MYRA

EXPERTENINTERVIEW

Managerhaftung bei IT-Sicherheitsvorfällen

MYRA
Neue digitale Sicherheit

Managerhaftung bei IT-Sicherheitsvorfällen

Das unterschätzte persönliche Risiko für deutsche Geschäftsführer und wie man es minimiert

Wir leben in Zeiten einer zunehmenden Digitalisierung von Gesellschaft, Wirtschaft und Verwaltung. Vor allem Unternehmen sehen sich einer wachsenden Zahl von Cyberangriffen ausgesetzt. Das Allianz Risk Barometer 2022 listet Cybervorfälle als das größte Geschäftsrisiko für Unternehmen weltweit. Neun von zehn Firmen haben im vergangenen Jahr Schäden durch Cyberattacken erlitten. Der Bitkom beziffert die Schadenshöhe allein für Deutschland auf 223 Milliarden Euro.

Auch der Gesetzgeber hat diese Entwicklung zur Kenntnis genommen und mit immer strengeren Anforderungen an IT-Sicherheit und Datenschutz darauf reagiert. Diese reichen von allgemeingültigen Sicherheitsvorgaben, wie sie beispielsweise in der Neuauflage des IT-Sicherheitsgesetzes (IT-SiG 2.0) formuliert sind, bis hin zu branchenspezifischen Auflagen, beispielsweise für Unternehmen aus dem Banken- oder Versicherungssektor. In allen Fällen verlangt die Umsetzung dieser Vorgaben zur IT-Sicherheit den Unternehmen umfassend auditierte Prozesse sowie den Einsatz von zertifizierten Anbietern und Technologien ab.

Maßnahmen zum Schutz der IT- und Datensicherheit werden in der Praxis sowohl durch die Angreifer als auch durch die jeweiligen Aufsichtsbehörden auf die Probe gestellt: Der Gesetzgeber verlangt Instrumente zur Verhinderung sowie zum Umgang mit Cyberangriffen. IT-Sicherheit sollte daher ganz oben auf der Prioritätenliste der Geschäftsleitung stehen. Denn das deutsche Haftungsrecht setzt Manager hierzulande zunehmend unter Druck. Das Risiko, für Fehlverhalten – auch und insbesondere im Bereich IT-Sicherheit – in Anspruch genommen zu werden, ist in den vergangenen Jahren erheblich gestiegen.

Daniel Laws, Rechtsanwalt bei der Baker Tilly Rechtsanwaltsgesellschaft mbH erläutert im Gespräch mit Myra Security, welche Risiken im Haftungsrecht in Deutschland für Manager bestehen, welche Haftungsregeln aktuell gelten, welche gesetzgeberischen Entwicklungen in der nahen Zukunft zu erwarten sind und wie Manager sich am besten gegen dieses Haftungsrisiko wappnen.

Daniel Laws
Partner Baker Tilly

Daniel Laws absolvierte sein Studium der Rechtswissenschaften an der Universität Mannheim sowie an der Universidad de Alicante, Spanien. Vor seiner Zeit bei Baker Tilly arbeitete er als Rechtsanwalt bei einer mittelständischen Sozietät von Rechtsanwälten/Steuerberatern im Rhein-Neckar-Kreis.

Seine Tätigkeitsschwerpunkte bei Baker Tilly umfassen die Gebiete Gesellschaftsrecht und Umstrukturierungen, Venture Capital, M&A sowie Handels- und Vertriebsrecht.

Welches Risiko gehen Manager in Deutschland ein, wenn sie das Thema IT-Sicherheit vernachlässigen?
Daniel Laws: Im Fall eines Cyberangriffs drohen Unternehmen hohe finanzielle Schäden, etwa durch Umsatzausfälle, zusätzlich entstehende Kosten, durch Geldbußen und eine Inanspruchnahme durch Dritte.

Um sich (weitestgehend) schadlos zu halten, können bzw. müssen Unternehmen die ihnen durch den Cyberangriff entstandenen Schäden gegenüber dem jeweiligen Führungsorgan geltend machen. Dieses Führungsorgan kann also persönlich für die Schäden haftbar gemacht werden, welche der Gesellschaft durch den Cyberangriff entstanden sind. Denn Geschäftsführer und Vorstandsmitglieder sind verpflichtet, sich stets gesetzestreu zu verhalten und die jeweilige Gesellschaft vor Schäden zu bewahren. Außerdem haben sie aktiv dafür zu sorgen und zu kontrollieren, dass Angehörige des Unternehmens geltendes Recht einhalten. Bei einem Verstoß gegen diese Pflichten

kommt ein Schadensersatzanspruch der Gesellschaft gegen das jeweilige Organmitglied, auch noch nach dessen Ausscheiden aus dem Unternehmen, in Betracht. Es droht also eine persönliche Haftung in erheblicher Höhe.

