Digitalisierung »DB1280123

RA Dr. Natalie Daghles, Düsseldorf

Cybersecurity-Compliance: Pflichten und Haftungsrisiken für Geschäftsleiter in Zeiten fortschreitender Digitalisierung

Dr. Natalie Daghles ist Partnerin der Sozietät Latham & Watkins LLP in Düsseldorf.
Kontakt: autor@der-betrieb.de

In Zeiten fortschreitender Digitalisierung verlagert sich die Wertschöpfung in Unternehmen weiter in den virtuellen Raum – damit wird das Thema IT-Sicherheit zugleich immer bedeutender. Die Relevanz von IT-Risiken steigt für Unternehmen jeder Größenordnung und unabhängig vom Geschäftsmodell. Welche spezifischen Anforderungen ergeben sich daraus für Geschäftsführung, Vorstand und Aufsichtsrat? Inwiefern geht damit ein erweitertes Haftungsrisiko einher? Der Blick in die USA zeigt, dass es Klagen gegen Management und ihre D&O-Versicherer im Zusammenhang von Pflichtverletzungen im Bereich IT-Sicherheit gibt.

I. Einleitung

Unternehmen setzen die digitalen Technologien immer weitreichender zur Effizienzsteigerung und zur Verknüpfung von Prozessschritten entlang der gesamten Wertschöpfungskette ein. Zudem sind diese sich schnell entwickelnden Technologien Grundlage völlig neuer Geschäftsmodelle. Es erfolgt damit eine Verlagerung der Wertschöpfung in den virtuellen Raum. Dabei ergeben sich nicht nur neue Möglichkeiten der Wertschöpfung und Effizienzsteigerung, sondern gleichzeitig neue Gefahren und Einfallstore für Hackerangriffe. Es drohen direkte Fremdeingriffe in die Prozesse und Produktionsabläufe mit schwerwiegenden Auswirkungen.

Beispiele für Hackerangriffe gibt es viele: Nicht nur politisch motivierte Angriffe wie jüngst auf das Datennetzwerk der Bundesverwaltung – der Informationsverbund Berlin-Bonn (IVBB), sondern immer häufiger empfindliche Attacken im wirtschaftlichen Bereich. Dabei treffen Hackerangriffe DAX-Konzerne ebenso wie mittelständische oder kleine Unternehmen. Der Gesamtschaden für die deutsche Wirtschaft in diesem Bereich wird auf jährlich rund 50 Mrd. € geschätzt.[1] Erst vor gut einem Jahr wurden über 230.000 Rechner in 150 Ländern durch WannaCry infiziert, eine Schadsoftware zur digitalen Erpressung. Derartige Schadsoftware sperrt den Zugriff oder verschlüsselt Daten, sodass die Zahlung eines Lösegelds – in Form einer Internetwährung wie z.B. Bitcoins – erpresst werden kann.

Vorstand und Aufsichtsrat müssen sich mit der sich wandelnden Risikolandschaft auseinandersetzen. Es ergeben sich neue Verantwortlichkeiten, welche gleichzeitig mit einer Erweiterung einer möglichen Haftung einhergehen. Die Grundlagen der Sorgfaltspflichten finden auch im Kontext von Cybersecurity-Risiken Anwendung (dazu unter II.). In den USA wurden in den letzten Jahren vermehrt Verfahren gegen Manager und ihre D&O-Versicherer im Zusammenhang mit IT-Sicherheitslücken geführt.[2] Vorwurf in diesen Verfahren waren regelmäßig nicht ausreichende Sicherheitsmaßnahmen zur Verhinderung von Hackerangriffen und Datenverlusten sowie die Verletzung von Berichtspflichten. Die Gesetzgebung hat an verschiedener Stelle gesetzliche Anforderungen an die IT-Sicherheit thematisiert (hierzu unter III.). Es stellt sich zudem die Frage nach etwaigen Offenlegungs- und Meldepflichten im Zusammenhang mit IT-Risiken oder konkreten Hackerangriffen (dazu unter IV.). Anregungen zur Überprüfung der unternehmensseitigen Organisation finden sich in einer Checkliste zum Thema IT-Sicherheit (vgl. unter V.).

II. Allgemeines Pflichtenregime

1. Sorgfaltspflicht

Vorstandsmitglieder haben die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, § 93 Abs. 1 Satz 1 AktG.[3] Diese Regelung ist eine Generalklausel der unternehmerischen Verhaltenspflicht, aus der wiederum situationsbezogene Einzelpflichten abgeleitet werden.[4] Primär enthält sie Treuepflicht und Sorgfaltspflicht der Vorstandsmitglieder.[5] Vorstandsmitglieder haben nicht nur im erwerbswirtschaftlichen Interesse der Gesellschaft zu agieren, sondern auch die Interessen der Aktionäre, Gläubiger und das Wohl der Arbeitnehmer und Allgemeinheit einzubeziehen.[6] Durch die generalklauselartige Umschreibung unterliegt der Umfang der Verhaltenspflicht keinen starren Vorgaben, sondern insgesamt einem stetigen Wandel – Kriterien sind nicht nur Art und Umfang des Unternehmens, dessen Beschäftigtenzahl oder die Konjunkturlage, sondern auch die jeweiligen Zeitumstände.[7]

Als Antwort auf das generalklauselartig umschriebene Pflichtenregime ist in § 93 Abs. 1 Satz 2 AktG die aus dem angloamerikanischen stammende Business Judgement Rule verankert. Eine Pflichtverletzung eines Vorstandsmitglieds ist dann nicht

1 So eine Studie des Digitalverbands Bitkom, vgl. PM des Bundesamts für Verfassungsschutz vom 21.07.2017, abrufbar unter: http://hbfm.link/4096 (Abruf: 07.09.2018).

2 Vgl. United States District Court of New Jersey in re Heartland Payment Systems Inc. (2008); United States District Court of New Jersey, FTC v. Wyndham Worldwide Corporation et al. (2010); United States District Court, D. Minnesota in re Target Corporation Customer Data Security Breach Litigation (2013); United States District Court for the Northern District of Georgia, Atlanta Division in re The Home Depot, Inc. Shareholder Derivative Litigation (2016); U.S. District Court Middle District of Florida (Orlando), Torres v. Wendy's International, LLC (2017).

