Cybersecurity und Unternehmensleitung

Gerald Spindler

A. Einleitung

IT-Sicherheit oder Cybersecurity hat nach langen Jahren inzwischen die Ebene der Top-Etagen des Managements als Thema erobert. Kaum noch ein Unternehmen kommt heute ohne massive IT-Unterstützung aus; gerade in Zeiten der Covid-19-Pandemie hat sich die Bedeutung der Digitalisierung massiv verstärkt. Umso wichtiger erscheint es, wo und wie das Thema „Cybersecurity" behandelt wird, insbesondere dass es nicht mehr zur Nebensache erklärt werden kann, sondern als eines der „Chef"-Themen angesehen werden muss.

Um diese grundsätzliche Aussage zu untermauern, bedarf es zunächst eines Blicks auf mögliche Angriffsszenarien und das damit verbundene Bedrohungs- und Gefährdungspotenzial für das Unternehmen (B.). Daran schließen sich Grundlegungen für die Pflichten der Geschäftsleitung an (D.), die dann schließlich bezogen auf die IT-Sicherheit konkretisiert werden (E.).*

B. Grundlagen: Cybersecurity und Bedrohungspotentiale

Die möglichen Schadensbilder, die sich aus einer Tätigkeit im IT-Bereich ergeben können, sind vielfältig. Aus der bisherigen Schadenserfahrung lässt sich allerdings auf bestimmte Risikokategorien schließen: Zu unterscheiden sind einerseits „technische" Risiken, wie unbefugte Eingriffe in Systeme, Schadsoftware, Systemfehler, Fehlbedienung, Falschberatung und das Ausspähen von Informationen und andererseits Risiken, die sich in erster Linie aus Inhalten im Internet ergeben, wie Verletzung der Privatsphäre, Beleidigung, Verleumdung, Wettbewerbsverstöße und die Verletzung geistigen Eigentums (Schutzrechte). Letztere können zwar ebenfalls bedeutsame Haftungsrisiken für eine Gesellschaft entfalten, werden hier

allerdings nicht näher behandelt, da sie nicht zum engeren Kreis der Cybersecurity-Risiken gehören.*

I. Unbefugte Eingriffe in Systeme (Hacking)

Eine ernste Gefahr für Unternehmen sind Schäden, die durch unbefugte Eingriffe in Systeme verursacht werden. Solche Schäden sind häufig durch mangelnde Sicherheitsvorkehrungen bedingt. Hier liegt ein erhebliches Risiko nicht allein für die eigenen Systeme, sondern auch eine Gefährdung für Dritte, wenn etwa der eigene Rechner zum Angriff auf Dritte missbraucht wird oder wenn im eigenen System gespeicherte Daten Dritter beschädigt werden. In solchen Fällen der Drittschädigung stellt sich die Frage der Haftung. Dabei ist jedoch zu berücksichtigen, dass praktisch jedes genutzte IT-System Schwachstellen aufweist – insbesondere die eingesetzte Software – und deswegen selbst stark gesicherte Systeme niemals zu 100 % vor unbefugten Eingriffen geschützt werden können.

Unbefugte Eingriffe in Systeme können als interne Angriffe aus dem Unternehmen selbst erfolgen oder als Angriffe von außen. Das interne, also von eigenen Mitarbeitern ausgehende Risiko, gilt gemeinhin als eine unterschätzte Gefahr.[1] Es ist deshalb besonders schwerwiegend, weil der entsprechende Schutz umfangreiche Vorkehrungen erfordert. Rein technische Lösungen, wie sie sich für die Abschirmung nach außen anbieten, genügen hier nicht. Ein Risiko stellen dabei nicht nur böswillige, sondern auch unvorsichtige Mitarbeiter dar.[2] Die allgemein angespannte Sicherheitssituation wird durch die verstärkte Fremdvergabe sicherheitsrelevanter Aufgaben noch verschärft. Wird etwa aus Kosten- oder Kapazitätsgründen ein externer Dienstleister eingebunden, dann erschwert dies die Kon-

---

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag beruht, ist abrufbar unter https://doi.org/10.17176/20201218-121603-0.

Vgl. nur Art. 2 Nr. 1 und 8 des „Cybersecurity Act" der Europäischen Union vom 17.04.2019, Verordnung (EU) 2019/881, ABl. L 151/15, der Cybersecurity allgemein als „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen" definiert, wobei der Begriff der Cyberbedrohung „einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung [beschreibt], der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte".

1 Dazu *BSI*, Top 10 Bedrohungen und Gegenmaßnahmen, 2019, S. 5 ff.

2 Das klassische Beispiel hierfür ist das mit einem Notizzettel am Bildschirmrand für jeden sichtbar befestigte Passwort für den Systemzugang.

trolle der vorhandenen Sicherheitsvorkehrungen und dementsprechend auch das Entdecken von Sicherheitslücken.

Externe Angriffe drohen etwa in Form von sog. Hackerangriffen.[3] In schädigender Absicht handelnde Hacker sind eine Gefahr für alle Unternehmen, deren IT-Systeme auch von außen her zugänglich sind, was praktisch häufig und mit nach wie vor zunehmender Tendenz der Fall ist.[4] Die Motivation von Hackerangriffen kann durchaus unterschiedlich sein, doch ist der Anteil der Angriffe, die gezielt bestimmten Unternehmen gelten, hoch. Eine weitere Spielart böswilliger Angriffe von außen sind die sogenannten **Distributed Denial of Service Attacks** (DDoS), welche etwa die Internetverbindungen der angegriffenen Unternehmen durch gezielte Überlastung zum Erliegen bringen.[5] Bereits eine kurzfristige DDoS-Attacke auf ein Unternehmen kann dieses allein an Arbeitszeit für EDV-Administratoren hohe Summen kosten.

