GMBH-GESCHÄFTS-FÜHRUNG 2021

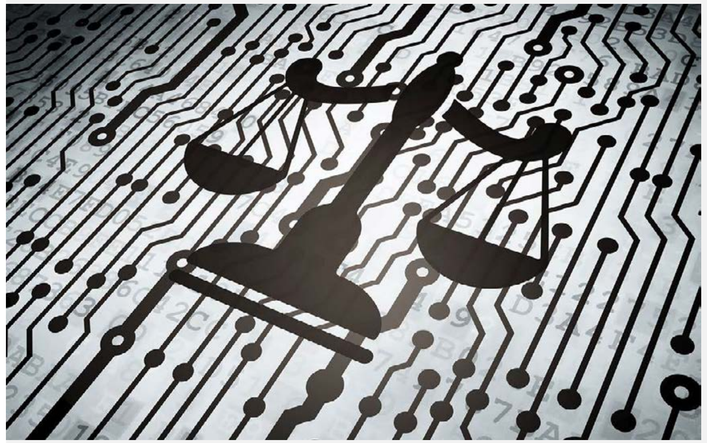
Fachbeitrag von Theodoros Bitis (Head of Cyber, Center of Excellence Howden)
im E-Book für die Geschäftsführung mit den haftungsträchtigen Themen dieser Zeit
– exklusiv und aktuell.

www.euroforum.de/geschaeftsfuehrer

euroforum

Herausforderungen für die Geschäftsleitung im Cyber-Zeitalter

Theodoros Bitis,
Head of Cyber, Center of Excellence,
Howden Deutschland



Cyber-Risiken haben sich in den vergangenen Jahren branchenübergreifend zu einem Top-Risiko für Unternehmen und Manager entwickelt. Versicherer berichten von jährlichen Vervielfachungen sowohl der Schadenhäufigkeit als auch der Schadenhöhe. In den nächsten Jahren wird damit gerechnet, dass ein Großteil aller Versicherungsverträge durch Cyber-Vorfälle schadenbelastet sein werden.

Proportional zur Cyber-Bedrohung sind auch die potenziellen Haftungsquellen für Manager gestiegen. Für sie wird es immer wichtiger, sich detailliert Gedanken über das unternehmensinterne Risikomanagement, die Bandbreite der Haftungsrisiken und den Transfer potentieller Restrisiken infolge von Angriffen auf die IT-Systeme zu machen.

Risikomanagement – mehr Schutzmaßnahmen sind nötig

Die verschärfte Bedrohungslage und der deutliche Anstieg an Cyber-Schäden machen deutlich, dass Unternehmen auf ihrer Agenda beim Tagesordnungspunkt Cyber-Risiken keinen schnellen Haken mehr setzen können. Die Komplexität der möglichen Cyber-Gefahren erfordert vielmehr ein ganzheitliches Risikomanagement, das zur Chefsache erklärt, mit einem adäquaten Budget ausgestattet und mit einer klaren Umsetzungsstrategie versehen wird.

Gaben sich vor nicht allzu langer Zeit Entscheiderinnen und Entscheider auf den Chefetagen noch mit Virenscannern, Firewalls und regelmäßigen Back-ups zufrieden, hat sich diese vermeintliche Sicherheit mittlerweile als gefährlicher Trugschluss entpuppt. Unternehmensleiterinnen und -leiter kommen heutzutage nicht daran vorbei, eine umfassende IT-Risikoorganisation mit einem breiten Spektrum an Maßnahmen zur Sicherstellung eines ordnungsgemäßen Betriebsablaufs aufzubauen und fortzuentwickeln. Unabdingbar sind dabei u.a. die Schaffung eines Richtlinienmanagements, Notfall- und Business-Continuity-Pläne, die Sicherheit mobiler Geräte, die Einführung einer Multifaktorauthentifizierung bei kritischen Anwendungen, eine Trennung von Admin- und sonstigen Benutzerkonten, erhöhte Schutzmaßnahmen im Bereich der OT sowie turnusmäßige Mitarbeiterschulungen. Hinzu kommt – zuletzt vor allem pandemiegetrieben – auch der Umgang mit „Bring-your-own-device“-Geräten.