3 Dasselbe gilt i.Ü. nach § 43 GmbHG für die Geschäftsführer einer GmbH, sodass die nachfolgenden Ausführungen diese gleichermaßen betreffen.

4 Koch, in: Hüffer/Koch (Hrsg.), Aktiengesetz, 13. Aufl. 2018, § 93 Rn. 5; Mertens/Cahn, in: Zöllner/Noack, Kölner Komm. z. Aktiengesetz, 3. Aufl., § 93 Rn. 10 f.; Spindler, in: MünchKomm- AktG, 4. Aufl. 2014, § 93 Rn. 21.

5 Dauner-Lieb, in: Henssler/Strohn, Gesellschaftsrecht, 3. Aufl. 2016, § 93 Rn. 4; Mertens/Cahn, a.a.O. (Fn. 4), § 93 Rn. 64 ff.

6 Spindler, a.a.O. (Fn. 4), § 76 Rn. 62.

7 Hölters, in: Hölters (Hrsg.), Aktiengesetz, 3. Aufl. 2017, § 93 Rn. 3 f.; Spindler, a.a.O. (Fn. 4), § 93 Rn. 25 f.; Spindler, CR 2017 S. 715 (716).

anzunehmen, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln. Dieser sog. Safe Habor gilt auch in Bezug auf Managemententscheidungen im Bereich der IT-Sicherheit. Eine nach der Business Judgement Rule erforderliche unternehmerische Entscheidung liegt vor, wenn der Vorstand eine mit Risiken verbundene, in die Zukunft gerichtete Entscheidung fällt.[8] Der Vorstand ist verpflichtet, alle ihm zur Verfügung stehenden Erkenntnisquellen auszuschöpfen, dabei hat er Kosten und Nutzen gegeneinander abzuwägen.[9] Vor diesem Hintergrund kann eine persönliche Haftung im Bereich der IT-Sicherheit drohen, wenn Risiken nicht angemessen identifiziert und adressiert werden und dem Unternehmen dadurch ein Schaden entsteht.

Für Entscheidungen im Bereich IT-Sicherheit bedeutet dies zunächst, dass Vorstandsmitgliedern die unternehmensspezifischen IT-Sicherheitsrisiken ihrer Gesellschaft grds. bekannt sein müssen. Vorstand und Aufsichtsrat sind gehalten, sich mit den Komplexitäten der IT-Sicherheit in ihrem Unternehmen vertraut zu machen und geeignete Maßnahmen zur Gewährleistung von IT-Sicherheit zu ergreifen.[10] Je bedeutsamer die IT für das Unternehmen und je gravierender die Auswirkungen eines etwaigen Angriffs auf die Systeme, desto mehr Informationen haben Vorstandsmitglieder einzuholen. Dazu gehört IT-Sicherheit als fester Bestandteil regelmäßig auf die Agenda von Vorstand und Aufsichtsrat. Wie auch z.B. bei der Errichtung einer angemessenen Compliance-Organisation[11], unterliegt die Ausgestaltung der Organisation zur Gewährleistung der IT-Sicherheit nach den allgemeinen Grundsätzen dem Ermessen des Vorstands im Rahmen der Business Judgement Rule.[12]

2. Legalitätspflicht

Aus den allgemeinen Regelungen leitet sich die Legalitätspflicht des Vorstands ab. Danach hat der Vorstand im Rahmen seiner Entscheidungen stets Recht und Gesetz einzuhalten.[13] Insoweit besteht kein der Business Judgement Rule inhärentes Ermessen; es gibt keinen Safe Harbor für gesetzeswidriges Verhalten.[14] Sind die rechtlichen Rahmenbedingungen nicht klar, hat der Vorstand u.U. Rechtsrat einzuholen.[15] Die Legalitätspflicht umfasst auch eine Kontrollpflicht, d.h. der Vorstand hat nicht nur eigene Gesetzesverstöße zu unterlassen, sondern auch aktiv Vorkehrungen zu treffen, um Gesetzesverstößen von Unternehmensangehörigen vorzubeugen.[16] Insgesamt ergeben Legalitäts- und Legalitätskontrollpflicht eine Compliance-Verantwortung des Vorstands.[17] Wie er dieser durch die Ausgestaltung konkreter (Überwachungs-)Maßnahmen und Systeme gerecht wird, unterfällt dabei seinem Ermessen.[18]

Der Vorstand hat sich daher über die auf sein Unternehmen anwendbaren Regelungen im Bereich der IT-Sicherheit zu informieren (zu ausgewählten relevanten gesetzlichen Normierungen gleich unter III.). Die Einhaltung der Vorschriften kann gerade im Bereich des Umgangs mit personenbezogenen Daten gezielte Sicherheitsvorkehrungen im Unternehmen erforderlich machen. Policies und Richtlinien sind insoweit zu verabschieden und stetig anzupassen und im Unternehmen zu verteilen. Es sollten Schulungen angeboten werden, um Mitarbeiter für das Thema IT-Sicherheit zu sensibilisieren und die Einhaltung bestimmter Standards zu gewährleisten.[19]

3. Einrichtung von Überwachungssystemen

§ 91 Abs. 2 AktG konkretisiert und ergänzt die allgemeine Sorgfaltspflicht, wonach der Vorstand geeignete Maßnahmen, insb. die Einrichtung eines Überwachungssystems, zu ergreifen hat, „damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden".

Zum einen wird damit das Ziel normiert, frühzeitig bestandsgefährdende Entwicklungen zu erkennen, zum anderen hat der Vorstand geeignete Maßnahmen zu treffen und entsprechend ein Überwachungssystem einzurichten.[20] Weiter regelt der Deutsche Corporate Governance Kodex (DCGK), dass der Vorstand für ein angemessenes Risikomanagement und Risikocontrolling sorgt und den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Risikolage und des Risikomanagements informiert (vgl. Ziff. 4.1.4 und 3.4 DCGK).