Mit Blick auf mögliche **Haftungsansprüche**[6] sind unbefugte Eingriffe eine besondere Gefahr für solche Unternehmen, die für die Sicherheit der IT-Systeme bzw. Daten anderer einzustehen haben, sei es als Lieferanten von Software bzw. Systemkomponenten oder als Dienstleister. Stellt sich bei einem Drittschaden heraus, dass die erforderlichen Sicherheitsvorkehrungen nicht oder unzureichend getroffen wurden, so rückt die Haftungsfrage in Gestalt von Regressansprüchen ins Bild. Die böswilligen Verursacher der Schäden, etwa Hacker, stehen dabei als Haftungsschuldner in der Regel nicht zur Verfügung.

---

3 Die Kriminalstatistik 2019 unterscheidet zwar nicht zwischen externen und internen Eingriffen, führt aber 3.183 Fälle (2018: 2.875 Fälle) von Datenveränderung bzw. Computersabotage auf, von denen auch zumindest ein gewisser Anteil auf Angriffe durch böswillig handelnde Hacker zurückzuführen sein wird.

4 S. dazu *Gaycken/Karger*, MMR 2011, 3, die für einen Paradigmenwechsel weg von der Vernetzung und hin zur Entnetzung in Bezug auf gewisse Systeme plädieren.

5 Dazu *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, S. 29; Auer-Reinsdorff/Conrad/*Schmidt/Pruß*, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 3 Rn. 271; Ernst/*Pierrot,* Hacker, Cracker & Computerviren, 2004, Rn. 128 ff.; siehe schon *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI), 2007, Rn. 87 ff.

6 S. dazu *Schmidt-Versteyl*, in diesem Band, II.

II. Schadsoftware

Wie beim Hackerangriff ist auch der Befall durch Schadsoftware zunächst ein Problem des primär betroffenen Unternehmens selbst. Schadsoftware kommt z.B. vor als Computervirus, Trojaner oder Backdoor[7]. Verbreiten sich diese allerdings weiter – häufig durch unzureichende Schutzvorkehrungen – und schädigen Dritte, dann stellt sich die Haftungsfrage.[8] Oft ereignet sich die Infizierung eines Systems mit bzw. die Verbreitung der Viren über das Internet, insbesondere über E-Mails. Hierbei wird von Kriminellen in vielen Fällen die Methode des Phishings verwendet. Dabei wird eine E-Mail und ggf. auch eine darin verlinkte Website so gestaltet, dass sie den Anschein erweckt, von einem anderen vertrauenswürdigen Absender zu stammen, etwa einer Bank oder einem Zahlungsdienstleister. Die Kriminellen erhoffen sich davon, dass der Empfänger in seinem Vertrauen auf die Echtheit der Mail einen schädlichen Anhang herunterlädt oder etwa Passwörter und andere wichtige Informationen preisgibt.[9]

Dieser Verbreitungsweg ist allerdings weder die einzige noch die vorherrschende Art der Ausbreitung von Schadsoftware. Verbreitungsquellen für Viren sind vielmehr etwa auch Originalsoftware, vorinstallierte Software auf vertriebener Hardware, Wartungs- und Servicepersonal sowie Anwender. Häufig begünstigen bestimmte, gerade massenweise genutzte

---

7 Trojanische Pferde sind Programme, „mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer", so die Definition des BSI, https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/T/Trojanisches_Pferd.html?nn=132116, (abgerufen am 05.07.2021); Backdoors sind nach der Definition des BSI „Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, beispielsweise um Angriffsspuren zu verstecken", https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132804, (abgerufen am 05.07.2021), s. Hintertür.

8 Dazu *Spindler*, in: Hornung/Schallbruch, IT-SicherheitsR-HdB, 2021, § 12 Rn. 23 ff.; *Riehm/Meier*, MMR 2020, 571, 573; *Habbe/Gergen*, CCZ 2020, 281, 283 f.; *Koch*, Versicherbarkeit von IT-Risiken, 2005, Rn. 375 ff.; *Libertus,* MMR 2005, 507 ff.

9 *Schmidt/Pruß* (Fn. 5), § 3 Rn. 274; zur Haftung bei Phishing etwa OLG Zweibrücken MMR 2010, 346; zu aktuellen Phishing-Methoden in Zeiten der Covid-19-Pandemie *Bou Sleiman/Gerdemann*, International Cybersecurity Law Review 2, 37 (2021).

Computerprogramme Schadsoftware in besonderer Weise; was insbesondere der Fall ist, wenn sie in hohem Maße Schwachstellen aufweisen, welche die Verbreitung erleichtern.[10] Ein besonderes Haftungsrisiko im Zusammenhang mit der Verbreitung von Schadsoftware haben neben Firmen, die Software produzieren, Unternehmen, die Arbeiten an Systemen Dritter vornehmen. Auf der Seite des Geschädigten wird bei der Verbreitung von Schadsoftware allerdings regelmäßig die Frage eines Mitverschuldens zu berücksichtigen sein, da darauf ausgerichtete, angemessene Vorkehrungen angesichts der allgemein bekannten Gefährdung heutzutage als Selbstverständlichkeit zu betrachten sind[11].

Ein besonderer Fall der Schadsoftware betrifft die sog. Ransomware oder Erpressungssoftware. Diese Art der Schadsoftware wird von Kriminellen dazu verwendet, vom Nutzer des infizierten Geräts Geld für die Entfernung der Schadsoftware bzw. für die Freigabe des Systems zu erpressen. Die Herangehensweisen sind dabei vielfältig und reichen von einem angeblichen Anti-Virus-Programm, das häufig falsche und störende Warnmeldungen sendet, über Software, die das gesamte System oder einzelne wichtige Dateien sperrt und nur gegen Zahlung eines Geldbetrags wieder freigibt.[12] Die Zahlung soll dabei häufig in Bitcoin oder einer anderen nicht rückverfolgbaren Kryptowährung erfolgen.[13] Ransomwareangriffe sind insbesondere seit 2016 ein vermehrt auftretendes Phänomen.[14] Kürzlich aufgetretene Beispiele für Ransomwareangriffe sind etwa die Software „Ryuk", die durch E-Mail-Anhänge übertragen wurde und von 2018 bis 2020 einen Schaden von über 50 Mio Euro verursacht hat,[15] oder der seit 2017 ebenfalls per Mail verbreitete Virus WannaCry, der weltweit über

10 *Raue*, NJW 2017, 1841, 1842; BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 11 ff.; zu den Schwachstellen *Rafsendjani/Bomhard*, in: Hornung/Schallbruch IT-SicherheitsR-HdB, 2021, § 9 Rn. 155 f.