Nicht weniger relevant ist auch der datenschutzrechtliche Aspekt einschließlich eines funktionierenden Incident-Management-Systems. Sind bei einem IT-Sicherheitsvorfall personenbezogene Daten betroffen, besteht nach Art. 33 DSGVO grundsätzlich eine Meldepflicht gegenüber den Datenschutzbehörden binnen 72 Stunden nach Kenntnisnahme. Die durch einen Sicherheitsvorfall betroffenen Kunden, Partner und Mitarbeiter sind nach Art. 34 DSGVO zu informieren, wenn voraussichtlich ein hohes Risiko für die Betroffenen besteht.

„Hafnium“-Vorfall macht Schwachstellen offenbar

Wie ernst zu nehmen das Thema ist, wurde im März 2021 durch den „Hafnium“-Vorfall deutlich, bei dem es um Schwachstellen bei Microsoft Exchange Servern ging. Selbst einige Wochen nach dem herausgegebenen Sicherheitsupdate hatte ein großer Teil der Unternehmen dieses nicht installiert, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) beklagte.

Weil kein automatisiertes Update möglich war, mussten die IT-Verantwortlichen selbst aktiv werden und auf Neudeutsch „patchen“. Kriminelle hätten so über einen längeren Zeitraum hinweg die Möglichkeit gehabt, unter Ausnutzung der Schwachstelle Zugriff auf E-Mail-Konten auf den betroffenen Servern zu erhalten.

Wenn solch ein Fall nachweislich eintritt, gehen die Datenschutzbehörden grundsätzlich von einem meldepflichtigen Vorfall nach Art. 33 DSGVO aus.

Einige Datenschutzbehörden gehen sogar noch weiter und sehen eine Meldepflicht bereits durch ein nicht rechtzeitiges Update als begründet an. Von einer Meldung kann demnach lediglich dann abgesehen werden, wenn Verantwortliche bereits nach den Handlungsempfehlungen des BSI geprüft haben, ob die Sicherheitslücke ausgenutzt wurde, und keine Kompromittierung festgestellt haben.

Verbreitung von Ransomware-Attacken steigt

Mit durchgeführten Sicherheitsupdates und der gegebenenfalls nötigen Meldung bei der Datenschutzbehörde sind die Unternehmen allerdings noch nicht in jedem Fall aus dem Schneider. Unter Ausnutzung von Schwachstellen in der IT-Sicherheit versuchen Kriminelle seit geraumer Zeit, Verschlüsselungssoftware in Unternehmen einzuschleusen. Diese sogenannten „Ransomware“-Attacken führen zu einer automatisierten Verschlüsselung der Daten, so dass diese für die betroffenen Unternehmen nicht mehr nutzbar sind. Für die Entschlüsselung verlangen die kriminellen Gruppierungen mittlerweile sehr hohe Lösegeldsummen.

Sind die Täter auch an sensible Daten herangekommen, kommt es vereinzelt zu einer zusätzlichen Erpressung verbunden mit der Drohung, die gestohlenen Daten zu veröffentlichen. Diese Vorgehensweise ist unter der Bezeichnung „DoppelPaymer Ransomware“ bekannt geworden und hat nach erstmaligem Auftreten in 2019 eine starke Verbreitung in 2020 gefunden.

Ransomware-Attacken haben mittlerweile auch in Deutschland zugenommen – hohe Aufmerksamkeit erlangte etwa der Angriff auf das Uniklinikum Düsseldorf im Herbst 2020 – und sie haben sehr häufig Schäden in Millionenhöhe angerichtet. Neben den hohen Lösegeldforderungen entstehen bei den Unternehmen immense Schäden durch die Betriebsunterbrechung sowie hohe Kosten für die Forensik, IT-Wiederherstellung und die Aufrechterhaltung des Geschäftsbetriebs.