Vor diesem Hintergrund sind Cyberrisiken und das Thema IT-Sicherheit im Unternehmen auch im Rahmen des Risikomanagements zu validieren.[21] Teil der Risikoprävention ist dabei der Schutz der IT-Infrastruktur, d.h. die Sicherstellung der IT-Sicherheit. Es sind grds. solche Maßnahmen zu veranlassen, die ein angemessenes Schutzniveau gewährleisten. Die Bestimmung der jew. erforderlichen Maßnahmen bedarf dabei einer individuellen Risikoanalyse, d. h. einer auf das Unternehmen mit seinen Anforderungen an IT-Sicherheit, seine Tätigkeitsbranche, seine Größe, die anfallende Datenmenge etc. zugeschnittenen Überprüfung.

Orientierungspunkte für die Einrichtung von derartigen Überwachungssystemen stellen die „IT-Grundschutzkataloge" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie die BSI-Standards dar.[22] Die IT-Grundschutz-Kataloge enthalten für typische Prozesse, Anwendungen und IT-Komponenten Bausteine. Zu jedem Thema werden Sicherheitsmaßnahmen empfohlen und die wichtigsten Gefährdungen beschrieben, vor denen man sich schützen sollte. Zudem haben sich die International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC) darauf geeinigt, internationale Standards zur Informationssicherheit in der ISO 2700x-Reihe

8 Hölters, a.a.O. (Fn. 7), § 93 Rn. 30; Mertens/Cahn, a.a.O. (Fn. 4), § 93 Rn. 17; Spindler, a.a.O. (Fn. 4), § 93 Rn. 36.

9 Hölters, a.a.O. (Fn. 7), § 93 Rn. 34; Mertens/Cahn, a.a.O. (Fn. 4), § 93 Rn. 32 ff.

10 Rath/Kuß, in: Umnuß (Hrsg.), Corporate Compliance Checklisten, 3. Aufl. 2017, Kapitel 8, Rn. 1 ff.; Schmidl, in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 46 f.

11 Vgl. dazu unten, insb. Fn. 17, 18.

12 Conrad, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 33 Rn. 38 ff.

13 Fleischer, in: Spindler/Stilz, Aktiengesetz, 3. Aufl. 2015, § 93 Rn. 14 ff.; Hölters, a.a.O. (Fn. 7), § 93 Rn. 54; Koch, a.a.O. (Fn. 4), § 93 Rn. 6d; Wiesner, in: Münchener Handbuch des Gesellschaftsrechts Bd. 4, 4. Aufl. 2015, § 25 Rn. 23 ff.

14 Fleischer, a.a.O. (Fn. 13), § 93 Rn. 37; Hopt, in: GK AktG, 5. Aufl. 2015, § 93 Rn. 74 ff., 82; Spindler, a.a.O. (Fn. 4), § 93 Rn. 73, 75.

15 Hölters, a.a.O. (Fn. 7), § 93 Rn. 76; Wiesner, a.a.O. (Fn. 13), § 25 Rn. 30 f.; zu den Voraussetzungen unter denen sich der Vorstand auf Rechtsrat verlassen darf, vgl. Fleischer, a.a.O. (Fn. 13), § 93 Rn. 35 ff.

16 Koch, a.a.O. (Fn. 4), § 93 Rn. 6d; Wiesner, a.a.O. (Fn. 13), § 25 Rn. 34.

17 Vgl. Ziff. 4.1.3 S. 1 DCGK; wobei jedoch die Einzelheiten an die Anforderungen der Ausgestaltung umstritten sind: Goette, ZHR 2011 S. 388; Koch, a.a.O. (Fn. 4), § 93 Rn. 13 ff. m.w.N.; Spindler, a.a.O. (Fn. 4), § 91 Rn. 63 ff.

18 Goette, ZHR 2011 S. 388 (399 f.); Hopt, a.a.O. (Fn. 14), § 93 Rn. 75, 77; Koch, a.a.O. (Fn. 4); Spindler, a.a.O. (Fn. 4), § 91 Rn. 6.

19 Schmidl, a.a.O. (Fn. 10), § 28 Rn. 27.

20 Müller-Michaels, in: Hölters (Hrsg.), Aktiengesetz, 3. Aufl. 2017, § 91 Rn. 4; Spindler, a.a.O. (Fn. 4), § 91 Rn. 15 ff.

21 Schmidl, a.a.O. (Fn. 10), § 28 Rn. 46 f.

22 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, abrufbar unter: http://hbfm.link/4097 (Abruf: 07.09.2018).

zusammenzuführen (z.B. ISO 27001, der internationale Standard zum Management von Informationssicherheit).
Insgesamt sollte ein ausgewogenes IT-Sicherheitssystem mit einer Risikoanalyse beginnen, regelmäßige Überprüfungen, bspw. in Form von Audits, sowie einen Notfallplan vorsehen.

4. Delegation von Aufgaben

Vorstandsmitglieder können im Grundsatz Aufgaben durch Ressortzuweisung an einzelne Vorstandsmitglieder oder hierarchisch nachgeordnete Personen delegieren. Die Übertragung unternehmerischer Aufgaben entbindet das einzelne Vorstandsmitglied jedoch keinesfalls von seiner Gesamtverantwortung. Vielmehr ändert sich im Fall vertikaler oder horizontaler Delegation lediglich der Verantwortungs- bzw. Pflichteninhalt, nämlich von einer Handlungspflicht in eine Auswahl- und Überwachungspflicht.[23]
Bei horizontaler Delegation trägt das Vorstandsmitglied zwar im Rahmen seiner Ressortzuständigkeit die umfassende alleinige Handlungsverantwortlichkeit, die mit einem gewissen Gestaltungs- und Entscheidungsspielraum einhergeht.[24] Die übrigen Vorstandsmitglieder sind jedoch zur angemessenen Überwachung verpflichtet, haben insb. Informationsansprüche.[25] Schließlich können die Leitung des Unternehmens an sich sowie Aufgaben, die kraft Gesetzes dem Gesamtvorstand übertragen sind, nicht einem einzelnen Vorstandsmitglied zugewiesen werden.[26]
Im Rahmen vertikaler Delegation ist zu beachten, dass der Vorstand nur solche Aufgaben weitergeben darf, die nicht in den Kernbereich seiner Leitungsverantwortung fallen.[27] Dies betrifft die wesentlichen grundlegenden Organisationsfragen, insb. die Definition der Unternehmenspolitik, die Unternehmenszielverwirklichung, Führungsentscheidungen sowie solche Pflichten, die dem Gesamtvorstand kraft Gesetzes übertragen sind.[28] In diesem Bereich können nur vorbereitende Aufgaben und Hilfstätigkeiten abgegeben werden, wobei die Letztentscheidung beim Vorstand verbleibt.[29]
Bei vertikaler Delegation bezieht sich die Auswahlpflicht vor allem auf Qualifikation und persönliche Eignung der beauftragten Personen. Im Rahmen der Überwachungspflicht sind laufende wie anlassbezogene Kontrollen erforderlich, und zwar in dem Maße, dass Unregelmäßigkeiten nicht vorkommen und Risiken frühzeitig identifiziert werden. Damit korrespondieren auch umfassende Dokumentationspflichten sowie ggf. Instruktionspflichten hinsichtlich Rechtspflichten und Risiken.
Diese allgemeinen Grundsätze zur Delegation von Aufgaben auf Vorstandsebene zeigen, dass der Vorstand das Thema IT-Sicherheit auch bei vertikaler Delegation an Fachpersonal nicht unbeachtet lassen kann. Vor dem Hintergrund der gravierenden Gefährdungslage und der sich sehr schnell verändernden Risikosituation, bleibt eine regelmäßige Abstimmung mit dem Fachpersonal notwendig.

