Cybersecurity als Unternehmensleitungsaufgabe – Neue Aspekte der Organhaftung

Sarah Schmidt-Versteyl

Angriffe auf die Cybersecurity von Unternehmen sowohl der Privat- als auch – und vor allem – der öffentlichen Wirtschaft führen zu Schäden in Höhe von vielen Milliarden pro Jahr. So schätzte der Branchenverband Bitkom, dass Attacken auf die deutsche Industrie 102,9 Milliarden Euro Schaden jährlich verursachen.[1]

Dieses Schadenspotential führt zu einer erheblichen Steigerung des Haftungsrisikos des Managements. Die Grundsätze der Organhaftung sind seit über 20 Jahren in der Rechtsprechung etabliert. Im Jahr 1997 hat der Bundesgerichtshof im Grundsatzurteil „ARAG/Garmenbeck"[2] festgestellt, dass Ansprüchen gegen die Organe des Unternehmens nachzugehen ist, soweit ein Schaden des Unternehmens auf einer Handlung oder Unterlassung des Organs beruht. Das in Anspruch genommene Organ trifft die Beweislast, dass die jeweilige Handlung oder Unterlassung nicht pflichtwidrig war. Es bedarf wenig Phantasie, um Schäden aufgrund von Angriffen auf die Cybersicherheit eines Unternehmens auf Handlungen oder Unterlassungen des Managements zurückzuführen, da ein Cyberangriff regelmäßig eine technische oder menschliche Sicherheitslücke im Unternehmen braucht, um erfolgreich zu sein. Der Entlastungsnachweis, dass hier keine Pflichtwidrigkeit zugrundeliegt, ist denkbar schwierig. Das Ergebnis ist ein sehr hohes Haftungsrisiko für die Geschäftsleitung von Unternehmen.

Das hohe Haftungsrisiko zeigt sich auch an den gestiegenen Compliance-Anforderungen. Seit mehreren Jahren gelten etablierte Grundsätze im Hinblick auf die erforderliche Compliance-Organisation im Unternehmen. 2013 hat das Landgericht München I im sogenannten „Siemens/Neubürger"-Urteil[3] dargelegt, dass die Unternehmensleitung in ihrem Ver-

1 Bitkom.de, Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr (abgerufen am 2.3.2021).

2 BGH NJW 1997, 1926.

3 LG München I NZG 2014, 345.

antwortungsbereich geeignete organisatorische Maßnahmen für ein gesetzestreues Verhalten nachgeordneter Unternehmensangehöriger festlegen muss. Der Weg zur haftungsrelevanten Cyber-Compliance ist damit bereitet.

Im Folgenden wird dargestellt, welche rechtlichen Fragestellungen damit verbunden sind und was die Beratungspraxis erwartet.* Häufig ist dem Management die Haftungsrelevanz von Cybersicherheit noch nicht bewusst, auch wenn Studien immer wieder zu dem Ergebnis kommen, dass Unternehmen kaum ein Risiko höher bewerten als Cyberrisiken.[4] Mit Blick auf die potenziell enormen Schadenssummen ist dies änderungsbedürftig.

Zwar gibt es auch in Deutschland seit einigen Jahren Cyber-Versicherungen, allerdings haben entsprechende Versicherungsprodukte bisher weder den Markt vollständig durchdrungen[5] noch spiegeln die vereinbarten Deckungssummen das veröffentlichte Schadensrisiko hinreichend wider.

Es stellt sich damit die Frage, wer letztlich für die ganzen Schäden bezahlt. Angesichts des Themas des Bandes und der Tagung – Cybersecurity als Unternehmensleitungsaufgabe –, ist naheliegend, in welche Richtung die Antwort gehen kann. Wir sehen uns im Folgenden an, welches Haftungsrisiko ein Unternehmen trägt (I.), ob dafür die Unternehmensleitung in Regress genommen werden kann (II.) und welche rechtlichen Mechanismen gegebenenfalls vor der Haftung schützen können (III.).

I. Haftungsrisiko des Unternehmens

Wie kommt ein Cyberangriff letztlich in die Beratungspraxis? Typischerweise ist es so, dass ein Mitglieds der Geschäftsführung anruft und berichtet, dass es im Unternehmen eine Systemverschlüsselung gegeben habe, die Computer „tot" seien und damit die Auftragsannahme, die Auftragsabwicklung und die Logistik nicht mehr funktioniere. Die Systeme seien her-

---

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag basiert, ist abrufbar unter https://doi.org/10.17176/20210315-161242-0.

4 Allianz.com, Allianz Risiko Barometer 2021, https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021-de.html (abgerufen am 2.3.2021).

5 Laut einer Studie des Digitalverbands Bitkom zum Wirtschaftsschutz in der deutschen Industrie aus dem Jahr 2020 haben 17 Prozent aller Unternehmen eine Cyberversicherung abgeschlossen, vgl. https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-vernetzten-Welt.

untergefahren, Mitarbeiter nach Hause geschickt worden und eventuell liegt auch schon eine Lösegeldforderung vor. In der Regel hat das Unternehmen bereits technische Experten beauftragt, die dann neben der Forschung nach der Ursache auch Beweise sichern. Anschließend muss das Unternehmen seinen Informationspflichten nachkommen.[6] Sind KRITIS-Unternehmen[7] betroffen, geht es um die Meldung des Cybervorfalls an das BSI[8]. Weitere Informationspflichten bestehen nach der DS-GVO, die gemäß Art. 33 DS-GVO verlangt, dass binnen 72 Stunden eine Meldung zu machen ist, soweit durch den Angriff auch personenbezogene Daten abgeflossen sind. Zudem ist bei börsennotierten Unternehmen gegebenenfalls der Kapitalmarkt zu informieren und auch Versicherer sind unverzüglich einzubinden.