Bei der Vernachlässigung des Themas IT-Sicherheit, dessen Bedeutung stetig wächst, drohen den Angehörigen der Geschäftsführungsorgane (Geschäftsführer, Vorstände) daher insbesondere erhebliche, gegebenenfalls sogar existenzgefährdende zivilrechtliche Konsequenzen.

Auch sind Bußgelder gegen derartige Organmitglieder zumindest nicht auszuschließen, etwa wenn durch den Cyberangriff gegen Datenschutzvorschriften verstoßen wurde. In einem derartigen Fall droht im schlimmsten Fall in strafrechtlicher Hinsicht auch eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe.

Wer genau droht auf Ebene der Gesellschaft in Anspruch genommen zu werden?
Daniel Laws: Personen, denen die Geschäftsführung obliegt, wie etwa Mitglieder des Vorstands einer Aktiengesellschaft sowie Geschäftsführer einer GmbH, haften bei Verstoß gegen die mit der Geschäftsführung einhergehenden Pflichten. Aber auch eine Haftung der Mitglieder des Aufsichtsrats kommt in Betracht, wenn diese ihrer Pflicht zur Überwachung der Geschäftsführung nicht nachkommen.

Was sind die wesentlichen Anknüpfungspunkte für eine Haftung?
Daniel Laws: Für den Vorstand einer Aktiengesellschaft regelt das Aktienrecht (§ 91 Absatz 2 AktG), dass dieser geeignete Maßnahmen zu treffen und insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Norm ist grundsätzlich auch auf die Geschäftsführer bzw. Vorstände anderer Gesellschaftsformen anzuwenden. Die Pflicht zur Einrichtung eines Überwachungssystems bezieht sich auch auf Maßnahmen zur Sicherstellung der IT-Sicherheit und Vermeidung bzw. Minimierung von Cyberrisiken. Hinzu kommen spezialgesetzliche Normen (etwa Art. 32 DSGVO oder § 165 TKG), die speziell der Vermeidung von Cyberrisiken dienen.

Eine Haftung droht immer dann, wenn das jeweilige Leitungsorgan diese Pflichten verletzt. Für den Fall, dass Leitungsorgane ihre Pflichten gegenüber der Gesellschaft verletzen, sehen insbesondere die § 93 Absatz 2 S. 1 (i.V.m. § 116) AktG bzw. § 43 Absatz 2 GmbHG vor, dass das jeweilige Mitglied des Leitungsorgans der Gesellschaft für entstandene Schäden haftet. Kommt es dann zu einem Schaden der Gesellschaft, liegt daher ein Regress der Gesellschaft bei dem jeweiligen Organmitglied nahe.

> ***Das Thema IT-Sicherheit betrifft jedes Unternehmen, und zwar in steigendem Maße, je mehr der wirtschaftliche Erfolg des Unternehmens von der Sicherheit der IT-Systeme abhängig ist.***

Sind je nach Unternehmensgröße unterschiedliche Maßstäbe anzulegen?
Daniel Laws: Grundsätzlich ist richtig, dass für große Unternehmen teilweise strengere Regelungen gelten (vgl. §§ 2 Absatz 14 Nr. 1, 8f BSIG) und auch in der Zukunft gelten sollen (vgl. hierzu den Vorschlag der geplanten EU-Richtlinie zur Aufhebung der EU-Richtlinie 2016/1148 vom 6. Juli 2016, NIS). Verschärfte Regelungen knüpfen etwa auch an kritische Funktionen oder Produkte des Unternehmens an.

Allerdings ist die Notwendigkeit der Einführung eines Systems zur Vermeidung und zum Umgang mit Cyberangriffen nicht auf große Unternehmen beschränkt. Das Thema IT-Sicherheit betrifft stattdessen jedes Unternehmen, und zwar zum einen in steigendem Maße, je mehr der wirtschaftliche Erfolg des Unternehmens von der Sicherheit der IT-Systeme abhängig ist. Es versteht sich von selbst, dass z. B. Unternehmen im Bereich E-Commerce stärker auf den Schutz ihrer IT-Systeme angewiesen sind als „analoge“ Unternehmen wie beispielsweise Bäckereien, Bauunternehmen oder Büchereien. Daneben hat der Gesetzgeber bestimmt, dass auch Unternehmen, die für die Allgemeinheit essenziell sind, strengere Regeln im Bereich der IT-Sicherheit beachten müssen, etwa im Bereich kritischer Infrastrukturen (KRITIS). Jedes Leitungsorgan sollte daher – schon aus eigenem Interesse zur Vermeidung

einer persönlichen Haftung – für die Implementierung ausreichender, auf das Risikoprofil seines Unternehmens zugeschnittener Vorkehrungen sorgen.