11 Hornung/Schallbruch/*Rafsendjani/Bomhard* (Fn.), § 9 Rn. 76 ff; Kipker/*Lapp*, Cybersecurity, 2020, Kapitel 8 Rn. 149; vgl. *Raue* (Fn.), 1842.

12 Näher zur Funktion s. *Kaspersky*, What is Ransomware, https://www.kaspersky.com/resource-center/definitions/what-is-ransomware, (abgerufen am 05.07.2021).

13 *Möllers*, in: Möllers, Wörterbuch der Polizei, Ransomware; *Vogelgesang/Möllers*, jM 2016, 381 ff.

14 Statista, Number of ransomware attacks per year 2014–2019, https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (abgerufen am 05.07.2021).

15 *Malwarebytes*, Ryuk Ransomware, https://www.malwarebytes.com/ryuk-ransomware/ (abgerufen am 05.07.2021).

200.000 Systeme befiel.[16] Indem für einen „erfolgreichen" Angriff mit Ransomware vergleichsweise wenig technische und organisatorische Ressourcen notwendig sind, stellt Ransomware eine der verbreitetsten Arten der Schadsoftware dar.[17]

III. Systemfehler, Fehlbedienung, Falschberatung

Neben böswillig herbeigeführten Beschädigungen sind Schäden an IT-Systemen häufig die Folge von Systemfehlern, Fehlbedienung, falscher Unterweisung etc. Werden dabei Dritte geschädigt, dann kommen Haftungsansprüche in Betracht. Betroffen sein können insbesondere Unternehmen, die Systemkomponenten an andere liefern, Arbeiten an fremden Systemen durchführen oder sonstige Dienstleistungen erbringen. Ein besonderer Schwerpunkt solcher Vorkommnisse liegt im Bereich der Beschädigung oder versehentlichen Löschung von Daten. Haftungsfälle infolge von Drittschäden durch Datenverlust ereignen sich in mannigfaltiger Weise, etwa bei Versagen eines nicht hinreichend getesteten Datensicherungsprogramms[18], durch unzureichende Installation eines Datensicherungssystems[19], Überlassung veralteter Datenbestände als „Datensicherung" an Auftraggeber[20] oder den fehlenden Hinweis in einer Software-Dokumentation auf die Möglichkeit eines Datenverlustes[21]. Allerdings ist bei der Beurteilung der Haftung regelmäßig die Frage eines möglichen Mitverschuldens des Geschädigten zu prüfen. Die Datensicherung im eigenen System gehört heute für alle Unternehmen zum selbstverständlichen Bestandteil eines ordnungsgemäßen IT-Riskmanagements, für dessen Einhaltung die Geschäftsleiter zu sorgen haben und auf deren Vorliegen sich Dritte verlassen können.[22]

---

16 *Kaspersky*, What is WannaCry ransomware, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (abgerufen am 05.07.2021).

17 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018, Rn. 300 f.

18 BGH NJW 1996, 2924.

19 LG Detmold CR 1999, 689.

20 OLG Köln NJW-RR 1997, 558; OLG Hamm MMR 2004, 487.

21 OLG Hamm CI 1999, 28.

22 Vgl. AG Bonn BeckRS 2016, 5850; OLG Koblenz CR 2010, 704 (705); OLG Hamm MMR 2004, 487; OLG Karlsruhe NJW-RR 1997, 554; OLG Düsseldorf MMR 2015, 237 ließ die Frage offen, während die Vorinstanz LG Duisburg MMR 2014, 735 (735) sie bejahte; dazu auch *Habbe/Gergen* (Fn.), 283 f.; s. ferner *Spindler* (Fn. 5), Rn. 327, zu den Geschäftsleiterpflichten Rn. 336 ff.; *Heydn*, in: Schus-

IV. Ausspähen von Informationen

Auch das Ausspähen von Informationen kann zu Schäden und Haftungsansprüchen führen.[23] Von dem Schaden hinsichtlich eigener Daten abgesehen, sind Drittschäden insbesondere in zwei Konstellationen denkbar: entweder speichert ein Unternehmen in den eigenen Systemen Daten Dritter, die dann in die falschen Hände gelangen, oder ein Unternehmen ist als Dienstleister für Dritte tätig und durch Fehler bei dieser Tätigkeit werden dem Dritten Informationen ausgespäht. Eine ungenügende Absicherung von Systemen kann im Rahmen einer Haftungsprüfung Indiz für ein gegebenes Verschulden sein, insbesondere wenn entsprechende Sicherheitslösungen ohne Weiteres verfügbar sind. Als mögliche Schäden ist hier unter anderem an den Missbrauch von Daten – etwa der Kreditkarteninformationen – zu denken. Aber auch der Wert der Daten als solcher, bspw. von Kundendaten oder Firmengeheimnissen etwa im Bereich von Daten über technische Neuentwicklungen, ist nicht zu unterschätzen.[24] Finanzielle Verluste in diesem Bereich sind allerdings teilweise schwierig zu beziffern.

C. Rechtliche Rahmenbedingungen für Cybersecurity

Die rechtlichen Rahmenbedingungen für ein umfassendes Regelwerk für Cybersecurity fehlen bislang noch, sowohl auf europäischer als auch auf nationaler Ebene.[25] Das BSI-Gesetz enthält nur für die Betreiber von kritischen Infrastrukturen, die in § 2 X BSIG bzw. in der KRITIS-V näher spezifiziert werden[26], in §§ 8a ff. BSIG etliche Regelungen, insbesondere die grundlegende Anforderung, dass der Betreiber „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der

---

ter/Grützmacher, IT-Recht, 2020, § 254 BGB Rn. 11 ff.; *Hörl,* ITRB 2014, 111, 112; *v. Holleben/Menz,* CR 2010, 63.