Allein diese unmittelbaren Kosten des Unternehmens infolge eines Cyberangriffs summieren sich gemäß einer aktuellen Studie von IBM aus dem Jahr 2020 auf einen durchschnittlichen Schaden für das betroffene Unternehmen von etwa 4 Mio. US-Dollar.[9]

Nicht im Blick haben die Unternehmen in der Regel, dass über diese unternehmensinternen Kosten auch Schadensersatzansprüche auf sie zukommen können. Solche können Vertragspartnern entstehen, wenn das betroffene Unternehmen seinen vertraglichen Pflichten etwa wegen einer Betriebsunterbrechung nicht mehr nachkommen kann. Dazu gehören Ansprüche aus Liefer- oder Abnahmeverzug oder Vertragsstrafen. Als Opfer einer Cyberattacke haftet das Unternehmen gleichwohl nach dem allgemeinen Grundsatz aus § 280 BGB, wenn das Unternehmen sich von der Verschuldensvermutung aus § 280 Abs. 1 S. 2 BGB nicht entlasten kann.

Noch gibt es keine Rechtsprechung zu Sorgfaltspflichten im Hinblick auf eine ordnungsgemäße Organisation zur Vermeidung von Cyberangriffen.[10] Gemäß der Rechtsprechung des Bundesgerichtshofs muss das Unternehmen dafür sorgen, dass es seinen Schutzpflichten gegenüber den Vertragspartnern nachkommt, so dass diesen kein Schaden entsteht: Der im Verkehr erforderlichen Sorgfalt ist genügt, wenn Sicherheitsvorkehrun-

---

6 Vgl. dazu *Brüggemeier*, in diesem Band.

7 Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

8 Bundesamt für Sicherheit in der Informationstechnik.

9 Bericht „Kosten einer Datenschutzverletzung", 2020 von IBM Security und dem Ponemon Institut, https://www.ibm.com/de-de/security/data-breach.

10 S. dazu *Spindler*, in diesem Band, D.

gen getroffen werden, die ein „*verständiger, umsichtiger, vorsichtiger und gewissenhafter Angehöriger des betroffenen Berufskreises für ausreichend halten darf, um andere Personen vor Schäden zu bewahren, und die den Umständen nach zuzumuten sind*".[11]

In diesem Zusammenhang stellt sich die Frage, ob das Unternehmen sich vom Verschuldensvorwurf wegen mangelhafter Sicherheitsvorkehrungen überhaupt entlasten kann, wenn das Unternehmen kein aktuelles Betriebssystem nutzt. Relevant wurde dies etwa bei den Angriffen mit der Malware *WannaCry* im Jahr 2017. Diese Schadsoftware nutzte eine Sicherheitslücke im Betriebssystem Windows XP, das vom Hersteller aus dem Programm genommen und nicht mehr mit Sicherheitsupdates versehen worden ist. Trotzdem war dieses Betriebssystem immer noch auf dem Markt verbreitet, weswegen sich *WannaCry* so rasant verbreiten konnte.[12] Ob diese Nutzung ohne Durchführung von Sicherheitsupdates fahrlässig ist, ist bisher nicht gerichtlich festgestellt. Anknüpfend an allgemeine Maßstäbe ist es wohl notwendig, dass die IT-Sicherheitsstruktur im Unternehmen grundsätzlich so angepasst ist, dass sie keine Schäden Dritter verursacht. Auf der anderen Seite war Windows XP offenbar insbesondere im öffentlichen Sektor noch stark verbreitet, z.B. in Krankenhäusern. Diese tragen nicht nur die finanzielle Herausforderung, ihre IT-Sicherheit auf dem aktuellen Stand zu halten, sondern auch die logistische Herausforderung ihre Betriebssysteme laufend zu aktualisieren. Ob hier die laufende Aktualisierung der IT-Sicherheit im Einzelfall „*den Umständen nach zumutbar ist*", ist zu bezweifeln.

Eine weitere ungeklärte Frage im Hinblick auf das Verschulden des Unternehmens im Fall von Schadensersatzansprüchen ist, ob das Unternehmen haftet, wenn ein Cyberangriff dadurch ermöglicht wird, dass ein Mitarbeiter eine E-Mail mit einem virusbehafteten Anhang öffnet. Grundsätzlich muss sich das Unternehmen das Verschulden seiner Mitarbeiter bei einer Schadensverursachung im Rahmen vertraglicher Beziehungen gemäß § 278 BGB zurechnen lassen. Ob ein Verschulden in diesen Fällen vorliegt, ist abhängig vom Einzelfall. Inzwischen sind die Angriffe subtiler und virenbehaftete Dateien weniger einfach zu erkennen, so dass die Verschuldensfrage im jeweiligen Einzelfall geklärt werden muss.

---

11 BGH r+s 2014, 96, 97.

12 Spiegel-Redaktion, "WannaCry"-Attacke – Fakten zum globalen Cyberangriff (Stand: 13.05.2017), https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html (abgerufen am 08.02.2021).

Weitere gegen das betroffene Unternehmen gerichtete Schadensersatzansprüche können sich aus Verstößen gegen die DS-GVO ergeben. Gemäß Art. 82 DS-GVO kann derjenige, dessen personenbezogenen Daten abhandengekommen sind, Schadensersatz geltend machen. Ein Pflichtverstoß liegt bereits dann vor, wenn ein unbeabsichtigter Datenverlust eintritt, also das Unternehmen Daten beispielsweise nach einem Cyberangriff verliert. Hinzugekommen ist, dass nach DS-GVO auch immaterielle Schäden zu ersetzen sind. Neu ist auch, dass das Unternehmen sich nur sehr schwer entlasten kann. Es gilt nicht nur der allgemeine aus dem BGB bekannte Grundsatz, dass sich das Unternehmen gegebenenfalls für seinen Mitarbeiter exkulpieren kann (vgl. § 831 Abs. 1 S. 2 BGB). Vielmehr ist danach ein Entlastungsnachweis nur dann möglich, wenn der Verantwortliche oder der Auftragsverarbeiter in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 Abs. 3 DS-GVO). „In keinerlei Hinsicht" ist offenbar noch einmal eine Erhöhung des Entlastungsnachweises. Zwar gilt nach DS-GVO, dass eine Zertifizierung von der Haftung befreien oder sie reduzieren kann (Art. 83 Abs. 2 lit. j DS-GVO), was aber ausdrücklich kein automatischer Haftungsausschluss ist. Allerdings sind die bisher mit Schadensersatzansprüchen befassten erstinstanzlichen Gerichte eher restriktiv. Nach der Rechtsprechung reicht das Vorliegen eines Pflichtverstoßes allein nicht aus, einen Schadensersatzanspruch zu begründen. Tatsächlich muss der Antragsteller zudem einen kausal verursachten Schaden durch den Datenabfluss darlegen, woran viele Klagen gescheitert sind.[13]

