GMBH-GESCHÄFTS-FÜHRUNG 2022

zum aktuellen Fachbeitrag

von Theodoros Bitis
Head of Cyber / CoE

Das E-Book für die Geschäftsführung mit den haftungsträchtigen Themen dieser Zeit – exklusiv und aktuell.

www.euroforum.de/geschaeftsfuehrer

euroforum
Live Experience by HANDELSBLATT MEDIA GROUP

Cyber-Risiken und Managerhaftung: Absicherungsmöglichkeiten im Zusammenhang mit IT-Sicherheitsvorfällen

Theodoros Bitis, LL.M.,
Prokurist, Syndikusrechtsanwalt,
Head of Cyber, Center of Excellence,
Howden

Mit der rasant wachsenden Bedrohung durch Cyberkriminalität steigen auch die Haftungsrisiken für die Unternehmensführung. Bekanntermaßen trägt die Geschäftsleitung die Verantwortung für die ordnungsgemäße Unternehmensführung – und dazu gehören auch die interne IT-Organisation und die IT-Sicherheit.

Erweisen sich die Maßnahmen vor und während eines IT-Sicherheitsvorfalls als lückenhaft, wird relativ zügig der Vorwurf eines Organisationsverschuldens laut. Bei schuldhaften Versäumnissen können dann die Manager auf Schadensersatz in Anspruch genommen werden.

Anders als ein einfacher Angestellter, der sich bei einem pflichtwidrigen Verhalten gegebenenfalls auf die Grundsätze des innerbetrieblichen Schadensausgleichs berufen kann, haftet ein Manager im Zusammenhang mit seiner beruflichen Tätigkeit unbeschränkt – und zwar mit seinem gesamten Privatvermögen. Wenn ihm beispielsweise schuldhafte Versäumnisse bei der Überwachung der IT-Sicherheit nachgewiesen werden, die in eine erfolgreiche Cyber-Attacke münden, kann das schwerwiegende finanzielle Folgen auch für ihn haben.

Aktuelle Entwicklungen

In den USA haben Gerichte und Behörden im Jahr 2021 einen neuen Höchststand an Managerhaftungsfällen verbunden mit Cyber-Risiken verzeichnet. In einem der bekanntesten Fälle befasste sich die US-Börsenaufsicht SEC sogar mit einem Versicherer: Das Management der First American Financial Corp. erfuhr erst durch die Anfrage eines Journalisten von einer Schwachstelle in den hauseigenen IT-Systemen, die vermeintlich zur Offenlegung einiger hundert Millionen von Datensätzen geführt hatte. Was die Unternehmensverantwortlichen, als sie sodann eine Stellungnahme veröffentlichten, nicht wussten: Die eigenen IT-Sicherheitsbeauftragten hatten die Schwachstelle bereits früher entdeckt, aber noch nicht an das Management gemeldet. In diesem Fall konnte sich das Management einer Haftung vorerst entziehen, da kein Organisationsverschulden nachgewiesen werden konnte. Hätte sich aber nachweisen lassen, dass das Management schon früher Kenntnis hatte und untätig blieb, hätten dem Unternehmen und seinen Vertretern empfindliche Strafen gedroht.

Ein weiterer aufsehenerregender Fall betraf Pearson plc, einen britischen Bildungsdienstleister, ebenfalls mit Börsennotierung in den USA. Im März 2019 entdeckte das Unternehmen, dass ein Hacker auf Daten von Schülern und Schulbediensteten zugegriffen und diese heruntergeladen hatte. Das Unternehmen informierte die betroffenen Personen über den Verstoß, entschied sich jedoch, diesen Vorfall nicht auch gegenüber der US-Börsenaufsicht zu kommunizieren. Als dies bekannt wurde, waren auch die Anleger verärgert. Das Unternehmen konnte den Streit durch Zahlung einer Geldstrafe in Höhe von 1 Million US-Dollar beilegen.

Beide Fälle zeigen: Es gibt immer mehr Alarmzeichen für Manager, beim Thema IT-Sicherheit höchste Sorgfalt walten zu lassen.