Die personelle Organisation ist durch den Vorstand an die jew. bestehende IT-Risikolandschaft anzupassen. Sicher ist es generell sinnvoll, Zuständigkeiten für die IT-Sicherheit zu schaffen,[30] etwa die Position eine Chief Information Security Officers. Das entbindet die Geschäftsleitung zwar nach o.g. Grundsätzen nicht von ihrer Verantwortung, ist für ein angemessenes Risikomanagement jedoch zu empfehlen.[31]

5. Rechtsfolgenseite: Haftung für IT-Sicherheit?

Vorstandsmitglieder haben Schäden, die der Gesellschaft durch Pflichtverletzungen des Vorstands entstanden sind, gem. § 93 Abs. 2 Satz 1 AktG zu ersetzen. Werden aufgrund mangelnder Sicherheitsvorkehrungen Geschäftsdaten des Unternehmens durch Hacker entwendet oder fällt eine Produktionsanlage wegen unzureichender Ausstattung oder Wartung der IT-Infrastruktur aus und entsteht der Gesellschaft hierdurch ein Schaden, droht eine Haftung des Vorstands, wenn die Gesellschaft nachweisen kann, dass der Vorstand eine Pflichtverletzung begangen hat – also z.B. kein angemessenes Cybersecurity Management System etabliert wurde oder die IT-Infrastruktur nicht den Anforderungen entsprach. Das Vorstandsmitglied kann sich dann nur exkulpieren, wenn es die Sorgfalt eines ordentlichen Kaufmanns angewendet hat bzw. bei einer unternehmerischen Entscheidung die Voraussetzungen der Business Judgement Rule vorlagen.[32]
Auch Geldbußen von Aufsichtsbehörden gegen das Unternehmen können grundsätzlich zum ersatzfähigen Schaden im Rahmen der Vorstandshaftung gehören.[33] Vor dem Hintergrund, dass z.B. Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) sehr hohe Geldbußen für Unternehmen nach sich ziehen können, ist nicht auszuschließen, dass Unternehmen zukünftig den Vorstand bzw. die D&O-Versicherung des Vorstands in Regress nehmen werden.
Daneben ist eine Haftung des Vorstands für die Verletzung von Organisationspflichten gegenüber Dritten nur im Ausnahmefall denkbar. Weitere Ausführungen hierzu bedürfen jedoch vor dem Hintergrund der jüngeren Rechtsprechung[34], die eine deliktische Haftung nur innerhalb von sehr engen Grenzen annimmt, einer umfassenderen Betrachtung, als sie der vorliegende Beitrag leisten kann.
In den letzten Jahrzehnten – insb. nach der ARAG/Garmenbeck-Entscheidung des BGH –[35] steht das Thema Vorstandshaftung im Fokus. In jüngster Vergangenheit waren gerade Verantwortlichkeiten für Compliance-Verstöße (z.B. Bestechungen, kartellrechtswidrige Absprachen, Verstöße gegen Geheimhaltungspflichten, Datenschutz oder Arbeitnehmerschutzvorschriften) Gegenstand der durch Unternehmen geführten Verfahren gegen Vorstandsmitglieder. Verstöße im Bereich der IT-Sicherheit waren bisher in Deutschland nicht Gegenstand der Rechtsverfolgung gegen Vorstände. Aufgrund der fortschreitenden Digitalisierung sämtlicher Unternehmensprozesse und der zunehmenden Regulierung könnte sich dies in Zukunft aber ändern, wie auch ein Blick in andere Rechtsordnungen zeigt.