Weiter drohen nach der DS-GVO hohe Bußgelder, soweit dem Unternehmen personenbezogene Daten abhandengekommen sind. Es ist bereits viel diskutiert worden, dass der Bußgeldrahmen für deutsche Verhältnisse extrem hoch ist. Wenn ein Unternehmen nach einem Cyberangriff seinen Meldepflichten nicht rechtzeitig nachgekommen ist, kann ein Bußgeld bis zu EUR 10,0 Mio. oder bis zu 2 % des weltweit erzielten Jahresumsatzes erhoben werden (Art. 83 Abs. 4 lit. a DS-GVO). Bei schwerwiegenderen Verstößen, beispielsweise wenn das Unternehmen selbst bei der Verarbeitung personenbezogener Daten Fehler gemacht hat, kann das Bußgeld bis zu EUR 20,0 Mio. oder bis zu 4 % des weltweit erzielten Jahresumsatzes betragen (Art. 83 Abs. 5 lit. a DS-GVO). Nach bisheriger Erfahrung handhaben

13 OLG Dresden NJW-RR 2020, 426 Rn. 22; OLG Dresden ZD 2019, 567 Rn. 12 f.; LG Feldkirch BeckRS 2019, 18276 Rn. 67 ff.; vgl. zu den Anforderungen an die Kausalität: *Wybitul/Haß/Albrecht*, NJW 2018, 113, 115 f.; *Krämer*, NJW 2020, 497, 502; *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021, Art. 82 Rn. 11; speziell zu Cyberattacken: *Schmitt/Suschinski/Heil*, ZIP 2019, 2092, 2094.

die Aufsichtsbehörden die Meldefrist von 72 Stunden relativ großzügig, jedenfalls wenn sich das Unternehmen innerhalb dieser Frist bei der Aufsichtsbehörde meldet und den Cybervorfall als solchen mitteilt. Welche Daten im Einzelnen abgeflossen sind, kann dann nach entsprechender Aufarbeitung nachgemeldet werden.

Nachdem anfangs spekuliert wurde, ob die Aufsichtsbehörden den rechtlichen Bußgeldrahmen überhaupt ausschöpfen würden, hat sich dies inzwischen geklärt: europaweit sind erhebliche Bußgelder verhängt worden. In Deutschland traf das höchste Bußgeld in Höhe von EUR 14,5 Mio. den Immobilienkonzern *Deutsche Wohnen*.[14] Allerdings wurde das Bußgeldverfahren kürzlich durch das Berliner Landgericht eingestellt; die Staatsanwaltschaft legte dagegen Beschwerde ein.[15] Im europäischen Ausland sind noch höhere Bußgelder verhängt worden. *Marriott International* wurde anfänglich ein Bußgeld in Höhe von EUR 107 Mio., wegen des Verlustes von Kundendaten infolge unzureichend gesicherter Computersysteme, auferlegt. Dieses wurde aber auf umgerechnet EUR 21 Mio. herabgesetzt.[16] *British Airways* ist zunächst mit EUR 204 Mio. Strafe belegt worden. Aber auch in diesem Fall erfolgte inzwischen eine deutliche Reduzierung, da sich der Umsatz der Fluglinie coronabedingt deutlich verschlechtert hat.[17] Dieser Trend liegt sicher auch an der Entwicklung in den USA. Dort sind aktuell eine Reihe von Aktionärsklagen im Nachgang zu Datenschutzverletzungen durch Cyberangriffe anhängig. Regelmäßig werden die Geschäftsleitungsorgane in diese Klagen einbezogen. Diese Fälle sind überwiegend noch nicht entschieden. Bekannt ist der Vergleich von Aktio-

14 *LTO-Redaktion*, Deutsche Wohnen soll Millionen-Bußgeld zahlen (Stand: 6.11.2019), https://www.lto.de/recht/kanzleien-unternehmen/k/dsgvo-verstoss-deutsche-wohnen-bussgeld-datenschutz-berlin/ (abgerufen am 08.02.2021).

15 *Haufe Online Redaktion*, DSGVO-Bußgeld gegen Deutsche Wohnen ist nicht vom Tisch (Stand: 04.03.2021), https://www.haufe.de/immobilien/wirtschaft-politik/deutsche-wohnen-wehrt-sich-gegen-bussgeld-wegen-dsgvo-verstoss_84342_503486.html (abgerufen am 09.03.2021).

16 *ICO*, ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure (Stand: 30.10.2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/ (abgerufen am 08.02.2021).