Noch ist die Zahl der gerichtlichen Klagen überschaubar und die Erfolgsbilanz der Klägerseite durchwachsen. Mit steigenden Cyber-Risiken ist aber keineswegs ausgemacht, dass dies auch in Zukunft so bleibt.

Investitionen in IT-Sicherheit

Angesichts der deutlich gestiegenen Haftungsrisiken liegt es auf der Hand, dass Unternehmen gut beraten sind, entsprechende Vorkehrungen gegen Cyber-Angriffe zu treffen. Unternehmensleiter kommen heutzutage nicht daran vorbei, eine umfassende IT-Risikoorganisation mit einem breiten Spektrum an Maßnahmen zur Sicherstellung eines ordnungsgemäßen Betriebsablaufs aufzubauen und fortzuentwickeln.

Wesentliche Elemente eines solchen Maßnahmenkonzepts für den Notfall sind die Bereitstellung angemessener Budgets für die IT-Sicherheit und ausreichende personelle Kapazitäten, organisatorische Maßnahmen wie Richtlinienmanagement, verpflichtende Mitarbeiterschulungen, Notfall-, Krisenreaktions- und Business-Continuity-Pläne, aber auch technische Maßnahmen wie z.B. die Einführung einer Multifaktorauthentifizierung bei externen Zugriffen, der Schutz mobiler Geräte, eine Trennung von Admin- und sonstigen Benutzerkonten, regelmäßige Backups und erhöhte Schutzmaßnahmen im Bereich der Produktionssysteme.

Herausforderungen für die Versicherungsbranche

Manager, die sich gegen Cyber-Risiken versichern möchten, stoßen sehr zügig an Grenzen. Herkömmliche Versicherungssparten bieten in diesem Bereich keinen oder nur einen unzureichenden Schutz für Unternehmen. Nicht selten suchen Manager einen Ausweg in der hauseigenen Managerhaftpflichtversicherung, der D&O-Versicherung. Diese verfolgt in erster Linie den Zweck, das Privatvermögen des Managers vor Drittansprüchen (Außenhaftung) oder Ansprüchen der eigenen Gesellschaft (Innenhaftung) zu schützen. Darüber hinaus dient die D&O-Versicherung dem Fortbestand der Gesellschaft, da die private Haftungsmasse des Managers zum Ausgleich von Schadenersatzansprüchen in der Regel nicht ausreicht.

Ob bei einem Cyber-Angriff ein Haftungsfall im Sinne der D&O-Versicherung vorliegt, ist aber sehr oft streitig. Der Versicherer bietet daher zunächst Deckung lediglich für die Verteidigung der in Anspruch genommenen Manager gegen die im Raum stehenden Vorwürfe von Pflichtverletzungen. Der Prozess nimmt dann in der Regel sehr viel Zeit in Anspruch und endet häufig mit einem Vergleich. Die Vergleichsbeträge erfassen meist nur einen geringen Teil des Gesamtschadens.

Bei Cyber-Vorfällen benötigen Unternehmen und ihre Manager allerdings eine sofortige Unterstützung. Denn wenn schwerwiegende Cyber-Attacken den Geschäftsbetrieb lahmlegen, kann dies schnell auch die Liquidität des Unternehmens gefährden und es in eine ernsthafte finanzielle Schieflage bringen. Langwierige Rechtsstreitigkeiten können sich weder die klagende Gesellschaft noch der beklagte Manager leisten. Ein langes Zuwarten auf die Schadenregulierung ist hier nicht möglich.

Dem Zweck des Fortbestands der Gesellschaft wird auch nicht gedient, wenn sich der Verdacht eines Organisationsverschuldens als unbegründet erweist und der Manager nicht schadensersatzpflichtig ist. Denn dann bleibt das Unternehmen auf dem Schaden sitzen.

Manager laufen zudem Gefahr, dass Versicherer anlässlich der offenkundigen Sicherheitslücken in der Unternehmens-IT ihren D&O-Versicherungsschutz mit gravierenden Deckungseinschränkungen versehen, etwa durch Bedingungsausschlüsse oder Deckungssummenreduzierungen. Im Worst Case kann sogar die Kündigung der D&O-Unternehmenspolice drohen.