> ***„Auch bei einer wirksamen Übertragung der Aufgaben der IT-Sicherheit auf eines der Mitglieder des Organs, bleiben die übrigen Mitglieder weiterhin zur angemessenen Überwachung verpflichtet."***

Kann eine Haftung innerhalb des Leitungsorgans verlagert oder auf einen Dritten abgewälzt werden?
Daniel Laws: Die Einhaltung des Legalitätsprinzips (also die Pflicht zur Einhaltung der geltenden Rechtsnormen) fällt in die Gesamtverantwortung von Geschäftsführung bzw. des Vorstandes als Gesamtorgan. Allerdings können Aufgaben – und damit auch die Pflichten im Zusammenhang mit IT-Sicherheit – grundsätzlich auf einzelne Mitglieder dieser Organe verlagert werden. Auch eine Verlagerung an Fachpersonal oder sowie an externe IT-Dienstleister ist möglich und wegen deren regelmäßig höherer Expertise häufig auch unverzichtbar. Denn regelmäßig fehlt den Mitgliedern der Geschäftsführung die eigene Expertise, den durch Cyberangriffen drohenden Risiken nur mit „Bordmitteln" adäquat zu begegnen. Bei wirksamer Übertragung und ordnungsgemäßer Durchführung können so Kenntnisse effektiv genutzt und Zuständigkeiten sinnvoll geschaffen werden.

Hierbei ist jedoch sorgfältig vorzugehen, denn eine Haftungsfreizeichnung kann nicht ohne Weiteres erreicht werden: Zum einen ist eine Übertragung auf einzelne Mitglieder des Organs immer nur insoweit möglich, wie nicht eine Zuständigkeit des Gesamtorgans im Sinne aller seiner Mitglieder gegeben ist. Auch bei einer wirksamen Übertragung, der Aufgaben der IT-Sicherheit auf eines der Mitglieder des Organs, bleiben die übrigen Mitglieder weiterhin zur angemessenen Überwachung verpflichtet. Das heißt, dass z. B. auch der eigentlich für den Vertrieb zuständige Geschäftsführer sich nicht ohne Weiteres darauf verlassen darf, dass der für den Bereich IT zuständige Geschäftsführer seinen Pflichten nachkommt. Stattdessen sollte er beispielsweise regelmäßig Rücksprache mit diesem halten und, wenn ihm Missstände im Bereich IT-Sicherheit bekannt werden, auch reagieren. Auf einen Dritten dürfen zudem nur solche Aufgaben übertragen werden, die nicht in den Kernbereich der Aufgaben des Organs fallen. Auch hier bestehen im Falle einer Übertragung etwa Pflichten zur Instruktion und Überwachung bzw. zu regelmäßiger Abstimmung.

Gibt es unterschiedliche Haftungsregeln in den verschiedenen Branchen, zum Beispiel Finance oder KRITIS?
Daniel Laws: Für bestimmte Branchen gelten Sonderregelungen zur IT-Sicherheit. Dies gilt insbesondere für solche Bereiche, die für die Infrastruktur als besonders erheblich angesehen werden, wie zum Beispiel im Bereich kritischer Infrastrukturen (KRITIS) oder im Bereich Finance.

Im Bereich kritischer Infrastrukturen (KRITIS) gilt § 8a BSIG, der die jeweiligen Betreiber dazu verpflichtet, angemessene Vorkehrungen zur Vermeidung von Störungen zu treffen. Betreiber in diesem Sinne ist, wer Verfügungsgewalt über die jeweilige Anlage oder Einrichtung ausübt. In der Regel ist daher die Gesellschaft, welche die jeweilige Anlage oder Einrichtung unterhält, Betreiberin.

Kritische Infrastrukturen sind solche aus Bereichen der Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Abfallentsorgung, sofern sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. In erster Linie stellen daher solche Dienstleister eine Kritische Infrastruktur im Sinne des Gesetzes dar, wenn sie für die Versorgung und das Zusammenleben der Bevölkerung von maßgeblicher Bedeutung sind. Selbstverständlich sind die Unternehmen in den aufgeführten Bereichen im Bereich IT-Sicherheit nicht alle gleichermaßen schutzbedürftig. Durch eine Rechtsverordnung, also durch Normen, die in diesem Fall das Bundesinnenministerium erlässt, werden die kritischen Infrastrukturen daher noch genauer bestimmt. Auch Anbieter digitaler Dienste oder Unternehmen in besonderem öffentlichen Interesse treffen nach dem BSIG besondere Pflichten im Bereich IT-Sicherheit.