17 *ICO*, ICO fines British Airways £20m for data breach affecting more than 400,000 customers (Stand: 16.10.2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/ (abgerufen am 08.02.2021).

nären mit *Yahoo*, bzw. dem D&O-Versicherer, über USD 29 Mio.[18] Eine weitere, aktuell anhängige Klage betrifft *Capital One*. Die amerikanische Bank ist 2019 Opfer eines großen Hackerangriffs geworden, bei dem über 100 Millionen Bankdaten abhandengekommen sind. Auch hier ist die Geschäftsleitung in die Klage einbezogen worden.[19]

In dem Zusammenhang ist zu erwähnen, dass auch das IT-Sicherheitsgesetz 2.0, welches seit 2019 in der Diskussion ist, einen erweiterten Bußgeldrahmen haben wird. Der am 16.12.2020 beschlossene Regierungsentwurf sieht vor, dass der Bußgeldrahmen des BSI-Gesetzes, der bisher am OWiG orientiert war, an den der DS-GVO angeglichen wird (§ 14 BSIG-E). Gleichzeitig wird der Anwendungsbereich deutlich erweitert, indem weitere Branchen und Sektoren einbezogen werden. So gilt das Gesetz künftig auch für Unternehmen, die der Gesetzgeber als „Unternehmen im besonderen öffentlichen Interesse" bezeichnet (§ 2 Abs. 14 BSIG-E). Dabei handelt es sich um Unternehmen der Rüstungsindustrie, Produzenten von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen, Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und Unternehmen, die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung sind. Das Haftungsrisiko für Unternehmen aus Cyberangriffen in Anspruch genommen zu werden, ist also künftig auch von dieser Seite hoch.

1. Haftungsreduzierung kaum möglich

In der Praxis kann ein Unternehmen dieses Risiko dadurch kaum minimieren, dass es vertraglich Haftungsbeschränkungen mit seinen Vertragspartnern vereinbart. Im Regelfall werden standardisierte Verträge verwendet, so dass AGB-Recht anwendbar ist. In AGB können Haftungsbeschränkungen für Cyberrisiken kaum wirksam vereinbart werden. Die Rechtsprechung verlangt vom Verwender von AGB das Einstehen für vorhersehbare

18 *LaCroix*, Yahoo Data Breach-Related Derivative Suit Settled for $29 Million (Stand: 21.01.2029), https://www.dandodiary.com/2019/01/articles/cyber-liability/yahoo-data-breach-related-derivative-suit-settled-29-million/ (abgerufen am 08.02.2021).

19 *LaCroix*, Data Breach-Related Securities Suit Filed Against Capital One (Stand: 03.10.2019), https://www.dandodiary.com/2019/10/articles/securities-litigation/data-breach-related-securities-suit-filed-against-capital-one/ (abgerufen am 08.02.2021).

Schadensfolgen im Rahmen der wesentlichen Vertragspflichten.[20] Vertrauliche Behandlung von Kundendaten oder Einhaltung von Lieferpflichten gehören zu wesentlichen Vertragspflichten. Folglich können lediglich auf individualvertraglicher Basis Beschränkungen für fahrlässige Verstöße vereinbart werden.

2. Überwälzung des Schadens auf Dritte

Somit stellt sich die Frage, wie das Unternehmen den mit einem Cyberangriff verbundenen Schaden weitergeben kann. Der Cyberkriminelle selbst ist in den meisten Fällen kaum haftbar zu machen. Selbst wenn man ihn identifizieren und gerichtlich in Anspruch nehmen könnte, wird es in der Regel kaum möglich sein, gegen den Cyberkriminellen zu vollstrecken.

Es gibt allerdings eine Ausnahme in den Fällen des sog. *CEO-Frauds*. Hier werden durch Cyberkriminelle gefälschte Identitäten, in der Regel des Unternehmenschefs, aufgebaut. Regelmäßig wird vorgetäuscht, dass E-Mails vom hierarchisch weit entfernten „Chef" stammen. Auf diese Weise werden Mitarbeiter getäuscht, die Anweisungen des vermeintlichen Chefs ausführen und Gelder tatsächlich an Cyberkriminelle weiterzuleiten. In diesen Fällen ist es manchmal sogar möglich, der Spur des Geldes zu folgen und die Angreifer zu identifizieren, wenn gegebenenfalls betroffene Drittländer Rechtshilfe gewähren.

In den statistisch häufigsten Fällen werden Unternehmen allerdings durch Schadsoftware geschädigt, die zur Datenverschlüsselung führt (sog. Ransomware). Insofern stellt sich die Frage nach der Inanspruchnahme des Herstellers der betroffenen Software, da die Schadsoftware regelmäßig eine Sicherheitslücke im System nutzt, um sich auszubreiten. Diese Frage stellte sich insbesondere bei dem *WannaCry*-Virus. Hier hieß es jedenfalls zunächst, dass sich der Virus über das Betriebssystem Windows XP verbreitete, für das der Hersteller bis zum Bekanntwerden des Virus keine Sicherheitsupdates mehr vorgesehen hatte.[21] Zwar besteht eine Produktbeobachtungspflicht des Herstellers. Ob diese soweit führt, dass der Herstel-

20 BGH NJW 1985, 3016, 3018; BGH NJW-RR 1993, 560, 561; BGH NJW 2002, 673, 675.

21 Spiegel-Redaktion, "WannaCry"-Attacke – Fakten zum globalen Cyberangriff (Stand: 13.05.2017), https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html (abgerufen am 08.02.2021).

ler sogar verpflichtet ist, Updates bereitzustellen, obwohl er das Produkt ausdrücklich nicht mehr unterstützt, ist offen.[22]

Auch der Verkäufer haftet in der Praxis nur selten für Cybervorfälle. Cyberangriffe, die auf Sicherheitslücken beruhen, betreffen in der Regel ältere Systeme. Die Sicherheitslücken werden häufig erst nach dem Verkauf als solche erkennbar. In dem Fall dürfte sich der Verkäufer entlasten können, wenn zum Zeitpunkt der Herstellung die Systeme dem Stand der Technik entsprachen.[23]

Es ist zu prüfen, ob der eigene IT-Dienstleister in Anspruch genommen werden kann. Hier lohnt sich – idealerweise präventiv – die Prüfung der vertraglichen Leistungspflichten und die Ausgestaltung der Haftung. In der Praxis scheitert eine Inanspruchnahme häufig an der mangelnden Vereinbarung solcher vertraglicher Leistungspflichten, der wirtschaftlichen Durchsetzbarkeit der hohen Schadensersatzansprüche oder einer hinreichenden Versicherungsdeckung des IT-Dienstleisters.