Cyber-Versicherung als „Retter in Not“?

Im Hinblick auf die Absicherung von Cyber-Risiken hat sich daher die Cyber-Versicherung in den Versicherungsbeständen von Unternehmen etabliert.

Die Cyber-Versicherung stellt dem Unternehmen im Notfall Spezialisten aus den Bereichen IT, Recht und PR zur Seite, die dem Management eine qualitativ hochwertige Unterstützung bieten. Dringende Fragen zu den Ursachen des Cyber-Vorfalls, ob und inwieweit der Manager Behörden, Betriebsangehörige, Kunden und Geschäftspartner informieren muss, und wie er den Schadensfall am besten in den Griff bekommt, werden zügig beantwortet. Dadurch wird vermieden, dass

beispielsweise die Anzeige eines Datenverlusts bei den zuständigen Behörden nicht ordnungsgemäß erfolgt oder dass durch mangelhafte Kundenkommunikation ein Reputationsschaden entsteht.

Das Notfallnetzwerk hat insbesondere im deutschen Mittelstand einen großen Anklang gefunden und ist sehr häufig auch der Hauptgrund für den Abschluss einer entsprechenden Versicherung. Entsprechende Netzwerke sind außerhalb der Versicherungslösung kaum oder nur zu sehr hohen Preisen erhältlich, die sogar die Versicherungsbeiträge übersteigen.

Die Cyber-Versicherung übernimmt neben den Kosten für die Wiederherstellung der Daten bzw. IT-Systeme auch die Ertragsausfälle durch die Cyber-Attacke. Dreh- und Angelpunkt der Cyber-Versicherung ist hier sehr häufig die Netzwerksicherheitsverletzung. Eine Netzwerksicherheitsverletzung wird überwiegend dann angenommen, wenn es einen Angriff (z.B. DDoS-Attacke) oder eine Zugangsverhinderung (z.B. Verschlüsselung der Systeme) auf Computersysteme gibt sowie ein Einschleusen oder die Weiterverbreitung von Schadenprogrammen vorliegt (z.B. Trojaner).

Ein weiteres Thema, das im deutschsprachigen Raum bis dato eine eher untergeordnete Rolle gespielt hat, in der Cyber-Versicherung aber immer relevanter wird, sind sog. Drittschäden. Über entsprechende Deckungsbausteine sind regelmäßig Haftpflichtansprüche von Betroffenen versichert, die aufgrund einer (vermuteten oder tatsächlich begangenen) Datenschutz-, Vertraulichkeits- oder Netzwerksicherheitsverletzung gegen das Unternehmen oder sogar einzelne Verantwortliche gerichtet werden.

Schaut man sich die aktuelle Situation im Cyber-Versicherungsmarkt und den deutlichen Schadenanstieg genauer an, sind Unternehmen nunmehr verstärkt in der Pflicht, das Schutzniveau für ihre IT-Infrastruktur deutlich anzuheben, wenn sie eine Cyber-Versicherung neu abschließen oder eine bestehende verlängern möchten. Der Risikotransfer mittels Cyber-Versicherung funktioniert seit geraumer Zeit nur noch bei gut aufgestellten Unternehmen. Er sollte daher keineswegs als Ersatz, sondern vorrangig als Ergänzung zu angemessenen IT-Sicherheitsmaßnahmen gesehen werden.

Ausblick

Die erhöhte Cyber-Kriminalität, der deutliche Anstieg an Cyber-Schäden und die erhöhten Haftungsrisiken für Manager machen deutlich: Manager kommen nicht mehr umhin, dem Thema IT-Sicherheit besondere Beachtung zu schenken. Unternehmensleiter müssen eine umfassende IT-Risikoorganisation mit einem breiten Spektrum an Maßnahmen zur Sicherstellung eines ordnungsgemäßen Betriebsablaufs aufbauen und fortentwickeln.

Das gilt auch dann, wenn Restrisiken auf eine Cyber-Versicherung transferiert werden sollen. Diese Option bietet sich immer häufiger nur noch den Unternehmensverantwortlichen an, die ihre Hausaufgaben in puncto IT-Sicherheit gemacht haben. ■