23 Die Kriminalstatistik 2019 führt 9.926 Fälle (2018: 8.762 Fälle) des Ausspähens von Daten einschl. Vorbereitungshandlungen (§§ 202a, 202b, 202c StGB) auf.

24 Ein aktuelles Beispiel stellen Cyberangriffe zur Erlangung medizinischer Forschungsdaten für die Entwicklung von Covid-19-Impfstoffen dar, s. etwa https://www.theguardian.com/world/2020/dec/09/hackers-accessed-vaccine-documents-in-cyber-attack-on-ema (abgerufen am 05.07.2021).

25 S. auch den Überblick bei *Schmidt-Versteyl*, NJW 2019, 1637, 1639.

26 BSI-Kritis-V vom 22.4.2016, BGBl. 2016 I 958, geändert durch Art. 1 Erste ÄndVO vom 21.6.2017, BGBl. I 1903.

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme" gemäß dem „Stand der Technik" zu treffen hat.[27] Die technische Konkretisierung dieser und anderer unbestimmter Rechtsbegriffe stellt die Praxis naturgemäß vor einige Herausforderungen.[28]

Auf europäischer Ebene kommt der sog. Cybersecurity Act in Gestalt der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)[29] hinzu; allerdings ist dieser in der niedrigsten Stufe auf eine freiwillige Zertifizierung ausgerichtet und bedarf auch für die höheren Vertrauensstufen vor allem eines auszufüllenden Referenzrahmens, der soweit ersichtlich noch im Aufbau begriffen ist.

Hinzu kommen für den Bereich personenbezogener Daten die Pflichten der DSGVO,[30] hier insbesondere die generelle Pflicht nach Art. 32 DSGVO zu „angemessenen technischen und organisatorischen Maßnahmen" sowie die Pflicht zur Mitteilung von Datenschutzverletzungen (insbes. sog. Dataleaks) gem. Art. 33 DSGVO.

Konkretisiert werden diese Anforderungen im Wesentlichen im sog. Grundschutzkatalog des BSI sowie in den Normungen der ISO 27000er Reihe. Letztere bezieht sich aber ähnlich dem Grundansatz des Qualitätsmanagements in der ISO 9.000er Reihe auf den Aufbau und Ablauf von Managementsystemen, enthält also weitgehend keine technischen Standards.[31] In ähnlicher Weise befasst sich der Grundschutzkatalog des BSI mit organisatorischen und prozessualen Elementen der IT-Sicherheit.[32]

Für besonders regulierte Branchen wie der Telekommunikationsbranche greifen Sonderregelungen ein, hier § 109 TKG, wonach der TK-Diensteanbieter die erforderlichen technischen Schutzmaßnahmen zu treffen hat, aber vor allem für den Finanzsektor in Gestalt der Banken – hier § 25a

27 Hierzu *Fischer*, in: Hornung/Schallbruch, Handbuch IT-Sicherheitsrecht, 2021, § 13 Rn. 65 ff.
28 Vgl. etwa *Kipker/Harner/Müller*, InTeR 2018, 24, 25 f. Zum Ermessen des Vorstands bei der Interpretation unbestimmter Rechtsbegriffe, s. unten unter C. 2.
29 Amtsblatt L 151 vom 7.6.2019, S. 15 ff., im Folgenden mit CSA-VO abgekürzt.
30 Eingehender Überblick bei *König,* AG 2017, 262, 263 ff. m.w.N.
31 *Jendrian*, DuD 2014, 552, 554; *Rost/Sowa,* DuD 2020, 659, 660 f.
32 *Djeffal*, MMR 2019, 289; *Alt,* DS 2020, 169,171; *Schmidl,* in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 121.

KWG – und der Versicherungen – hier § 26 VAG – treten besondere Konkretisierungen hinzu. So hat die BaFin erst 2017 aus den allgemeinen MaRisk angesichts der zunehmenden Bedeutung der IT ein eigenes Rundschreiben zu „Bankaufsichtsrechtlichen Anforderungen an die IT (BAIT)" herausgebracht.[33]

D. Pflichten der Unternehmensleitung

Vor diesem Hintergrund des rechtlichen Umfelds sind die Pflichten der Unternehmensleitung näher zu beleuchten.

I. Grundlagen der Sorgfaltspflicht

Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, § 93 Abs. 1 S. 1 AktG. Der Vorstand hat hierbei nicht nur die erwerbswirtschaftlichen Interessen der Gesellschaft, sondern auch die Interessen der Aktionäre und Gläubiger sowie das Wohl der Arbeitnehmer und der Allgemeinheit zu berücksichtigen.[34] Solange keine Anhaltspunkte für eine sorgfaltswidrige Geschäftsführung vorliegen, ist ein Vorstandsmitglied trotz des Grundsatzes der Gesamtverantwortung nicht verpflichtet, Aufsichtsmaßnahmen in Bezug auf ein Nachbarressort zu ergreifen.[35] Unter der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters ist eine Sorgfalt zu verstehen, wie sie ein Geschäftsleiter, der ein Unternehmen unter eigener Verantwortung leitet, anzuwenden hat, insbesondere als Treuhänder fremder Vermögensinteressen.[36] Die Anforderungen an die Sorgfaltspflicht be-

---

33 *BaFin*, Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderung an die IT (BAIT) vom 6.11.2017, zuletzt geändert am 14.09.2018, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html (abgerufen am 05.07.2021).

34 *Spindler,* in: MüKo AktG, 5. Aufl. 2019, § 76 Rn. 64 ff., 62 m.w.N.

35 BGH NJW 2019, 1067 (1068 ff.); BGHZ 133, 370 (378 f.) (jeweils für die Geschäftsführer einer GmbH); OLG Köln NZG 2001, 135; OLG Hamburg AG 2001, 141 (144); OLG Köln AG 2000, 281 (284); *Koch,* in: Hüffer/Koch AktG, 14. Aufl. 2020, § 93 Rn. 42; *Mertens/Cahn,* in: Kölner Komm AktG, 3. Aufl. 2009, § 93 Rn. 92.