In der Regel ist es ebenfalls nicht sinnvoll, den Mitarbeiter, der durch eine Handlung die Ausbreitung des Virus und den damit verbundenen Schaden verursacht hat, in Anspruch zu nehmen. Jedenfalls wenn nur Fahrlässigkeit des Mitarbeiters vorliegt, greifen die Grundsätze des innerbetrieblichen Schadensausgleiches ein, so dass die Haftung bereits rechtlich auf wenige Monatsgehälter beschränkt ist.[24] Selbst wenn der Mitarbeiter grob fahrlässig oder sogar vorsätzlich gehandelt hat und damit keine rechtliche Haftungsbeschränkung greift, ist regelmäßig ein Schaden, der mehrere Millionen beträgt, wirtschaftlich gegenüber dem Mitarbeiter nicht durchsetzbar. In diesem Bereich gibt es allerdings eine Ausnahme in der Rechtsprechung, die interessanterweise auch wieder einen *CEO-Fraud* betrifft: So hat das Sächsische Landesarbeitsgericht mit Urteil vom 13.06.2017 entschieden, dass eine Mitarbeiterin, die gefälschte E-Mails

---

22 Nach *Raue*, NJW 2017, 1841, 1845, ist eine Updateverpflichtung für den Hersteller so lange zumutbar, wie er das Produkt vertreibt und ihn vertragliche Gewährleistungsrechte dazu verpflichten. Dement-sprechend muss der Hersteller die Nutzer jedenfalls noch zwei Jahre nachdem letzten Verkauf der Soft-ware mit Sicherheitsupdates versorgen. Allerdings kann auch nach diesem Zeitpunkt eine Produktbe-obachtungspflicht bestehen, wenn die Software weiterhin stark verbreitet ist, diese beschränkt sich dann aber in der Regel auf Warnungen; *Wiesemann/Mattheis/Wende*, MMR 2020, 139, 140; *Wiebe*, NJW 2019, 625, 630; *Schrader/Engstler*, MMR 2018, 356, 359 f.; *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, 2007, Rn. 135.

23 *Wiebe*, NJW 2019, 625, 627; *Schrader/Engstler*, MMR 2018, 356, 357 f.; *Raue*, NJW 2017, 1841, 1843.

24 Vgl. BAG NZA 1994, 1083, 1085 ff.

nicht als solche erkannt hat und dadurch dem Unternehmen einen Schaden von EUR 400.000 zugefügt hat, EUR 150.000 ersetzen musste.[25] Das Gericht nahm eine Schadensteilung an, da grobe Fahrlässigkeit der leitenden Mitarbeiterin vorgelegen habe und sich das Unternehmen gleichzeitig nicht vernünftig organisiert habe.

II. Haftungsrahmen der Geschäftsleitung für Cybersecurity

So kommen wir zu der eigentlichen Frage, ob die Geschäftsleitung für Schäden in Regress genommen werden kann. Dafür spricht, dass es etablierte Rechtsprechung gibt, nach der Schadensersatzansprüche gegen die Geschäftsleitungsorgane grundsätzlich zu verfolgen sind.[26] In der Praxis ist es für Organe schwierig, sich gegen Ansprüche zu verteidigen, wenn das Unternehmen, das einen Schaden erlitten hat, dargelegt hat, dass für den Schaden eine Handlung oder Unterlassung der Geschäftsleitung ursächlich war. In dem Fall muss das betroffene Organ sein pflichtgemäßes Handeln darlegen oder dass der Schaden auch bei rechtmäßigen, pflichtgemäßen Alternativverhalten eingetreten wäre.[27] Die Anforderungen sind recht hoch, gerade im Hinblick auf Cyberangriffe, die nur erfolgreich sein können, wenn natürliche oder technische Sicherheitslücken im Unternehmen vorhanden sind. Es gibt speziell zur Organhaftung bei Cyberattacken noch keine Rechtsprechung, dies dürfte aber nur eine Frage der Zeit sein. Hierfür spricht auch, dass die D&O-Versicherungsbedingungen, die – anders als Cyber-Versicherungen – flächendeckend vorhanden sind, Vermögensschäden aufgrund von Cyberangriffen noch nicht ausgeschlossen haben.

1. Haftungsmaßstab

Die anzuwendenden Grundsätze der langjährig geltenden Maßstäbe für Organhaftung sind bekannt: Ausgehend vom allgemeinen Haftungsmaßstab in § 93 Abs. 1 AktG und – vergleichbar – in § 43 Abs. 1 GmbHG haben die Organmitglieder bei ihrer Geschäftsführung die Sorgfalt eines or-

25 LAG Sachsen BeckRS 2017, 127707.
26 St. Rspr., Grundsatzurteil: BGH NJW 1997, 1926 – ARAG-Garmenbeck, zuletzt: BGH NJW 2019, 596; BGH NJW 2018, 3574; BGH ZIP 2014, 1728.
27 BGH NZG 2018, 1189 Rn. 38 ff.

