IT-Sicherheit ist Chefsache. Bei der Abwehr von Cyberkriminalität sind Unternehmensleiter in der Pflicht

Cyberangriffe sind in aller Munde. Nicht nur auf den Ausgang der US-amerikanischen Präsidentschaftswahl sollen Hacker Einfluss genommen haben. Auch Unternehmen sehen sich erheblichen Bedrohungen durch Cyberangriffe ausgesetzt. So wurde der Onlineriese Yahoo gleich mehrfach Opfer derartiger Attacken. Dem Softwareunternehmen Adobe Systems wurden 38 Millionen Kundendatensätze gestohlen, unter anderem Kreditkarteninformationen. Doch auch kleine und mittlere Unternehmen sind vor Hackerangriffen nicht gefeit.

Im Gegenteil, laut einer Untersuchung des Security-Herstellers Symantec konzentriert sich über ein Drittel der kriminellen Cyberaktivitäten auf Unternehmen mit weniger als 250 Angestellten. Mittlerweile sind bereits 69% der deutschen Industrieunternehmen Opfer von Cyberangriffen geworden. Hierdurch entstehen Schäden, die vom Digitalverband Bitkom auf über 50 Milliarden Euro jährlich taxiert werden. Die Bundesregierung hob Ende 2016 im Jahr ihrer „Cyber-Sicherheitsstrategie für 2016“ hervor, dass Cybersicherheit ein gemeinsamer Auftrag von Staat und Wirtschaft sei.

Im Zuge ihrer Raubzüge greifen Hacker zu verschiedenen Methoden. Besonders beliebt ist die Infiltrierung des Zielunternehmens mit Schadsoftware, sogenannter Malware. Ebenso zu nennen ist das berüchtigte Phishing, also die Erlangung vertraulicher Unternehmensdaten durch gefälschte Websites oder E-Mails. Neben der Verwendung und dem Weiterverkauf der auf diese Weise erbeuteten Daten kommt es oftmals auch zu Erpressungen. Hier hat eine Reihe von Krankenhäusern Lehrgeld zahlen müssen. Die für die Attacke verantwortlichen Hacker oder Dritte drohen, erlangte Informationen zu veröffentlichen, falls das betroffene Unternehmen nicht einen bestimmten Betrag zahlt. Alternativ legen Hackemit sogenannter „Ransomware“ die IT-Infrastruktur eines Unternehmens lahm oder sperren Teile der Software oder Daten. Erst wenn das Unternehmen ein „Lösegeld“ gezahlt hat, erlangt es wieder vollständigen Zugriff auf sein IT-System.

Im Folgenden soll dargestellt werden, welche Pflichten die Prävention derartiger Cyberangriffe für die Unternehmensleitung mit sich bringt und welche Folgen sich aus entsprechenden Pflichtverletzungen ergeben können.

Anforderungen an die Unternehmensleitung

Für die Betreiber kritischer Infrastrukturen gilt das IT-Sicherheitsgesetz, wonach effektive Sicherheitsmaßnahmen zu etablieren sind. Auch Unternehmen außerhalb dieses Adressatenkreises müssen sich angesichts der zuvor geschilderten Lage um das Thema IT-Security kümmern und ein funktionsfähiges IT-Risikomanagement etablieren. Hierfür trägt in erster Linie die Geschäftsleitung die Verantwortung. Es lässt sich festhalten: IT-Sicherheit ist Chefsache.

Aus haftungsrechtlicher Sicht sind – abhängig von der für das Unternehmen gewählten Rechtsform – verschiedene Rechtsgrundlagen einschlägig, um die Sorgfaltspflichten der Geschäftsleitung zu bestimmen. Relevant ist etwa § 91 Abs. 2 AktG, der für Aktiengesellschaften und über § 278 Abs. 3 AktG auch für Kommanditgesellschaften auf Aktien gilt und vorsieht, dass der Vorstand geeignete Maßnahmen zu treffen hat, um den Fortbestand der Gesellschaft gefährdende Entwicklungen früh zu erkennen. Trotz fehlender vergleichbarer Regelung im GmbHG prägen die Grundsätze zu § 91 Abs. 2 AktG in entsprechender Anwendung auch die Sorgfaltspflicht des Geschäftsführers einer Gesellschaft mit beschränkter Haftung (§ 43 Abs. 1 GmbHG).