36 BGHZ 129, 30 (34) (für den Geschäftsführer einer GmbH); OLG Düsseldorf AG 1997, 231 (235); OLG Hamm AG 1995, 512 (514); OLG Koblenz ZIP 1991, 870 (871); *Böttcher*, NZG 2009, 1047, 1049; *Krause*, BB 2009, 1370,1371; *Mertens/Cahn*

messen sich nicht nach einem einheitlichen festen Maßstab, sondern bestimmen sich nach der Art und Größe des Unternehmens, der Zahl der Beschäftigten, der Konjunkturlage, den Zeitverhältnissen sowie den besonderen Aufgaben des einzelnen Mitglieds.[37] Um den Anforderungen zu genügen, müssen die Vorstandsmitglieder die Fähigkeiten und Kenntnisse besitzen, die zur Wahrnehmung ihrer Leitungsaufgabe erforderlich sind.[38] So ist die Sorgfaltspflicht des Vorstandsmitglieds eines Bankunternehmens[39] naturgemäß eine andere als die eines Industrie- oder Versorgungsunternehmens; dies gilt insbesondere auch für IT-Unternehmen oder solche mit stark IT-geprägter Tätigkeit.

Nach wie vor offen ist, welche Bedeutung die Befolgung bestimmter betriebswirtschaftlicher Management- oder Organisationsmodelle für die Frage der Pflichtwidrigkeit nach § 93 I, II AktG hat.[40] Sie können durchaus zur Konkretisierung des Pflichtenprogramms herangezogen werden.[41] Indes können betriebswirtschaftliche Standards nicht *per se* in rechtliche Verbindlichkeiten umgemünzt werden, da der Pflichtenumfang eine rechtliche Einordnung darstellt und keine betriebswirtschaftliche Praktikabilitätserwägung ist.[42] Dafür weisen derartige Grundsätze entweder einen zu hohen Abstraktionsgrad auf oder sie können nicht auf alle Unternehmens-

---

(Fn. 35), § 93 Rn. 10; *Koch* (Fn. 35), § 93 Rn. 6; *Eckert* in Wachter AktG, 3. Aufl. 2018, § 93 Rn. 6; *Dauner-Lieb,* in: Henssler/Strohn GesR, 5. Aufl. 2021, § 93 Rn. 7.

37 Ebenso *Fleischer,* in: BeckOGK AktG, 15.01.2020, § 93 Rn. 55; *Hopt/Wiedemann,* in: Hirte/Mülbert/Roth GroßkommAktG, Band 3, 5. Aufl. 2015, § 93 Rn. 58; *U. Schmidt,* in: Heidel NK-AktG, 5. Aufl. 2020, § 93 Rn. 75 f.; *Hölters,* in: Hölters AktG, 3. Aufl. 2017, § 93 Rn. 26; *Liebscher* in BeckHdB der AG, 3. Aufl. 2018, § 6 Rn. 130; *Böttcher* (Fn. 36), 1050.

38 *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 59; *Mertens/Cahn* (Fn. 35), § 93 Rn. 136 f.; *Hölters,* in: Hölters (Fn. 37), § 93 Rn. 27; *Goette,* in: Hommelhoff/Hopt/v. Werder HdB Corporate Governance, 2. Aufl. 2010, S. 719.

39 Vgl. hierzu *Hopt,* ZIP 2013, 1793, 1793 ff.

40 Für Konkretisierung *Groß/Amen*, WPg 2003, 1161, 1176 ff. Zu den Grundsätzen ordnungsmäßiger Unternehmensführung, *v. Werder*, ZfbF Sonderheft 36/1996, 1, 27 ff.

41 So vor allem *v. Werder*, Organisationsstruktur und Rechtsnorm, 1986, S. 98 ff.; *ders.*, DB 1987, 2265, 2265 ff.; *ders*., DB 1999, 2221, 2221 ff. für die Arbeit des Aufsichtsrates; *ders*., ZGR 1998, 69; *Grundei/v. Werder*, AG 2005, 825, 828 ff.; *Arbeitskreis „Externe und interne Überwachung der Unternehmung" der Schmalenbach Gesellschaft für Betriebswirtschaftslehre eV*, DB 2006, 2189, 2193 ff.; ausführlich zu den betriebswirtschaftlichen Grundsätzen ordnungsgemäßer Unternehmensleitung s. *v. Werder* (Fn. 40), 27 ff.

42 *Theisen*, ZGR 2013, 1, 16 f.

situationen übertragen werden.[43] Dies gilt auch für Normungen des Managementsystems, wie sie die ISO in den letzten Jahren zunehmend verabschiedet hat, insbesondere auch im IT-Bereich mit der ISO 27001 ff. Normenreihe. Im Grundsatz muss auch hier das Leitungsermessen des Vorstands eingreifen, so dass er nicht verpflichtet ist, ein bestimmtes betriebswirtschaftliches Managementsystem bzw. -modell oder eine Normung zu wählen, sofern es sich um eine vertretbare, sachlich begründete Wahl handelt.

Daraus folgt aber auch umgekehrt, dass die Befolgung eines bestimmten Managementsystems oder einer Normung keine Vermutungswirkung erzeugen kann, die die Darlegungs- und Beweislastregel des § 93 II AktG aushebeln könnte. Vielmehr obliegt es dem Vorstand, darzulegen und nachzuweisen, ob die Wahl eines Managementsystems den besonderen Bedingungen ihres Unternehmens entspricht.[44] Normungen sind allerdings nicht ohne jede Wirkung: Der Vorstand muss sich mit ihnen auseinandersetzen und gegebenenfalls klären, ob bzw. warum man der Normung folgt oder nicht und welche Modifikationen erforderlich sind. Unterlässt er eine solche Auseinandersetzung, gerät der Vorstand leicht in Gefahr, die Voraussetzungen der Business Judgment Rule nach § 93 I S. 2 AktG, namentlich der ordnungsgemäßen Informationsbasis, nicht zu erfüllen.