23 Fleischer, a.a.O. (Fn. 13) , § 76 Rn. 63 ff., § 77 Rn. 47 ff., § 93 Rn. 100; Hoffmann/Schieffer, NZG 2017 S. 401 (406); Schmidt-Husson in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance, 3. Aufl. 2016, § 6 Rn. 12; Spindler, a.a.O. (Fn. 4), § 93 Rn. 148 ff.; Spindler, CR 2017 S. 715 (721 f.).
24 Fleischer, a.a.O. (Fn. 13), § 77 Rn. 47 ff.; Koch, a.a.O. (Fn. 4), § 14 ff.; Wiesner, a.a.O. (Fn. 13), § 22 Rn. 24.
25 Spindler, a.a.O. (Fn. 4), § 77 Rn. 55 ff.; Schmidt-Husson a.a.O. (Fn. 23), § 6 Rn. 32 ff.; Wiesner, a.a.O. (Fn. 13), § 22 Rn. 24.
26 Fleischer, a.a.O. (Fn. 13), § 77 Rn. 47 ff.; Schmidt-Husson, a.a.O. (Fn. 23), § 6 Rn. 15; Spindler, a.a.O. (Fn. 4), § 77 Rn. 62.
27 Fleischer, a.a.O. (Fn. 13), § 93 Rn. 99; Hoffmann/Schieffer, NZG 2017 S. 401 (405); Schmidt-Husson, a.a.O. (Fn. 23), § 6 Rn. 16; Wiesner, a.a.O. (Fn. 13), § 19 Rn. 31, § 25 Rn. 37.
28 Hoffmann/Schieffer, NZG 2017 S. 401 (405); Koch, a.a.O. (Fn. 4), § 76 Rn. 8 f.; Schmidt-Husson, a.a.O. (Fn. 23), § 6 Rn. 16 ff.; Wiesner, a.a.O. (Fn. 13), § 19 Rn. 17.
29 Koch, a.a.O (Fn. 4), § 76 Rn. 8 f.; Schmidt-Husson, a.a.O. (Fn. 23), § 6 Rn. 24.
30 Spindler, CR 2017 S. 715 (721 f.).
31 Teilweise werden Fragen der Informationssicherheit, insb. datenschutzrechtliche Auswirkungen, sogar der Leitungszuständigkeit der Geschäftsleitung zugeordnet, vgl. Koch, a.a.O (Fn. 4), § 76 Rn. 9; Behling, ZIP 2017 S. 697 (698 ff.).
32 Fleischer, a.a.O. (Fn. 13), § 93 Rn. 200 ff., 221; Voigt, IT-Sicherheit, 2018, Rn. 200 f.
33 Zu Umfang und Grenzen der Regresshaftung von Organen für Geldbußen gegen die Gesellschaft vgl. Fleischer, DB 2014 S. 345; Bayer/Scholz, GmbHR 2015 S. 449; Voigt, a.a.O. (Fn. 32), Rn. 202.
34 BGH vom 10.07.2012 – VI ZR 341/10, DB 2012 S. 1799; vom 18.06.2014 – I ZR 242/12, DB 2014 S. 1799; vgl. dazu Fleischer, a.a.O. (Fn. 13), § 93 Rn. 314 ff.
35 BGH vom 21.04.1997 – II ZR 175/95, DB 1997 S. 1068.

a) Blickrichtung USA

Wirft man einen Blick in Richtung USA sieht man bereits eine entsprechende Entwicklung: Dort gab es in den letzten Jahren einige Fälle, in denen das Management im Zusammenhang mit Hackerangriffen zur Verantwortung gezogen werden sollte.[36] Keine der Klagen hatte dabei aber bisher Erfolg. Zuletzt hatte der U.S. District Court of Georgia[37] über eine Klage gegen die Geschäftsführung der Baummarktkette Home Depot wegen eines Vermögensschadens nach einem Hackerangriff zu entscheiden, bei dem über Malware in Kassensystemen Kreditkartendaten und E-Mail-Adressen von Kunden in den USA und Kanada gestohlen wurden. Das Management konnte sich exkulpieren. Es hatte regelmäßige Cybersecurity-Reports durch ein vom Management eingesetztes Audit-Committee gegeben und das Management hatte sich umfassend mit der Aufdeckung von IT-relevanten Sicherheitslücken befasst. Ebenso gab es ein Verfahren gegen das Management von Heartland Payment Systems, wegen des Diebstahls von 130 Mio. Kreditkarten-Informationen und einem Schaden von 110 Mio. US-Dollar. Target Corporation ging gegen das Management wegen Diebstahls von 70 Mio. kundenbezogenen Daten und 40 Mio. Kreditkarteninformationen einschließlich zugehöriger PINs vor.

Die Fast-Food Kette Wendy's führte ein Verfahren gegen das Management, da Malware im Kassensystem von 1.000 Filialen entdeckt wurde. Das Verfahren endete im Mai 2018 mit einem Vergleich. Die Anteilseigner von Wendy's hatten ihre Klage u.a. auf die Verletzung der Loyalitätspflicht und die Pflicht zu ordnungsgemäßer und gewissenhafter Geschäftsführung wegen nicht effektiver Kontrolle von Datensicherheit sowie die mangelhafte Veröffentlichung der Verletzung verschiedener Sicherheitsstandards gestützt. Interessant ist hierbei, dass auch ein Verstoß gegen Veröffentlichungspflichten gerügt wurde (dazu unten unter IV. mehr).

b) D&O- und Cyber-Versicherungen

Die Haftungsrisiken, die sich aus der Organtätigkeit als Vorstand ergeben, können durch den Abschluss einer D&O-Versicherung zumindest größtenteils abgesichert werden. Es handelt sich dabei regelmäßig um eine (Vermögensschadens-)Haftpflichtversicherung, die im Fall von (nicht vorsätzlichen) Sorgfaltspflichtverletzungen greift. Grds. sind auch Cyber-Risiken von D&O-Versicherungen umfasst.[38] Dennoch sollten Vorstände und Aufsichtsräte im eigenen Interesse überprüfen, dass diese Risiken auch im konkreten Einzelfall angemessen abgedeckt sind.

Weiterhin erlangen zunehmend sog. Cyber-Versicherungen von Unternehmen an Bedeutung.[39] Diese decken als Kombination aus Haftpflicht-, Betriebsausfall- und Datenversicherung solche IT-Risiken und IT-Schäden ab, die nicht von den üblichen Versicherungen erfasst sind.[40] Dabei geht es insb. um die Deckung von Eigenschäden aufgrund von Betriebs- und Ertragsausfall sowie Dritt- und Vermögensschäden.[41] Zudem lassen sich Cyber-Versicherungen mit Lösegeldversicherungen kombinieren, was gerade im Kontext von Hackerangriffen interessant werden kann.[42] Vor dem Hintergrund des allgemeinen Pflichtenregimes von Vorstand und Aufsichtsrat sollte in Betracht gezogen werden, ob eine solche Versicherung im konkreten Fall für ein Unternehmen interessengerecht ist.[43]

III. Gesetzliche Anforderungen an IT-Sicherheit

Im Bereich der IT-Sicherheit hat der Gesetzgeber in unterschiedlichem Zusammenhang Vorgaben getroffen. Vorstand und Aufsichtsrat bindet die Legalitätspflicht an die Einhaltung der Regelungen. Eine eindeutige gesetzliche Definition der Anforderungen an die IT-Sicherheit lässt sich dem Gesetz jedoch nicht entnehmen. Vielmehr sind in verschiedenen Gesetzen abstrakte Vorgaben enthalten:

1. IT-Sicherheitsgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und zum Schutz von kritischen Infrastrukturen

So normiert das IT-Sicherheitsgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und zum Schutz von kritischen Infrastrukturen (KRITIS) in Deutschland für Betreiber kritischer Infrastrukturen in § 8a BSIG die Pflicht „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind". Weiter enthält es u.a. die Pflichten, eine Kontaktstelle zu benennen, den „Stand der Technik" umzusetzen und dies alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen. Das Gesetz richtet sich insoweit an Telekommunikationsunternehmen, Anbieter von digitalen Diensten (z.B. Online-Marktplätzen, Suchmaschinen, Cloud-Computing-Diensten) und Betreiber von kritischen Infrastrukturen (z.B. in den Sektoren Energie, Ernährung und Wasser, Informationstechnik und Telekommunikation, Finanzen, Gesundheit sowie Transport und Verkehr).[44] Aber auch für andere Unternehmen könnten die Vorgaben des BSIG Anhaltspunkte zur Best Practice bei der Etablierung einer geeigneten IT-Sicherheit bieten.[45]

Neben dem IT-Sicherheitsgesetz sind noch eine Vielzahl spezialgesetzlicher Regelungen zur IT-Sicherheit zu berücksichtigen, z.B. §§ 13 Abs. 7 TMG, 109, 109a TKG, § 11 EnwG.

2. Bankaufsichtsrechtliche Anforderungen an die IT (BAIT)/ versicherungsaufsichtsrechtliche Anforderungen an die IT (VAIT)

Für Kredit- und Finanzdienstleistungsunternehmen ergeben sich besondere organisatorische Pflichten aus dem KWG und den Mindestanforderungen an das Risikomanagement (MaRisk). Die BaFin hat diese Anforderungen für den Bereich IT im November 2017 mit ihren „Bankaufsichtlichen Anforderungen an die IT (BAIT)" konkretisiert.[46] Zentrales Thema der BAIT ist es, das IT-Risikobewusstsein der Unternehmensleitung zu schärfen und Risikotransparenz zu schaffen. Nach der BAIT muss die Geschäftsleitung eines Kredit- bzw. Finanzdienstleistungsinstituts zunächst eine nachhaltige IT-Strategie festlegen,

36 Vgl. die Fälle in Fn. 2.

37 United States District Court for the Northern District of Georgia, Atlanta Division in re The Home Depot, Inc. Shareholder Derivative Litigation (2016).

38 Achenbach, VersR 2017 S. 1493 (1496); Erichsen, CCZ 2015 S. 247 (250); Ihlas, in: Langheid/Wandt (Hrsg.), MünchKomm-VVG, 2. Aufl. 2017, Bd. 3, 2. Teil, 3. Kapitel, Rn. 830.

39 Vgl. bspw. Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber), Musterbedingungen des GDV (Stand: April 2017).

40 Hierzu insgesamt: Achenbach, VersR 2017 S. 1493; Wirth, BB 2018 S. 200 (202).

41 Erichsen, CCZ 2015 S. 247 (249).

42 Achenbach, VersR 2017 S. 1493 (1498); Wirth, BB 2018 S. 200 (205).

43 So auch Achenbach, VersR 2017 S. 1493 (1496 f.); Erichsen, CCZ 2015 S. 247 (250).

44 Vgl. zur Erweiterung des Anwendungsbereichs RegE zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie), BT-Drucks. 18/11242; zu den Neuregelungen insgesamt auch Hornung, NJW 2015 S. 3334.

45 So bspw. auch Rath/Kuß, a.a.O. (Fn. 10), Kapitel 8 Rn. 7.

46 Bundesanstalt für die Finanzdienstleistungsaufsicht, Rundschreiben 10/2017 (BA) vom 03.11.2017, Bankaufsichtliche Anforderungen an die IT (BAIT).

die sich an der Geschäftsstrategie orientiert. In dieser sind die grundsätzliche IT-Organisation, die gängigen IT-Standards und die Zuständigkeiten zu regeln. Ausgehend von dieser Strategie müssen Steuerung und Überwachung der IT-Systeme durch umfassende IT-Governance sichergestellt werden. Diese sind Teil des zu errichtenden Informationsrisikomanagements, dessen Umfang von den Geschäftsaktivitäten sowie der Risikosituation des jeweiligen Instituts abhängig ist. In diesem Rahmen sind insb. die mit den Informationsrisiken verbundenen Aufgaben und Zuständigkeiten zu definieren und abzustimmen. Daneben gilt es, ein Informationssicherheitsmanagement zu etablieren, das u.a. interne Informationssicherheitsleitlinien, die Position eines Informationssicherheitsbeauftragten sowie dessen Berichtspflichten an die Geschäftsleitung vorsieht. Die Pflicht zur Errichtung eines Informationssicherheitsmanagements korrespondiert mit der Vorgabe, ein Benutzerberechtigungsmanagement einzuführen, das den Umfang und die Bedingungen der Berechtigungen für die IT-Systeme festlegt. Schließlich muss die Einhaltung der vorgenannten Pflichten regelmäßig überprüft und die Umsetzung angepasst und verbessert werden. Auch eine Auslagerung von IT-Dienstleistungen ist nur im Einklang mit der IT-Strategie und den Bedürfnissen des jeweiligen Instituts möglich.

§ 26 VAG verpflichtet Versicherungsunternehmen, ein wirksames Risikomanagementsystem zu etablieren. Aktuell hat die BaFin auch hierzu ein Rundschreiben zur Auslegung der Vorschriften über die Geschäftsorganisation mit Blick auf die IT-Infrastruktur veröffentlicht. Das Schreiben will einen praxisnahen Rahmen insbesondere für das Management der IT-Ressourcen, für das Informationsrisiko- und -sicherheitsmanagement vorgeben.[47]

3. Sicherheit personenbezogener Daten

Die DSGVO setzt ebenfalls Anforderungen an die Sicherheit der Verarbeitung von personenbezogenen Daten (Art. 25 Abs. 1 i.V.m. Art. 5 Art. 1 f), 32 DSGVO) und schreibt vor, dass Datenverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau für die Daten zu gewährleisten.[48] Verstöße gegen die neuen Vorgaben können empfindlich sanktioniert werden. Es drohen Geldbußen von bis zu 20 Mio. € bzw. im Falle eines Unternehmens 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist.[49] Gerade auch im Hinblick auf die Größenordnung der Bußgeldandrohung sollten Vorstände und Aufsichtsräte Prozesse etablieren, um die Einhaltung der Vorgaben sicherzustellen.[50]