Autoren: Simon J. Heetkamp und Dr. Michael Rath

Unternehmen sind heutzutage beinahe ausnahmslos auf Informationstechnik angewiesen. Demnach sind unerkannte oder nicht adäquat mitigierte Risiken im IT-Bereich in der Lage, das Schicksal des betroffenen Unternehmens in erheblicher Weise negativ zu beeinflussen und damit den Fortbestand der Gesellschaft zu gefährden. Für viele Unternehmen stellen die digital abgelegten Kundendaten oder elektronisch gespeichertes fachliches Know-how die entscheidenden Vermögenswerte dar. Sollte ein Hacker mit seiner Attacke gegen ein Unternehmen erfolgreich sein, droht dem Unternehmen (neben dem Verlust der „Kronjuwelen“) auch ein Reputationsverlust, der sich spürbar auf die wirtschaftlichen Kennzahlen des Unternehmens auswirken kann.

Die Brisanz gerade der Angriffsszenarien auf vernetzte Gebäudetechnik wird in den nächsten Jahren mit Internet of Things kontinuierlich zunehmen und geht über Angriffe auf die Systeme zur Immobilienverwaltung weit hinaus. Die Aufzählung lässt sich leicht fortsetzen, zeigt aber deutlich wie zahlreich die Angriffspunkte und wie wirtschaftlich brisant die Auswirkungen sein können.

Grundsätze der IT-Sicherheitspolitik eines Unternehmens

Durch die immense Bedeutung der Informationstechnik für Unternehmen wird das Bedürfnis nach einer praktischen Konkretisierung der Handlungsanforderungen und Haftungsvoraussetzungen – auch im Interesse der Geschäftsleitung – umso dringlicher. Denn der Passus der zu ergreifenden „geeigneten Maßnahmen“ vermag aus sich heraus keine belastbaren Leitlinien vorzugeben. Ein Blick in die Rechtsprechung bringt noch keine belastbaren Erkenntnisse. Denn Fälle, in denen ein geschädigtes Unternehmen sich nach einem Cyberangriff (erfolgreich) mit einem Schadensersatzbegehren an seine Geschäftsleitung gewandt hat, sind noch nicht entschieden worden. Damit kann die Frage der Haftung der Geschäftsleitung nur anhand der folgenden Erwägungen beantwortet werden. Bei der Beurteilung der zu ergreifenden Maßnahmen kann man sich an den Best Practices der regulierten Industrien orientieren. So ist beispielsweise durch die Bundesnetzagentur für die Energieversorger die Einrichtung und Zertifizierung eines Informationsmanagementsystems nach ISO 27001 obligatorisch. Hieran sollten sich auch nicht regulierte Industrien und Unternehmen orientieren.

Nach den Vorgaben der Business Judgement Rule kann ein Gericht (trotz dieser Best Practices) lediglich überprüfen, ob der Vorstand oder der Geschäftsführer im Rahmen des ihm zuzubilligenden Ermessens gehandelt hat. Grundsätzlich liegt damit die Beurteilung der Eignung der ergriffenen Maßnahmen zum Schutz der IT-Sicherheit im Ermessen der Geschäftsleitung. Nur wenn diese ersichtlich nicht ausreichend waren, kommt eine Haftung der Geschäftsleitung in Betracht. Die Anforderungen an ein Risikomanagement müssen nun auf die konkrete IT-spezifische Fragestellung zugeschnitten werden, um beurteilen zu können, ob die Geschäftsleitung im Rahmen ihres Ermessens gehandelt hat. Orientieren können sich Unternehmen an Regelwerken wie den IT-Grundschutzkatalogen des BSI und dem bereits angeführten ISO 27001, die sich mit der Implementierung geeigneter Sicherheitsmechanismen befassen.