II. Business Judgment Rule

Auch Entscheidungen der Geschäftsleitung über IT-relevante Fragen fallen in den Bereich der Business Judgment Rule – die für den GmbH-Geschäftsführer ebenfalls Anwendung findet. § 93 I S. 2 AktG greift seinem Wortlaut nach nur, wenn es sich um unternehmerische Entscheidungen handelt;[45] diese sind durch ihre Zukunftsbezogenheit, insbesondere Prog-

---

43 Wie hier auch *Mertens/Cahn* (Fn. 35), § 111 Rn. 36; *Fleischer* (Fn. 37), § 93 Rn. 68; *Semler*, Leitung und Überwachung, 1996, Rn. 86 ff.; *v. Schenck*, NZG 2002, 64, 66; aA. *Kort* GroßkommAktG, Band 4/1, 5. Aufl. 2015, vor § 76 Rn. 12.

44 Zur Beweislast bei § 91 Abs. 2 AktG: OLG Celle OLGR 2009, 180 (181) = AG 2008, 711 (712); *Mertens/Cahn* (Fn. 35), § 91 Rn. 39; *Fleischer* (Fn. 37), § 91 Rn. 23; *Bitz*, Risikomanagement nach KonTraG, 2000, S. 4; *Spindler*, in: Fleischer VorstandsR-HdB, 1. Aufl. 2006, § 19 Rn. 66.

45 S. dazu etwa *S. H. Schneider*, DB 2005, 707, 707 ff.; *Fleischer*, ZIP 2004, 685, 690; *Schäfer*, ZIP 2005, 1253, 1255 ff.; *Gehb/Heckelmann*, ZRP 2005, 145, 146; *Seibt/Wollenschläger*, DB 2009, 1579, 1579; *U. H. Schneider*, DB 2011, 99, 100; *Weber-Rey/Buckel*, AG 2011, 845, 849.

nosen sowie das Eingehen von Risiken geprägt.[46] Unternehmerische Entscheidungen können hierbei nicht nur durch positives Tun getroffen werden, sondern auch durch Unterlassen einer Geschäftschance, etwa weil der Geschäftsleiter die Chancen-Wahrnehmung als zu riskant erachtet.[47] Gerade Entscheidungen über Investitionen in neue Technologien,[48] insbesondere in neue IT-Produkte ebenso wie deren Einsatz im Unternehmen, sind von einer Prognose bestimmt und zählen zu den unternehmerischen Entscheidungen. Ausgeschlossen von der Business Judgment Rule sind Treuepflichten ebenso wie die Einhaltung gesetzlicher Pflichten;[49] insbesondere

---

46 Begr. RegE UMAG BT-Drucks. 15/5092, S. 11; *Koch* (Fn. 35), § 93 Rn. 6 f.; s. bereits *Johannes Semler*, Entscheidungen und Ermessen im Aktienrecht, in: Habersack/Hüffer/Hommelhoff/Schmidt (Hrsg.), Festschrift für Peter Ulmer zum 70. Geburtstag, 2003, 627, 627 f.; *Hommelhoff*, Die Konzernleitungspflicht: Zentrale Aspekte eines Konzernverfassungsrechts, 1982, S. 171; ähnlich *Ihrig*, WM 2004, 2098, 2104: Keine eindeutige Beurteilung möglich, was richtig und was falsch ist; *Baums*, ZGR 2011, 218, 223; *Fleischer*, NZG 2008, 371; *ders*., NZG 2011, 521, 522; der Unsicherheit wenig Relevanz zusprechend *v. Falkenhausen*, NZG 2012, 644, 646; *S. H. Schneider* (Fn. 45), 708; *Grundei/v. Werder* (Fn. 41), 833; zur näheren Umschreibung des Risikobegriffs *Baums*, ZGR 2011, 218, 222 ff.

47 *Kock/Dinkel*, NZG 2004, 441, 443; *S. H. Schneider* (Fn. 45), 712; *Fleischer* (Fn. 37), § 93 Rn. 97; *Mertens/Cahn* (Fn. 35), § 93 Rn. 22; *Bürgers,* in: Bürgers/Körber/Bürgers AktG, 4. Aufl. 2017, § 93 Rn. 15; *M. Roth*, Unternehmerisches Ermessen und Haftung des Vorstandes, 2001, S. 109 f.; *Paefgen*, AG 2004, 245, 251; zum Unterlassen als unternehmerische Entscheidung im Allgemeinen *Jean Nicolas Druey*, Standardisierung der Sorgfaltspflicht? Fragen zur Business Judgment Rule, in: Habersack/Hommelhoff (Hrsg.), Festschrift für Wulf Goette zum 65. Geburtstag, 2011, 57, 66.

48 BGHZ 175, 365 (368) Tz. 11 ff. = NZG 2008, 389 Tz. 11 ff.; *Peter Kindler*, Vorstands- und Geschäftsführerhaftung mit Augenmaß – Über einige neuere Grundsatzentscheidungen des II. Zivilsenats des BGH zu §§ 93 AktG und 43 GmbHG, in: Habersack/Hommelhoff (Hrsg.), Festschrift für Wulf Goette zum 65. Geburtstag, 2011, 231, 232.