Nach § 8a Absatz 1a BSIG sind die Betreiber kritischer Infrastrukturen ab dem 1. Mai 2023 zudem dazu verpflichtet, Systeme zur Angriffserkennung einzusetzen. Diese sollen auch in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Eine derartige Bedrohung stellen insbesondere Angriffe durch DDoS-Attacken (Distributed-Denial-of-Service) dar. Hierbei wird durch mehrere Systeme ein Angriff auf Dienste, Webseiten, einzelne Systeme oder ganze Netze ausgeführt. Das betroffene Ziel ist dadurch wegen seiner Überlastung nicht mehr verfügbar.

Die jeweiligen Betreiber bzw. Anbieter können diesen Pflichten häufig nur mit erheblicher externer fachlicher Unterstützung nachkommen. Bei der Auswahl externer Dienstleister bietet das Bundesamt für Sicherheit in der Informationstechnik (auf Grundlage des § 3 Absatz 3 BSIG) Unterstützung. Auf seiner Website veröffentlicht es Listen qualifizierter Sicherheitsdienstleister, etwa solcher zur Abwehr von DDoS-Angriffen.

Im Bereich Finance gelten darüber hinaus etwa Pflichten zur Aufstellung eines Risikomanagements, auch betreffend IT-Systeme (§ 25a Absatz 1 S. 3 Nr. 5 KWG), sowie die Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) durch Rundschreiben, etwa die Mindestanforderungen an das Risikomanagement (MaRisk), nebst Bankenaufsichtliche Anforderungen an die IT (BAIT).

> ***Die Gesetzgebung wird stetig an die immer neuen und komplexer werdenden Herausforderungen im Bereich IT-Sicherheit angepasst.***

Welche gesetzgeberischen Entwicklungen sind im Bereich der IT-Sicherheit zu erwarten?
Daniel Laws: Festzuhalten ist zunächst, dass die Gesetzgebung im Bereich IT-Sicherheit stetig an die immer neuen und komplexer werdenden Herausforderungen im Bereich IT-Sicherheit angepasst wird (etwa durch das neue IT-Sicherheitsgesetz 2.0 vom 18. Mai 2021). Die Entwicklung in diesem Bereich ist daher dauerhaft im Auge zu behalten.

Eine wesentliche Entwicklung, die hier insbesondere zu beobachten ist, ist das Vorhaben der EU, die EU-Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS) aufzuheben und durch eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 2) zu ersetzen. Durch diese Richtlinie sollen insbesondere Maßnahmen zum Cybersicherheitsrisikomanagement und Meldepflichten bei einem Sicherheitsvorfall festgelegt werden. Als Richtlinie würden diese Bestimmungen zwar grundsätzlich nicht unmittelbar Geltung finden. Allerdings ist (aktuell) vorgesehen, dass die Richtline innerhalb von 24 Monaten nach ihrem Inkrafttreten durch die Mitgliedstaaten umzusetzen ist. Beispiele aus anderen Bereichen der EU-Rechtsetzung, wie z. B. zur Vermeidung der Geldwäsche und Terrorismusfinanzierung, zeigen, dass Unternehmen hier häufig sehr umfangreiche Beobachtung und Präventionsobliegenheiten auferlegt werden und bei Verstößen hohe Ordnungsgelder drohen.

Die Zahl der registrierten Cybervorfälle nimmt beständig zu. Was können Manager in Deutschland konkret tun, um sich vor einer persönlichen Inanspruchnahme in Zusammenhang mit Cyberkriminalität wirksam zu schützen?
Daniel Laws: Für eine Inanspruchnahme eines Organmitglieds durch die Gesellschaft aufgrund eines Cyberangriffs ist insbesondere erforderlich, dass (i) auf Ebene der Gesellschaft ein Schaden entstanden ist und (ii) das Organmitglied nicht vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln (sog. Business Judgement Rule).