dentlichen und gewissenhaften Geschäftsleiters anzuwenden. Der Pflichtenrahmen der Geschäftsleitung bestimmt sich einerseits nach dem Gesetz. Gesetzesverstöße des Unternehmens, die auftreten, weil die Geschäftsleitung das Unternehmen nicht richtig organisiert hat, führen ohne Weiteres zu einem haftungsrelevanten Pflichtverstoß. Ausdrücklich hat das LG München I im bekannten Siemens/Neubürger-Urteil entschieden, dass die Mitglieder der Geschäftsleitung zur eigenen Haftungsvermeidung für eine Unternehmensorganisation sorgen müssen, die Gesetzesverletzungen verhindert.[28] Insofern ist an die vielen Spezialgesetze zu denken, die eine angemessen geschützte IT-Infrastruktur vorschreiben. Dazu gehören etwa Art. 32 DS-GVO, wonach Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, verpflichtet sind, die zum Schutz der Daten „*angemessenen technischen und organisatorischen Maßnahmen*" zu treffen oder § 109 TKG, wonach jeder Telekommunikationsdiensteanbieter die erforderlichen technischen Schutzmaßnahmen zu treffen hat oder § 13 Abs. 7 TMG für Diensteanbieter im Bereich der Telemedien. Für die Betreiber so genannter Kritischer Infrastrukturen gilt gemäß § 8a BSIG, dass sie „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme*" vorsehen. Kritische Infrastrukturen sind gemäß § 2 Abs. 10 BSIG unter anderem Unternehmen der Energie-, IT-, Telekommunikations-, Finanz- oder Versicherungswirtschaft. Für den Bankensektor gibt es entsprechende Spezialregelungen wie § 25a Abs. 1 Nr. 5 KWG.[29]

Soweit keine Spezialgesetze einschlägig sind, hat der Geschäftsleiter entsprechend dem spezifischen *Risk Exposures* seines Unternehmens angemessene Maßnahmen zu ergreifen. Hier gibt § 91 Abs. 2 AktG den Rahmen vor, wonach eine Pflicht der Geschäftsleitung als Gesamtgremium besteht, für ordnungsgemäßes Risikomanagement eben auch im Hinblick auf die IT-Sicherheit zu sorgen. Die eingangs genannten Untersuchungen zeigen, dass Cyberangriffe im Zweifel für viele Unternehmen existenzgefährdendes Potential haben, so dass sich die Geschäftsleitung darum kümmern muss, solche Angriffe möglichst zu verhindern und Risiken daraus zu minimieren. Dafür ist im ersten Schritt eine Risikoanalyse erforderlich, mit der die Geschäftsleitung den Ist-Zustand erfasst, Risikopotenziale erkennt,

28 LG München I NZG 2014, 345 (juris-Rn. 103).
29 S. dazu *Spindler*, in diesem Band, C.

analysiert und eine Prognose abgibt.[30] Die Geschäftsleitung hat im Weiteren gemäß § 91 Abs. 2 AktG geeignete Überwachungsmaßnahmen zu ergreifen, mit denen die Umsetzung und Einhaltung der eingeleiteten Maßnahmen zur Risikominimierung kontrolliert werden. Bisher gibt es zu dieser Norm wenige Urteile[31]. Klar ist jedoch, dass die Einrichtung eines solchen Risikomanagementsystems eine Organisation erfordert, die „*unmissverständliche Zuständigkeiten begründet, ein engmaschiges Berichtswesen aufbaut und entsprechend dokumentiert ist. Es ist sicherzustellen, dass vom verantwortlichen Sachbearbeiter über die jeweiligen Hierarchieebenen bis hin zur Unternehmensleitung sämtliche relevante Stellen von vorhandenen Risiken Kenntnis erlangen, um die entsprechenden Maßnahmen zur Beherrschung dieser Risiken einleiten zu können*".[32] Dazu gehört, dass die Geschäftsleitung verstehen muss, welchen individuellen Risiken das Unternehmen ausgesetzt ist. Dies ist vielfach branchenabhängig. Ein Unternehmen, das im internationalen Anlagebau tätig ist und hierfür Spezialtechnologien verwendet, trägt andere Cyberrisiken als beispielsweise ein Handelsunternehmen. Die Geschäftsleitung hat für diese Risikosituation jeweils angepasste Gegenmaßnahmen zu ergreifen. Diese Gegenmaßnahmen sind nicht nur einmal zu beschließen und dann an die Fachabteilung zur Umsetzung zu übergeben, sondern fortlaufend auf ihre Aktualität und Angemessenheit zu überwachen und ihre Einhaltung zu kontrollieren.

Auch der Aufsichtsrat trägt nach § 116 i.V.m. § 93 AktG grundsätzlich ein Haftungsrisiko, wenn auch im Vergleich zu der operativ tätigen Geschäftsleitung deutlich abgeschwächt. Der Aufsichtsrat ist im Hinblick auf die wesentlichen Geschäftsrisiken überwachungspflichtig. Teilweise wird daher auch vertreten, dass der Aufsichtsrat deswegen jetzt selbst IT-Kompetenz haben muss.[33] Jedenfalls sollte beim Aufsichtsrat ein Bewusstsein für diese Verantwortung existieren sowie die Fähigkeit, das von der Geschäftsleitung präsentierte Sicherheitskonzept plausibilisieren zu können.

---

30 *Dauner-Lieb,* in: Henssler/Strohn (Hrsg.), GesellschaftsR, 5. Aufl. 2021, § 91 Rn. 7; *Spindler,* in: MüKo AktG, 5. Aufl. 2019, § 91 Rn. 20; *Fleischer,* in: BeckOGK, AktG, Stand: 15.01.2020, § 91 Rn. 31.

31 OLG Celle AG 2008, 711; LG Stuttgart NZG 2018, 665 Rn. 214 ff. zu Überwachungspflichten im Konzern.

32 LG München I NZG 2008, 319.

33 *Noack*, ZHR 2019, 105, 140; *Meckl/Schmidt*, BB 2019, 131, 132; *Kaspar*, Board 2018, 202; vgl. *Hanenberg* in: Hopt/Binder/Böcking (Hrsg.), Handbuch Corporate Governance von Banken und Versicherungen, 2. Aufl. 2020, § 17 Rn. 26 f.