49 Begr. RegE BT-Drucks. 15/5092 S. 11, Stellungnahme BReg ebd. S. 41; *Koch* (Fn. 35), § 93 Rn. 6 f.; *U. Schmidt* (Fn. 37), § 93 Rn. 83; *Fleischer* (Fn. 45), 690; *S. H. Schneider* (Fn. 45), 708; *Spindler*, AG 2011, 725, 726; *v. Falkenhausen* (Fn. 46), 645; *Fleischer* (Fn. 37), § 93 Rn. 85; *Langenbucher*, DStR 2005, 2083, 2085; *Marcus Lutter*, Verhaltenspflichten von Organmitgliedern bei Interessenkonflikten, in: Hommelhoff/Rawert/K. Schmidt (Hrsg.), Festschrift für Hans-Joachim Priester zum 70. Geburtstag, 2007, 417, 423; *Carsten Jungmann*, Die Business Judgment Rule – ein Institut des allgemeinen Verbandsrechts? – Zur Geltung von § 93 Abs. 1 Satz 2 AktG außerhalb des Aktienrechts, in: Bitter/Lutter/Priester u.a. (Hrsg.), Festschrift für Karsten Schmidt zum 70. Geburtstag, 2009, 831, 843 f.; *Frank Kebekus/Wolfgang Zenker*, Business Judgment Rule und Geschäftsleiterermessen – auch in Krise und Insolvenz?, in: Grunewald/Westermann (Hrsg.), Festschrift für Georg Maier-Reimer zum 70. Geburtstag, 2010, 319, 328; *Hanno Merkt*,

auf die Einhaltung von Recht und Gesetz (Compliance) wird hier noch zurückzukommen sein.[50]

1. Ausreichende Informationsgrundlage

Von nicht zu unterschätzender Bedeutung ist in diesem Rahmen die Forderung des Gesetzgebers, dass die Business Judgment Rule eine ausreichende Informationsgrundlage erfordert.[51] Der Vorstand ist daher verpflichtet, alle ihm zur Verfügung stehenden Erkenntnisquellen auszuschöpfen, allerdings unter Abwägung von Kosten und Nutzen einer ausgiebigen Tatsachenermittlung.[52] Je nach Bedeutung der Entscheidung wird daher eine breitere Informationsbasis rechtlich gefordert sein.[53] So wird bei strategischen Entscheidungen grundsätzlich eine breite Informationsgrundlage zu

---

Managerhaftung im Finanzsektor: Status Quo und Reformbedarf, in: Erle/Goette/Kleindiek u.a. (Hrsg.), Festschrift für Peter Hommelhoff zum 70 Geburtstag, 2012, 711, 715; anders anscheinend *Schäfer* (Fn. 45), 1256.

50 S. unten unter V.

51 S. bereits zum früheren Recht BGHZ 135, 244 (253) = NJW 1997, 1926; *S. H. Schneider*, Informationspflichten und Informationseinrichtungspflichten im Aktienkonzern, 2006, S. 89 ff., 91; *M. Roth* (Fn. 47), S. 80 ff.; *Semler* (Fn. 46), 632 f.; *Holger Fleischer*, Die „Business Judgment Rule" im Spiegel von Rechtsvergleichung und Rechtsökonomie, in: Fleischer/Frey/Hirte u.a. (Hrsg.), Festschrift zum 70. Geburtstag von Herbert Wiedemann, 2002, 827, 840 f.; zu § 93 Abs 1 S. 2: *Freund*, NZG 2015, 1419, 1422; *S. H. Schneider* (Fn. 45), 708; *Peters*, AG 2010, 811, 812; *Florstedt*, AG 2010, 315, 317; *P. Schaub/M. Schaub*, ZIP 2013, 656, 659; *Jungmann* (Fn. 49), 843; *Dauner-Lieb* (Fn. 36), § 93 Rn. 22.

52 BGH JZ 2017, 580 Rn. 34; *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 105; *Ulmer*, DB 2004, 859, 860 ff.; *Ihrig* (Fn. 46), 2105 f.; *v. Werder* ZfB 67 (1997), 901 ff.; *Fleischer* (Fn. 51), 841; *Paefgen*, Unternehmerische Entscheidungen und Rechtsbindung der Organe in der AG, 2002, S. 223 ff.; *Paefgen* (Fn. 47), 254; OLG Celle WM 2008, 1745 (1746) = AG 2008, 711 (711); *Bosch/Lange* JZ 2009, 225, 231; *Böttcher* (Fn. 36), 1049; *Seibt/Wollenschläger* (Fn. 45), 1579; *Grunewald/Hennrichs*, in: FS Maier-Reimer (Fn. 49), 2010, 147, 148 f.; *Kebekus/Zenker* (Fn. 49), 319, 330 f.; *P. Schaub/M. Schaub* (Fn. 51), 659; strenger *Kossmann* NZG 2011, 46, 49.

53 Wie hier BGH JZ 2017, 580 (Rn. 34); s. dazu auch *S. H. Schneider* (Fn. 45), 707 ff.; *Ulmer* (Fn. 52), 860 ff.; *Ihrig* (Fn. 46), 2106; *Seibt/Wollenschläger* (Fn. 45), 1581; *Thole*, ZHR 173 (2009), 504, 524; *Peters* (Fn. 51), 813; *Andreas Cahn/Henny Mücher*, Die Verantwortlichkeit der Organmitglieder einer Sparkasse für den Erwerb riskanter Wertpapiere, in: Burgard/Hadding/Mülbert u.a. (Hrsg.), Festschrift für U. H. Schneider zum 70. Geburtstag, 2011, 197, 209; *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 106; für Einbettung im Rahmen des Risikomanagements nach § 91 Abs. 2 AktG *Hauschka*, ZRP 2004, 65, 67.

fordern sein,[54] erst recht, wenn es sich um eine Entscheidung des Gesamtvorstands handelt.[55]

Überträgt man diese Grundsätze auf Entscheidungen im IT-Bereich, muss ein Vorstandsmitglied umso mehr Informationen über den Einsatz, die Art und Güte der IT, ihre Pflegebedürftigkeit und nötige Anpassung einholen, je bedeutsamer die IT für das Unternehmen ist. Basiert etwa der gesamte Arbeitsablauf in einem Unternehmen auf einer bestimmten Software, muss diese äußerst sorgfältig im Vorfeld analysiert werden. Dazu gehört auch, ob das Unternehmen durch die Wahl einer bestimmten IT faktisch abhängig wird von einem Softwarelieferanten bzw. -hersteller, insbesondere hinsichtlich der Wahl von Dateiformaten. Alternativen müssen hier sorgfältig geprüft werden, gegebenenfalls auch Escrow-Vereinbarungen getroffen werden, um dem Risiko einer Insolvenz des Softwareherstellers vorzubeugen und den Zugriff auf den Quellcode in diesem Fall zu gewährleisten. Auch die Vertrags- und Lizenzgestaltung einschließlich technischer Fragen, etwa der Interoperabilität mit anderen IT-Komponenten, muss beachtet werden. Eine ungünstige Vertragsgestaltung kann z.B. bei Bestellung einer EDV-Anlage gegen das Interesse der Gesellschaft verstoßen.[56]