Bestandsaufnahme als Ausgangspunkt

Um angemessene IT-Sicherheitsmaßnahmen ergreifenzu können, ist als Erstes eine Erfassung und Bewertung des informationstechnischen Bestands des Unternehmens erforderlich. So stellen sich etwa Fragen nach der verwendeten Hard- und Software, nach der Struktur der Informationstechnik, insbesondere im Hinblick auf die Vernetzung und die Abhängigkeit einzelner Unternehmensbereiche voneinander, aber auch organisatorsche Aspekte wie etwa Kontrollen. Hinzu kommen bestehende rechtliche Verpflichtungen, die sich etwa aus datenschutzrechtlichen Vorschriten ergeben können.

IT-Sicherheit ist Chefsache. Bei der Abwehr von Cyberkriminalität sind Unternehmensleiter in der Pflicht

Wurde ein umfassendes Bild des Status quo gezeichnet, ist im nächsten Schritt zu prüfen, welche Risiken sich für das Unternehmen aus dem IT-Bestand ergeben. Damit einher geht eine Beurteilung der negativen Auswirkungen im Fall des Eintritts der identifizierten Risiken.

Bestimmung von Schutzmaßnahmen

Aus der Bestandsaufnahme sollen wiederum belastbare Aussagen darüber entwickelt werden, welchen Risiken auf welche Weise und in welchem Umfang zu begegnen ist. Es müssen also die Maßnahmen bestimmt werden, die aus vernünftiger Sicht zu treffen sind, um den Eintritt von IT-Risiken, wozu auch Angriffe durch Hacker zählen, zu verhindern. Zu diesen Maßnahmen zählen stets technische Vorkehrungen zur Abwehr äußerer Bedrohungen, allen voran Virenschutz und Firewall. Jedoch dürfen auch physische Schutzmechanismen gegen Brand, Diebstahl und ähnliche Risiken nicht vernachlässigt werden. Daneben treten Maßnahmen zur Vorbeugung menschlicher Fehler durch Schulung der Mitarbeiter und IT-spezifische Beaufsichtigung der Anwender.

Zur Abwendung einer unmittelbar drohenden Realisierung eines Schadens durch einen laufenden oder gerade erfolgten Cyberangriff muss zudem ein Notfallkonzept erarbeitet werden. Teil eines solchen Notfallkonzepts könnte ein Wiederanlaufplan für ein gekapertes IT-System oder die Schaffung einer redundanten IT-Infrastruktur sein, die im Fall eines Hackerangriffs die unternehmenswichtigen IT-Funktionen übernimmt und auf regelmäßig gesicherte Datenbestände (Back-ups) zugreifen kann. Hier bieten die ISO-Standards gute Hilfestellung bei der Etablierung der passenden Managementsysteme.

Fortlaufende Überwachung und Verbesserung

Die beschriebenen Anforderungen können freilich in vielen Fällen nicht allein von der Unternehmensleitung erfüllt werden. Vielmehr hat sie die einzelnen Aufgaben ordnungsgemäß an fachkundige Personen zu delegieren (etwa einen IT-Sicherheitsbeauftragten), diese zu instruieren und anschließend ausreichend zu überwachen. Genügt sie diesen Vorgaben, trifft sie kein Organisationsverschulden, und eine persönliche Verantwortung wäre ausgeschlossen. Um eine eigene Haftung auszuschließen, müssten Geschäftsleiter zudem ein engmaschiges Berichtswesen etablieren. Dieses hat sicherzustellen, dass (neue) IT-Risiken und mögliche Verbesserungen in der IT-Sicherheit an die Geschäftsleitung kommuniziert werden. Des Weiteren hat die Geschäftsleitung dafür zu sorgen, dass dem Thema IT-Sicherheit angemessene finanzielle, personelle und zeitliche Ressourcen gewidmet werden. Um eine stete Verbesserung der IT-Sicherheit zu gewährleisten, sollten regelmäßige Wirksamkeitsüberprüfungen (wie Penetrationstests) und die Auswertung von erfolgten Cyberangriffen durchgeführt werden.