Eine Haftung kann daher vermieden werden, wenn ein für die Bedürfnisse des Unternehmens adäquates Sicherheitssystem geschaffen wird. Hierbei können folgende drei Stufen identifiziert werden: Auf einer ersten Stufe (1.) hat das geschäftsführende Organ (stets) die unternehmensspezifischen Risiken im Bereich IT und Cyberkriminalität zu identifizieren. Diese unternehmensspezifischen Risiken hängen jeweils vom konkreten Geschäftsmodell des Unternehmens ab. Sodann (2.) sind Vorkehrungen zu treffen, um die

identifizierten Risiken zu minimieren und einem Cyberangriff vorzubeugen bzw. diesen abwehren zu können. Außerdem (3.) sind Maßnahmen vorzusehen, um einen möglichen und trotz ausreichender Abwehrmaßnahmen dennoch stattgefundenen Cyberangriff zu melden und den Schaden so zu minimieren. Teilweise handelt es sich hierbei um gesetzliche Meldepflichten. Eine Meldung empfiehlt sich jedoch häufig auch, um Schadensersatzansprüche durch Vertragspartner oder sonstige Dritte zu vermeiden oder möglichst gering zu halten.

Darüber hinaus können Mitglieder der geschäftsführenden Organe oder des Aufsichtsrates eine persönliche Inanspruchnahme durch den Abschluss einer D&O-(Directors & Officers-) Versicherung jedenfalls minimieren. Insbesondere aufgrund von Durchsetzungsrisiken und wegen eines möglichen Reputationsverlusts für das Unternehmen sowie einer teilweise verbleibenden Eigenbeteiligung bietet dies jedoch keinen Ersatz für ein funktionierendes Sicherheitssystem.

Auch der Abschluss einer Cyberversicherung ist möglich. Je nach Ausgestaltung können etwa Mehrkosten im Falle eines Cyberangriffs für dessen Beseitigung sowie unter Umständen auch die Kosten einer Betriebsunterbrechung sowie für Rechtsberatung gedeckt sein. Allerdings ist auch die Cyberversicherung nur neben einem Sicherheitssystem zu empfehlen, da auch hier häufig kein umfassender Schutz (etwa hinsichtlich vertraglicher Sekundäransprüche) gegeben ist.

Gibt es (in Deutschland oder weltweit) bereits Urteile gegen Manager im Zusammenhang mit Cyberangriffen?
Daniel Laws: Soweit ersichtlich, sind noch keine derartigen Urteile in Deutschland ergangen. Allerdings ist nicht auszuschließen, dass derartige Verfahren bereits geführt und, etwa durch einen Vergleich, von der Öffentlichkeit abgeschirmt beendet wurden.

In den USA nimmt die Inanspruchnahme von Managern sowie ihrer Versicherungen im Zusammenhang mit Cyberangriffen dagegen zu. Auch die Bedeutung eines IT-Sicherheitssystems wird hierdurch nochmals verdeutlicht: So konnte sich etwa das Management der Baumarktkette Home Depot durch den Nachweis derartiger Maßnahmen exkulpieren und dadurch eine persönliche Haftung abwehren.

Glossar

AktG	Das deutsche Aktiengesetz regelt die Errichtung, die Verfassung, Rechnungslegung, Hauptversammlungen und Liquidation von Aktiengesellschaften sowie von Kommanditgesellschaften auf Aktien. Darüber hinaus ist das deutsche Konzernrecht im Aktiengesetz geregelt.
TKG	Das Telekommunikationsgesetz ist ein deutsches Bundesgesetz, welches Regelungen im Bereich der Telekommunikation und Telekommunikationsinfrastrukturen trifft, um dadurch den Wettbewerb in diesem Bereich zu regulieren und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.
GmbHG	Ist das Gesetz, in dem Regelungen über die Gesellschaft mit beschränkter Haftung (GmbH) enthalten sind. Es regelt im Wesentlichen die Errichtung und das Erlöschen der GmbH sowie die Rechtsverhältnisse der Gesellschaft und der Gesellschafter.
BSIG	Das deutsche BSI-Gesetz enthält Regelungen insbesondere in Bezug auf die Aufgaben des Bundesamts für Sicherheit in der Informationstechnik.
KWG	Zweck des Kreditwesengesetzes ist die Marktregulierung und Marktordnung des Kreditwesens. Das KWG gilt unter anderem für Kreditinstitute und Finanzdienstleistungsinstitute. Das KWG dient insbesondere der Sicherung und Erhaltung der Funktionsfähigkeit der Kreditwirtschaft.
NIS2	Die EU NIS-Richtlinie ist aktuell der europäische Rahmen für Cyber Security im Bereich Kritischer Infrastrukturen. Die EU-Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union reguliert Cyber Security bei Betreibern in EU-Sektoren, die neue EU NIS2 wird Sektoren und Cybersecurity-Pflichten deutlich erweitern.
i.V.m.	Ist die Abkürzung für „in Verbindung mit“, welche hauptsächlich in den Rechtswissenschaften bei Vergleichen und Hinweisen auf mehrere Paragraphen oder Absätze, die miteinander in Zusammenhang stehen, Verwendung findet.