2. *Enthaftung möglich?*

Weiter stellt sich die Frage, ob die Geschäftsleitung als Gesamtgremium für die Kernaufgabe der Cybersicherheit zuständig ist oder Aufgaben – so wie es üblich und zweckmäßig ist – delegieren kann. Der nichtzuständige Geschäftsleiter könnte sich so gegebenenfalls enthaften.

a. Horizontale Delegation

Bei Leitungsaufgaben besteht allerdings die Verpflichtung des Gremiums, selbst Grundsatzentscheidungen zu treffen und diese zu verantworten. So hat der Bundesgerichtshof in seinem Urteil vom 06.11.2018[34] zum wiederholten Male[35] klargestellt, dass eine Delegation von Leitungsaufgaben die anderen Geschäftsführungsmitglieder nicht von ihrer eigenen Verantwortung entbindet. Zwar ist es zulässig, Ressorts zu verteilen – das ist auch richtig und wichtig –, aber der Ressortverantwortliche bleibt vom übrigen Gremium eng zu überwachen und zu kontrollieren. Die grundsätzliche Gesamtverantwortung gilt trotz Delegation weiterhin. Denn hinsichtlich der horizontal delegierten Aufgaben verbleibt bei jedem einzelnen Geschäftsführungsmitglied eine Aufsichts- und Überwachungspflicht.[36]

b. Enthaftung durch vertikale Delegation

Der Grundsatz gilt dann erst recht für die vertikale Delegation. Kernaufgaben der Geschäftsleitung können nicht auf untergeordnete Mitarbeiter delegiert werden.[37] Dies betrifft allerdings nur den Kernbereich, also dem Grunde nach das „Ob" der jeweiligen Maßnahme. Die Umsetzung kann

---

34 BGH NZG 2019, 225 Rn. 15.

35 BGH NZG 2001, 320, 322; BGH NJW 1997, 130, 132.

36 BGH NZG 2001, 320, 322; *Hoffmann/Schieffer*, NZG 2017, 401, 405; *Koch*, in: Hüffer/Koch (Hrsg.), AktG, 14. Aufl. 2020, § 77, Rn. 15; *Fleischer* (Fn. 30), § 77 Rn. 60; *Spindler* (Fn. 30), § 93 Rn. 170; *Ziemons*, in: Michalski/Heidinger/Leible/J. Schmidt (Hrsg.), GmbHG, 3. Aufl. 2017, § 43 Rn. 341; *Knierim*, in: Wabnitz/Janovsky/Schmitt (Hrsg.), Wirtschafts-/SteuerstrafR-HdB, 5. Aufl. 2020, 5. Kap. Rn. 39.

37 *Spindler* (Fn. 30), § 76 Rn. 18; *Hoffmann/Schieffer*, NZG 2017, 401, 405; *Knierim* (Fn. 36), 5. Kap. Rn. 42; *Schulze*, NJW 2014, 3484, 3485; *Wentrup*, in: Münchener HdB d. GesellschaftsR Bd. 4, 5. Aufl. 2020, § 19 Rn. 34.

und soll an die zuständigen Mitarbeiter übertragen werden, deren Einhaltung und Aktualisierung dann aber zu kontrollieren ist.[38]

Eine Enthaftung im Rahmen der vertikalen Delegation ist nur möglich, wenn die Geschäftsleitung ihrer Pflicht, das Unternehmen im Hinblick auf Cyberrisiken ordnungsgemäß zu organisieren, hinreichend nachkommt.[39] Dazu gehört etwa, dass Mitarbeiter auf den Umgang mit Cyberrisiken hingewiesen und geschult worden sind. Allein der Einwand des rechtmäßigen Alternativverhaltens, also dass der Schaden durch den Cyberangriff auch bei ordnungsgemäßer Mitarbeiterschulung eingetreten wäre, führt danach wohl nicht zu einer Enthaftung. Nach der Rechtsprechung des Bundesgerichtshofs reicht die bloße Möglichkeit, dass der Schaden auch bei rechtmäßigem Verhalten hätte eintreten können, nicht zur Enthaftung der Geschäftsleitung aus.[40] Vielmehr muss klar sein, dass der Schaden in jedem Fall eingetreten wäre. Diese Hürde ist hoch.

c. Enthaftung durch Zertifizierung?

Es dürfte zur Enthaftung der Geschäftsleitung auch nicht allein ausreichen, auf eine Zertifizierung des Unternehmens zu verweisen. Ob eine Zertifizierung als Sicherheitsvorkehrung ausreichend sind, ist durch die Rechtsprechung nicht geklärt. Jedoch hat das BSI ein IT-Grundschutz-Kompendium herausgegeben, das auch Grundlage für eine Zertifizierung eines Unternehmens nach ISO 27001 sein kann. Ziel dieses Grundschutzes ist die Umsetzung der notwendigen IT-Sicherheitsmaßnahmen und eines Managementsystems für Informationssicherheit (ISMS). Insofern kann eine Zertifizierung geeignet sein, das Management des Unternehmens nach einem Angriff von dem Vorwurf nicht hinreichender Cybersecurity zu entlasten.

Dies dürfte aber nicht uneingeschränkt gelten. Das Zertifikat hat eine Gültigkeit von drei Jahren.[41] Die Zertifizierung ist aber nur eine Momentaufnahme. Drei Jahre sind in der IT-Sicherheit ein langer Zeitraum. Folglich kann ein möglicherweise einige Jahre altes Zertifikat nicht zuverlässig garantieren, ob das Unternehmen noch gegen aktuelle Angriffe gewappnet

38 *Spindler* (Fn. 30), § 76 Rn. 18; *Schulze*, NJW 2014, 3484, 3485; *Wentrup* (Fn. 37), § 19 Rn. 35 f.; *Knierim* (Fn. 36), 5. Kap. Rn. 42.
39 Vgl. dazu auch *Spindler*, in diesem Band, E.I.
40 BGH NZG 2018, 1189 Rn. 39.
41 BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema, Version 2.1 vom 21.05.2019, S. 14.

ist. Jedenfalls sollte sich die Geschäftsleitung bemühen, die im Rahmen des Zertifizierungsverfahrens vorgesehenen jährlichen Überwachungsaudits vorzunehmen und die dafür vorgesehenen Regelungen einzuhalten, sowie die Zertifizierungsstelle des BSI bei etwaigen wesentlichen Änderungen am zertifizierten Informationsverbund (z.B. größere Änderungen im Managementsystem) zu informieren.[42] Zum anderen ist die Zertifizierung – jedenfalls der BSI-Grundschutz – ein standardisierter Schutz. Für das Unternehmen muss also geprüft werden, ob dieser Grundschutz die individuelle Bedrohungs- bzw. Risikosituation abdeckt.

d. Enthaftung durch Versicherungslösung?