Die Cyberversicherung als Teil des Risikomanagements

Angesichts der verschärften Risikolage durch Cyber-Angriffe in den letzten Jahren hat sich die Cyber-Versicherung auch bei den deutschen Unternehmen vom „nice to have“ zum Pflichtprogramm entwickelt. Ausschnittslösungen über andere Versicherungssparten haben sich nicht als qualitativ tragfähig erwiesen.

Die Cyber-Versicherung übernimmt im Regelfall neben den finanziellen Folgen, die den Unternehmen durch Störung des Betriebsablaufs aufgrund einer Cyber-Attacke oder interne Systemausfälle entstehen, die Kosten für forensische und rechtliche Aufarbeitung des Vorfalls, die Wiederherstellung der IT-Systeme, Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebes, Haftpflichtansprüche Dritter und die Krisenkommunikation.

Besonders für mittelständische Unternehmen interessant: Über die Cyber-Versicherung steht den Unternehmen in vielen Fällen bei einem Notfall auch ein Netzwerk von hochspezialisierten Forensikern, Rechtsanwälten und PR-Beratern zur Seite. Diese Dienstleistungen sind in der Versicherungsprämie mit eingepreist und damit schneller und kostengünstiger als separat im freien Markt erhältlich.

Managerhaftung in Zusammenhang mit IT-Sicherheitsvorfällen

Manager tragen die Verantwortung für die ordnungsgemäße Unternehmensführung, und dazu gehört auch ein funktionierendes IT-Risikomanagement. Erweisen sich die darin festgelegten Maßnahmen vor und während eines IT-Sicherheitsvorfalls als lückenhaft, wird schnell der Vorwurf eines Organisationsverschuldens laut. Bei schuldhaften Versäumnissen können dann die Manager auf Ersatz eines Vermögensschadens in Anspruch genommen werden.

Es springt dann die D&O-Versicherung ein, die nicht nur bei Ansprüchen der eigenen Gesellschaft (Innenhaftung), sondern auch bei Drittansprüchen (Außenhaftung) greift.

Der D&O-Versicherer bietet zunächst Deckung für die Verteidigung der in Anspruch genommenen Manager gegen die im Raum stehenden Vorwürfe von Pflichtversäumnissen. Oft sind dann langwierige Rechtsstreitigkeiten vorprogrammiert, die häufig in einem Vergleich mit einem geringen Bruchteil der Gesamtschadenssumme resultieren. Bei IT-Sicherheitsvorfällen geht es aber primär um schnelle Abhilfe. Jegliche Verzögerungen können ein Unternehmen in seinem Bestand gefährden. Ein langes Zuwarten auf die Schadenregulierung ist hier – anders als in anderen D&O-Schadenangelegenheiten – nicht möglich.

Ausblick

Zahlreiche Schadenfälle aus jüngerer Vergangenheit machen deutlich, dass Manager nicht mehr umhinkommen, ein speziell auf die Bedürfnisse des Unternehmens abgestimmtes IT-Risikomanagement einzurichten, es kontinuierlich aufrechtzuerhalten und bei Bedarf den neuen Gegebenheiten anzupassen. Immer mehr Manager nehmen die Cyber-Bedrohung sehr ernst und gehen die notwendigen Schritte an, um sich bestmöglich für die Zukunft auszurüsten. Der Bedeutung einer maßgeschneiderten Transferlösung für Cyber-Risiken sind sich viele mittlerweile sehr bewusst.

Gleichzeitig haben Versicherer – forciert durch die Versicherungsaufsicht und die Rückversicherer – in den letzten Jahren angefangen, die Risiken neu zu bewerten und Kunden einen transparenten Überblick über versicherte Cyber-Risiken zu geben. Einige Versicherer sprechen hier seit Neuestem von „affirmativen“ Lösungen, d.h. ausdrücklicher Versicherungsschutz oder ausdrücklicher Ausschluss in den anderen Versicherungspolicen. Die Folgen dieser Neubewertung werden dann auch für die Manager sehr häufig gravierend sein: Zahlreiche D&O-Versicherungspolicen werden zukünftig mit Vollausschlüssen für Cyber-Risiken in der D&O-Versicherung versehen. Spätestens dann führt an einer umfassenden Cyber-Versicherung kein Weg mehr vorbei. ■