssummenreduzierungen, versehen wird. In schwerwiegenden Fällen droht sogar die Kündigung der D&O-Versicherungspolice.

Deckungslücken in den herkömmlichen Versicherungssparten

Führt eine Cyber-Attacke zu Betriebsunterbrechungen, ist den Unternehmen auch nicht mit den herkömmlichen Versicherungen geholfen.

Betriebsunterbrechungsschäden, die aus Hackerangriffen resultieren, sind grundsätzlich nicht vom Deckungsschutz marktgängiger Sachversicherungen erfasst. Diese greifen in der Regel nur bei sachschadenbedingten Betriebsunterbrechungen. Cyber-Angriffe führen jedoch sehr selten zu Sachschäden.

Der überwiegende Teil der Cyber-Schäden wird jedoch durch nicht zielgerichtete Attacken, beispielsweise durch breit gestreute Verschlüsselungstrojaner, ausgelöst.

Der Einkauf von Cyber-Ausschnittsdeckungen und -Zusatzbausteinen, die vornehmlich in Sach- oder Vertrauensschaden-Versicherungskonzepten vorzufinden sind, wird ebenfalls nicht den Anforderungen an ein zeitgemäßes Risiko- und Versicherungsmanagement gerecht. Diese kommen regelmäßig nur bei zielgerichteten Eingriffen in die IT-Systeme zur Anwendung. Der überwiegende Teil der Cyber-Schäden wird jedoch durch nicht zielgerichtete Attacken, beispielsweise durch breit gestreute Verschlüsselungstrojaner, ausgelöst.

Cyber-Versicherung als sinnvolle Ergänzung

In den letzten Jahren hat sich daher die Cyber-Versicherung als sinnvolle Ergänzung zu den konventionellen Bestandsversicherungen eigenständig etabliert.

Die Cyber-Versicherung greift zum einen bei den finanziellen Folgen, die den Unternehmen durch Störung des Betriebsablaufs aufgrund einer Cyber-Attacke oder durch Haftpflichtansprüche Dritter wegen Datenschutzverletzungen entstehen.

Zum anderen bietet die Cyber-Versicherung ein Netzwerk von hochspezialisierten Forensikern, Rechtsanwälten und PR-Beratern […].

Zum anderen bietet die Cyber-Versicherung ein Netzwerk von hochspezialisierten Forensikern, Rechtsanwälten und PR-Beratern, welches den Betroffenen bei der Bewältigung von Sicherheitsvorfällen zur Seite steht. Das Leistungsspektrum des Expertennetzwerks erfasst insbesondere die forensische und rechtliche Aufarbeitung des Cyber-Vorfalls, die Wiederherstellung der IT-Systeme, Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebes und die Krisenkommunikation.

Krisenmanagement und Versicherungsschutz am Beispiel einer „Ransomware“-Attacke

Die Wichtigkeit eines funktionierenden Cyber-Krisenmanagements und eines maßgeschneiderten Versicherungsschutzes wird an folgendem Beispiel sehr deutlich.

Im November 2018 wurde der Maschinenbaukonzern Krauss-Maffei mittels einer Verschlüsselungssoftware („Ransomware“) attackiert. Kriminelle konnten hierdurch einen überwiegenden Teil der Konzern-IT verschlüsseln und stellten Lösegeldforderungen für die Entschlüsselung. Aufgrund dieser Attacke konnte an einigen Standorten der Unternehmensgruppe für ca. zwei Wochen nur mit erheblich reduzierter Leistung gearbeitet werden.

Hierdurch wird ersichtlich, dass erfolgreiche Cyber-Attacken nicht unerhebliche Geschäftsausfälle und in schwerwiegenden Fällen sogar einen Gesamtschaden in Millionenhöhe verursachen können. Die Cyber-Versicherung springt in derartigen Fällen ein und übernimmt die hohen Ertragsausfälle.

Für seine Entscheidung kann er einen Expertenrat über die Cyber-Versicherung in Anspruch nehmen.

Für den Geschäftsführer stellt sich in einem Cyber-Vorfall auch die Frage, ob und inwiefern er Behörden, Betriebsangehörige, Kunden und Geschäftspartner zu informieren hat. Für seine Entscheidung kann er einen Expertenrat über die Cyber-Versicherung in Anspruch nehmen. Dadurch wird vermieden, dass die Anzeige des Vorfalls unvollständig oder verspätet bei den zuständigen Behörden und den betroffenen Personen erfolgt.

Letzteres wird in einem aktuellen Fall dem Management der internationalen Unternehmensgruppe Marriott angelastet. Kriminelle hatten sich bereits vor einigen Jahren unautorisierten Zugang zu einem Online-Reservierungssystem des Hotelkonzerns verschafft und damit Zugriff auf ca. 500 Mio. Kundendaten erlangt. Dem Management werden nunmehr IT-Sicherheitsverletzungen bezüglich des internen Umgangs mit Kundendaten und die verspätete Benachrichtigung von Kunden, Behörden und Aktionären über den Cyber-Vorfall vorgeworfen.

Die Cyber-Versicherung übernimmt in derartigen Fällen für das Unternehmen die Kosten für die Haftungsabwehr und die Schadenszahlungen gegenüber Dritten.

Aktuelle Marktentwicklung im Bereich der Cyber-Versicherung

Bis dato wurden Cyber-Versicherungspolicen nur im Ausland, schwerpunktmäßig in USA, Israel und Großbritannien, als selbstverständlich angesehen. In den Chefetagen deutscher Unternehmen wird in jüngster Zeit zunehmend erkannt, dass selbst der Einkauf neuester Technologien nicht vor erfolgreichen Angriffen schützt und damit den Unternehmen regelmäßig ein versicherbares (Rest-)Risiko verbleibt.

Darüber hinaus gewinnt auch ein weiterer Faktor immer mehr an Bedeutung: Die durch die Cyber-Versicherung bereitgestellten Spezialisten haben bereits zahlreiche Erfahrungen im Rahmen von Cyber-Schadenfällen sammeln können und bieten den Betroffenen im Ernstfall eine qualitativ hochwertige Unterstützung mit ihrer fachlichen Expertise und kontinuierlichen Marktbeobachtung. Die Cyber-Versicherung entwickelt sich daher mit dem bereitgestellten Netzwerk zu einem nicht mehr wegzudenkenden Teil des IT-Risikomanagements für die Unternehmen.

Über 20 Versicherer bieten derzeit in Deutschland Cyber-Versicherungslösungen an. Angesichts des sehr inhomogenen Leistungsspektrums lassen sich die Cyber-Versicherungskonzepte – ähnlich wie die D&O-Versicherungsbedingungen – nur mühsam miteinander vergleichen und erfordern daher eine Beratung durch Versicherungsspezialisten oder Rechtsexperten. ■