Haftung der Geschäftsleitung

Kommt ein Geschäftsleiter seiner Pflicht, ein derartiges funktionierendes IT-Sicherheitsmanagementsystem einzurichten, nicht nach, sieht er sich im Schadensfall Ansprüchen der Gesellschaft ausgesetzt. Dies ergibt sich für Gesellschaften, auf die das Aktiengesetz Anwendung findet, aus § 93 Abs. 2 Satz 1 AktG und für solche, für die das GmbH-Gesetz gilt, aus § 43 Abs. 2 GmbHG. Dabei ist aus prozessualer Sicht auf die den Geschäftsleiter treffende Darlegungs- und Beweislast hinzuweisen. Geschäftsleiter müssen entsprechend darlegen und beweisen, dass sie – freilich aus Ex-ante-Sicht – taugliche Maßnahmen getroffen, also die erforderliche Sorgfalt beachtet haben oder dass sie kein Verschulden trifft. Für den Vorstand einer AG ergibt sich dies aus § 93 Abs. 2 Satz 2 AktG, dieser gilt für den Geschäftsführer einer GmbH – trotz fehlender vergleichbarer Regelungen im GmbHG– entsprechend. Daher ist den Geschäftsleitern zu einer umfassenden Dokumentation der Risikoanalyse und der ergriffenen Maßnahmen zu raten.

Die Inanspruchnahme des verantwortlichen Geschäftsleiters ist für ein durch einen Cyberangriff geschädigtes Unternehmen eine überlegenswerte Handlungsoption zur Abmilderung des entstandenen

Autoren: Simon J. Heetkamp und Dr. Michael Rath

Schadens – insbesondere, wenn für die Mitglieder der Geschäftsleitung – wie so häufig – eine D&O-Versicherung abgeschossen wurde. Besteht in der Gesellschaft ein Aufsichtsrat, der die Gschäftsleitung zu überwachen hat, ist dieser in der Regel sogar verpflichtet, bestehende Regressansprüche gegen das verantwortliche Geschäftsleitungsmitglied zu verfolgen.

FAZIT

Die Unternehmensleitung trifft die Verantwortung, für eine hinreichende Wehrhaftigkeit des Unternehmens gegen Cyberattacken zu sorgen. Konkret ist damit die Aufgabe gemeint, ein funktionierendes IT-Risiko- und -Sicherheitsmanagement einzurichten, um die Angriffsmöglichkeiten für Hacker auf ein Minimum zu reduzieren. Ziele sind hierbei das Identifizieren potentieller Gefahrenquellen sowie die Ergreifung geeigneter Gegenmaßnahmen. Hervorzuheben ist, dass die IT-Sicherheit ein fortlaufendes Tätigwerden des Geschäftsleiters erfordert. Denn das IT-Sicherheitsmanagement setzt nicht nur voraus, dass Sicherheitsmaßnahmen entwickelt, implementiert und durchgeführt werden. Vielmehr müssen sie stetig überwacht, überprüft und verbessert werden. Wurde diesen Pflichten nicht genügt und hatte eine Cyberattacke deshalb Erfolg, kann die Geschäftsleitung hierfür haftbar gemacht werden ■

Quellenhinweis

Der Beitrag „IT-Sicherheit ist Chefsache. Bei der Abwehr von Cyberkriminalität sind Unternehmensleiter in der Pflicht“ ist in der Ausgabe 04/2017 des Deutscher AnwaltSpiegel erschienen.

http://www.deutscheranwaltspiegel.de/impressum/

Die Autoren

Simon J. Heetkamp

ist Rechtsanwalt und Associate der Luther Rechtsanwaltsgesellschaft mbH in Köln.

Dr. Michael Rath

ist Rechtsanwalt und Partner der Luther Rechtsanwaltsgesellschaft GmbH in Köln.