4. IT-Sicherheit und Buchführung

Unternehmen sind zum Zwecke der Rechnungslegung und Erstellung der Jahresabschlüsse zum Führen von Handelsbüchern verpflichtet, § 238 HGB. IT-basierte Buchführung ist heutzutage die Regel. Für die interne und externe Revision muss sichergestellt werden, dass Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können, §§ 239 Abs. 4 Satz 2 , 146 Abs. 5 Satz 2 AO. Um diese Überprüfung gewährleisten zu können, hat die Geschäftsleitung für die erforderliche Datensicherheit Sorge zu tragen. Die Ausgestaltung dieser handels- und steuerrechtlichen IT-Sicherheitspflichten konkretisieren die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).[51]

5. EU-Verordnung über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik

Auch die EU-Kommission arbeitet an einer Strategie, die IT-Sicherheit in der EU zu stärken. Für Unternehmen ist dabei insbesondere der Vorschlag für eine Cybersecurity-Verordnung von Bedeutung.[52] Einer der Kernpunkte des Verordnungsvorschlags ist die Einführung eines EU-Rahmens zur Cybersicherheitszertifizierung, um sicherzustellen, dass Produkte der Informations- und Kommunikationstechnologie sowie entsprechende Dienste die dafür relevanten Cybersicherheitskriterien auf einheitliche Weise erfüllen. Das Inkrafttreten der Verordnung ist für 2019 avisiert.

IV. Publizitäts- und Meldepflichten

Das Thema Cybersecurity – und insb. Hackerangriffe oder Datenverluste – ist auch im Kontext von Veröffentlichungs- und Meldepflichten relevant.

Das IT-Sicherheitsgesetz regelt eine Meldepflicht gegenüber dem BSI bei Cyber-Attacken bzw. schwerwiegender Beeinträchtigung informationstechnischer Systeme, Komponenten und Prozesse. Diese Pflicht richtet sich an sämtliche Energieversorgungsnetzbetreiber. Weiter müssen Beeinträchtigungen von Telekommunikationsnetzen und -diensten sowohl an die Bundesnetzagentur als auch an das BSI gemeldet werden.

Auch aus der DSGVO ergibt sich eine Pflicht, die Verletzung des Schutzes personenbezogener Daten unverzüglich (möglichst binnen 72 Stunden) ab Bekanntwerden der Verletzung gegenüber der zuständigen Datenschutzbehörde zu melden. Diese Meldung ist nicht nur allgemeiner Natur, sondern soll nach Art. 33 DSGVO u.a. die Art der Verletzung, die ungefähre Zahl der Betroffenen, Name und Kontaktdaten des Datenschutzbeauftragten, die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgesehen Maßnahmen bezeichnen.

Daneben ist denkbar, dass die Tatsache eines Hackerangriffs oder auf kompromittierten IT-Systemen gespeicherte Informationen als relevante Insiderinformation i.S. der Marktmissbrauchsverordnung (MMVO) zu qualifizieren ist und so eine unverzügliche Offenlegung zu prüfen ist. Es ist nicht auszuschließen, dass durch einen Hackerangriff derart in die Prozesse eingegriffen wird, dass dies als solches eine Insiderinformation darstellt. Gleichzeitig können im Rahmen eines Hackerangriffs Insiderinformationen ausgespäht werden oder

47 Rundschreiben 10/2018 Versicherungsaufsichtliche Anforderungen an die IT (VAIT), abrufbar unter: http://hbfm.link/4105.

48 Vgl. Voigt, a.a.O. (Fn. 32) Rn. 312 ff.; Martini, in: Paal/Pauly, DSGVO/BDSG, 2. Aufl. 2018, Art. 25 Rn. 34 f.; Frenzel, in: Paal/Pauly, DSGVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 46 f.; Baumgartner, in: Ehmann/Selmayr, 2. Aufl. 2018, Art. 25 Rn. 11 ff.; Kramer/Meints, in: Auernhammer, DSGVO/BDSG, 6. Aufl. 2018, Art. 32 Rn. 1; Mantz, in: Sydow, Europäische Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 32 Rn. 1.

49 Vgl. zum Streit bzgl. des Unternehmensgriffs Punte/Rode, DB 2018 S. 2161; Faust/Spittka/Wybitul, ZD 2016 S. 120.

50 Ausführlich hierzu auch Behling, ZIP 2017 S. 697.

51 BMF vom 14.11.2014, BStBl. I 2014 S. 1450 = DB 2014 S. 2683; Goldsteyn/Thelen, DB 2015 S. 1126; Voigt, a.a.O. (Fn. 32), Rn. 61 f.

52 Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit") COM(2017) 477 final (BR Drs. 680/17).

diese fälschlich öffentlich zugänglich gemacht werden, so dass auch in diesem Fall über eine Veröffentlichungspflicht nachzudenken ist. Daher ist es wichtig, dass die Verantwortlichen im Unternehmen (insb. die Rechtsabteilung) im Notfallplan für den Fall eines Hackerangriffs eingebunden sind.

In den USA veröffentlichte die SEC am 01.02.2018 Richtlinien zu Offenlegungspflichten bei Cybersecurity Risiken und Vorfällen.[53] Nach den Richtlinien müssen Cybersecurity Vorkommnisse, die für Investoren relevant sind, umgehend veröffentlich werden. Diese Pflicht wird dadurch ergänzt, dass Notfallpläne solche etwaigen Veröffentlichungspflichten einbeziehen müssen und gegenüber Investoren die Informationen über die Rolle des Managements in Bezug auf die Überwachung von Cybersecurity Risiken offenzulegen sind. In der Veröffentlichung sind die jeweiligen Risiken spezifisch zu bezeichnen, eine allgemeine Information oder ein genereller Hinweis sind danach nicht ausreichend.