Zuletzt stellt sich die Frage, ob die Risiken aus Cyberangriffen abschließend versicherbar sind und das Haftungsrisiko so auf einen Dritten übergewälzt werden kann. So wird vereinzelt bereits diskutiert, ob alleine der Nicht-Abschluss einer Cyberversicherung haftungsbegründend wirkt.[43] Das kann aber nur der Fall sein, wenn eine Pflicht zum Abschluss einer Cyberversicherung bestünde. Eine solche Pflicht kann nur bestehen, wenn aufgrund einer Ermessensreduzierung auf Null jede andere Entscheidung ermessensfehlerhaft wäre. Das wird nur sehr selten der Fall sein. Cyberversicherungen wirken in der Regel nur risikominimierend und nicht ausschließend, weil die Schäden durch einen Cyberangriff die Deckungssumme wohl häufig überschreiten.

Bemerkenswert ist in diesem Zusammenhang auch, dass es in anderen Versicherungsprodukten aktuell noch keinen Risikoausschluss für Schäden aus Cyberangriffen gibt. In der Branche wird dieses Phänomen unter dem Stichwort „*Silent Cyber*“ diskutiert. Solche Versicherungsfälle, die auf Cyberrisiken zurückzuführen sind, wurden von den Versicherern nicht berücksichtigt und demzufolge auch nicht zuvor einkalkuliert. Die Versicherer sehen sich dadurch einer zusätzlichen Exponierung ausgesetzt, das heißt einer Abdeckung von Cyberrisiken, die bei der Entwicklung des jeweiligen Produktes häufig nicht bedacht wurden. Der Grund dafür liegt in der Aktualität der Entwicklung. Zum Zeitpunkt der Konzeption der meisten herkömmlichen Policen spielte der Faktor Cyberrisiken allenfalls eine

---

42 BSI, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema, Version 2.1 vom 21.05.2019, S. 14 f.

43 Vgl. *Fortmann,* r+s 2019, 688, 691.

untergeordnete Rolle.[44] Hier lohnt sich wiederum der Blick in die USA. Dort ist ein vielbeachteter Deckungsstreit aus einer Sachversicherung nach einem Cyberangriff mit der Malware *NotPetya* anhängig. In dem Fall *Mondelez International Inc* gegen *Zurich American Insurance Company* hat *Mondelez* seinen Sachversicherer über USD 100 Mio. verklagt, nachdem *Mondelez* einen Cyberangriff erlitten hat, der nicht nur zu einer Systemverschlüsselung führte, sondern auch die Hardware nachhaltig zerstörte, so dass ein Schaden in dreistelliger Millionenhöhe entstanden ist. In dem Rechtsstreit hat sich *Zurich* – soweit bekannt – nicht etwa auf den Standpunkt gestellt, dass die Sachversicherung bei Cyberangriffen nicht einschlägig sei. Vielmehr hat der Versicherer sich auf einen „Kriegs"-Deckungsausschluss berufen: der *NotPetya* Angriff sei staatlich gesteuert gewesen und deshalb einer kriegerischen Handlung gleichzusetzen.[45] Ob dieses Argument erfolgreich ist, ist noch nicht bekannt. Die Sache läuft – soweit ersichtlich – noch.[46]

Dies zeigt einerseits, dass Unternehmen nach einem Cyberangriff überprüfen sollten, ob ein solcher in den Anwendungsbereich ihrer Versicherungen fällt, auch wenn noch keine gesonderte Cyberversicherung abgeschlossen worden ist. Zum anderen bringt das auch die D&O-Versicherung ins Spiel, die bisher ebenfalls keinen Deckungsausschluss für Schäden aus einem Cyberangriff vorsieht. Damit liegt die Inanspruchnahme – wie der Trend in den USA zeigt – auch in Deutschland nahe.

III. Fazit

Es spricht viel dafür, dass Organhaftung im Zusammenhang mit Cyberangriffen ein Rechtsthema der Zukunft sein wird. In diesem Bereich besteht ein großes Haftungsrisiko für die Geschäftsleitung, das vor allen Dingen durch Prävention in den Griff zu bekommen ist. Die Geschäftsleitung

---

44 *Gebert/Klapper*, in: Veith/Gräfe/Gebert (Hrsg.), Der Versicherungsprozess, 4. Aufl. 2020, § 24 Cyberversicherung Rn. 48.

45 *Wolf*, Reasons for Communicating Clearly With Your Insurer Regarding the Scope of Coverage Before Purchasing Cyber Insurance, National Law Review, Volume X, Number 155 (Stand: 03.06.2020), https://www.natlawreview.com/article/reasons-communicating-clearly-your-insurer-regarding-scope-coverage-purchasing-cyber (abgerufen am 08.02.2021).

46 Der aktuelle Stand des Rechtsstreits kann unter „http://www.cookcountyclerkofcourt.org/CourtCaseSearch/DocketSearch.aspx" abgerufen werden. Dafür muss unter „Select a Division" „Law" ausgewählt und die Case Number „2018-L-011008" eingegeben werden.

muss die Cyberrisiken des eigenen Geschäftsmodells verstanden haben und ein Konzept zur Risikominimierung vorsehen und fortlaufend aktualisieren.