In Deutschland kann ein Bericht über Risiken, die sich aus IT-Sicherheitsvorfällen oder der Verletzung von Datenschutzpflichten ergeben, im Rahmen des Lageberichts ggf. angezeigt sein. Nach § 289 Abs. 1 Satz 4 HGB ist inhaltlich die voraussichtliche Entwicklung der Gesellschaft mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern. Um den Erfordernissen an die Vollständigkeit des Lageberichts gerecht zu werden, müssen insb. auch besondere Ereignisse während des Berichtszeitraumes aufgenommen werden. Cyber-Attacken oder Datenschutzverstöße könnten solche berichtswürdigen Umstände darstellen.[54] Der Geschäftsbericht 2017 der Deutschen Bahn AG, die maßgeblich von der Ransom-Software WannaCry betroffen war, behandelt ausführlich das IT-Sicherheitsmanagement des Unternehmens und beschreibt insb., welche Auswirkungen konkret WannaCry auf das Unternehmen hatte und wie darauf reagiert wurde.[55]

V. Umsetzung eines Cybersecurity Management Systems / Checkliste

Für die Implementierung eines Cybersecurity Management Systems hat der Vorstand zunächst unter Berücksichtigung von Art und Umfang des Unternehmens eine mit der Geschäftsstrategie konsistente IT-Strategie zu definieren, von der Zielsetzungen für ein Informationsrisiko- sowie Informationssicherheitsmanagement abzuleiten sind. Ausgangspunkt ist die Identifikation und Bewertung der relevanten IT-Risiken. Unter Beachtung von regulatorischen Vorgaben sowie in der Praxis bewährten Standards und Normen[56] sollten die technische Infrastruktur und Geschäftsprozesse entwickelt werden, die die identifizierten Risiken angemessen adressieren. Dazu ist die Schaffung eines organisatorischen Rahmens erforderlich. Die Infrastruktur und die Geschäftsprozesse sind in einer Prozessbeschreibung zu dokumentieren; die mit der IT-Sicherheit betrauten Mitarbeiter müssen sorgfältig ausgewählt, instruiert sowie überwacht werden. Außerdem müssen Kontroll- und Berichtsstrukturen geschaffen werden, die das Reporting an die fachliche Leitung und den Vorstand sicherstellen. Innerhalb des organisatorischen Rahmens müssen technische Maßnahmen wie der Schutz der IT-Systeme z.B. durch die Beschränkung von Zugangs- und Zugriffsrecht, Verschlüsselung, Virenschutz etc. festgelegt werden. Zudem sind Notfallkonzepte zu entwickeln, um im Schadens- oder Angriffsfall systemrelevante Geschäftsprozesse aufrechterhalten zu können. Das Cybersecurity Management System sollte einer regelmäßigen Überprüfung unterzogen und ggf. an neue Entwicklungen angepasst werden.[57]

Als Leitfaden für die Praxis zur Etablierung eines angemessenen Cybersecurity Management Systems sind in der nachfolgenden Checkliste wesentliche Aspekte zusammengefasst.[58] Ob und in welchem Umfang die jeweiligen Kriterien aufzugreifen sind, ist im Einzelfall abzuwägen.

Abb. 1: Checkliste

Früherkennung und Prävention	Policies
▪ Regelmäßige Cybersecurity Audits ▪ IT Security Response Team ▪ Notfallplan, inkl. Meldepflichten ▪ Wiederherstellungsplan ▪ Obligatorische Schulungen ▪ (Theoretische) Übungen ▪ Stress Tests ▪ Regelmäßiger Agendapunkt ▪ Cyber-Versicherung ▪ Technische Sicherheit ▪ Einbeziehen der Rechtsabteilung ▪ Zusammenarbeit mit Behörden ▪ Überprüfung von Vertragspartnern	▪ Passwörter ▪ Internetnutzung und Sozialen Medien ▪ Aufbewahrung von Dokumenten ▪ Datenschutz ▪ Verschlüsselung ▪ „Bring-your-own-device“
Personelle Organisation	
▪ Chief Information Officer (CIO) ▪ Privacy/Security Manager ▪ Chief Information Security Officer (CISO) ▪ Chief Risk Officer (CRO) ▪ Chief Privacy Officer (CPO) ▪ Chief Security Officer (CSO)	

VI. Fazit

Vorstand und Aufsichtsrat haben das Thema IT-Sicherheit regelmäßig in ihren Gremien zu diskutieren. Das Thema IT-Sicherheit ist insb. einhergehend mit einer Digitalisierung von weiteren Prozessen neu zu validieren. Ein ausgeprägtes IT-Risikobewusstsein angepasst auf die jeweilige Risikolandschaft im Unternehmen ist notwendiger Ausgangspunkt für Prävention und Notfallreaktion. Es muss eine Analyse der bestehenden Risiken durchgeführt und Schwachstellen aufgedeckt werden. Auch in personeller Hinsicht sollten Unternehmen den neuen Herausforderungen in Form einer Cyber-Organisation begegnen. Der Vorstand hat bei der Ausgestaltung der Organisation und Maßnahmen ein Ermessen. Wesentlich ist die Einholung umfangreicher Information – nicht zuletzt um eine etwaige Haftung auszuschließen.

Redaktionelle Hinweise:

Zum Thema IT-Sicherheit vgl. u.a. auch:

- *Spindler*, Zukunft der Digitalisierung – Datenwirtschaft in der Unternehmenspraxis, DB 2018 S. 41 = DB1259038;
- von *Baum/Appt/Schenk*, Die vernetzte Fabrik: Rechtliche Herausforderungen in der Industrie 4.0 (Teil 2), DB 2017 S. 1888 = DB1245830.

53 Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746.

54 Für die umfassende Behandlung datenschutzrechtlicher Aspekte, insb. vor dem Hintergrund der DSGVO, Keppeler/Berning, ZD 2018 S. 157 (160); zum Begriff des Risikos vgl. Lange, MünchKomm-HGB, 3. Aufl. 2013, § 289 Rn. 77, 80 f.

55 Deutsche Bahn Konzern, Integrierter Bericht 2017, S. 154 f.

56 Bspw. ISO/IEC 27001, https://www.iso.org/standard/54534.html.

57 Vgl. zur Implementierung eines Cybersecurity Management Systems Voigt, a.a.O. (Fn. 32), Rn. 160 ff.

58 Angelehnt an ACC Foundation: The State of Cybersecurity Report, An In-House Perspective (2018), S. 8.