2. *Höchstpersönliche Vorstandspflicht*

Zwar kann das Vorstandsmitglied diese Fragen auch auf untere Ebenen delegieren; je bedeutsamer jedoch die eingesetzte IT für das Unternehmen wird, umso mehr muss sich das Vorstandsmitglied selbst informieren und notfalls auch externen Rat einholen. Ähnliches gilt für die Fragen der Organisation im IT-Bereich: Vergleichbar den allgemein zu § 831 BGB bzw. vertikalen Organisationspflichten entwickelten Grundsätzen[57] kann der Vorstand sich grundsätzlich auf die Information durch die unternehmenseigenen Abteilungen verlassen (Vertrauensgrundsatz), solange keine Anhaltspunkte für Fehleinschätzungen oder fehlerhafte Informationen vorlie-

54 Vgl. *Grundei/v. Werder* (Fn. 41), 826 ff.; *Arbeitskreis externe und interne Überwachung der Unternehmung der Schmalenbach Gesellschaft für Betriebswirtschaft eV*, ZIP 2006, 1068; zust. *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 107 f.

55 S. auch Begr. RegE BT-Drucks. 15/5092 S. 12; *Paefgen* (Fn. 47), 254 f.

56 BGH WM 1985, 552 (555 ff.).

57 *Förster,* in: BeckOK BGB, 56. Edition 2020, § 831 Rn. 62 f.; *Spindler,* in: BeckOGK Stand 1.2.2021, § 831 Rn. 38 ff., jew. m.w.N.

gen.[58] Bei erst eingerichteten Abteilungen oder neu eingestelltem Personal muss der Vorstand naturgemäß vorsichtiger verfahren und häufiger Stichproben durchführen, gegebenenfalls auch die Informationen durch einen Dritten kontrollieren lassen, sofern die Bedeutung der Maßnahme bzw. der Information dies gebietet. In ähnlicher Weise kann der Vorstand sachverständige Dritte heranziehen: Bei entsprechender Reputation und Vertrauenswürdigkeit, etwa im Rahmen von früheren Aufträgen, kann der Vorstand sich hierauf verlassen.

3. Bewertung und Abwägung

Abgesehen von der Schaffung einer ausreichenden Tatsachengrundlage muss der Vorstand vor allem die einzelnen Aspekte im Rahmen einer Entscheidung bewerten und die damit verbundenen Risiken abwägen.[59] Allerdings gibt es auch kein unternehmerisches Wirtschaften ohne Risiko; in der Vornahme solcher Geschäfte ist nicht *per se* eine unternehmerische Pflichtwidrigkeit oder ein Verschulden zu sehen.[60] Besonders intensiver Auseinandersetzung mit den zur Verfügung stehenden Informationen und den Chancen und Risiken bedarf es, wenn die Maßnahme zur Existenzgefährdung der Gesellschaft führen würde.[61] Wie bereits angedeutet, kann gerade die völlige Abhängigkeit eines Unternehmens von digitalen Prozessen, die das Unternehmen nicht mehr selbst in der Hand hat, durchaus zu einer Existenzgefährdung führen. Gleiches gilt etwa für vollkommene Auslagerung aller Daten in eine Cloud: Stets muss sichergestellt sein, dass der Vorstand zumindest für den Notfall über Möglichkeiten der Steuerung des Unternehmens verfügt, etwa bei einer Cloud, dass die Daten regelmäßig gesichert werden.

---

58 *Spindler* (Fn. 34), § 93 Rn. 174 ff.; *Harbarth*, ZGR 2017, 211; *Fleischer,* NZG 2003, 449, 453 ff.

59 Keine überspannte Risikobereitschaft: BGHZ 135, 244 (253); so auch schon vorher BGHZ 69, 207 (213 f.); BGH NJW 1980, 1628 (1629).

60 BGHZ 135, 244 (253); s. auch *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 88, 113; vgl. Für die aus dem US-amerikanischen Recht stammende Business Judgment Rule (zu ihrem Verhältnis zum deutschen Recht noch weiter unten) auch Joy v. North, 692 F.2d 880 (2. Cir. 1982): „rule of tolerance and mistake".

61 *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 114; *Böttcher* (Fn. 36), 1049; *Brüning/Samson*, ZIP 2009, 1089, 1092; *Balthasar/Hamelmann*, WM 2010, 589, 590.

II. Legalitätspflicht der Geschäftsleitung

1.Grundlagen

Von den unternehmerischen Entscheidungen des Vorstands ist die Erfüllung gesetzlicher Pflichten zu unterscheiden.[62] Als juristische Person unterfällt die AG, und damit der für sie organschaftlich handelnden Vorstand, im Außenverhältnis denselben Pflichtenkreisen wie andere Personen des Rechts auch, so dass der Vorstand sich an sämtliche Rechtspflichten halten muss, ohne dass es etwa Rechtsnormen „zweiter Klasse" gäbe.[63] Soweit der Vorstand als Organ der juristischen Person im Außenverhältnis an gesetzliche Pflichten gebunden ist, bestehen diese Pflichten prinzipiell auch im Innenverhältnis gegenüber der juristischen Person, mit der Folge, dass eine Verletzung externen, staatlich gesetzten Rechts auch eine Pflichtverletzung einschließlich potentieller Haftung gegenüber bzw. zugunsten der juristischen Person herbeiführt. Wenngleich die genau dogmatische Herleitung dieser „Legalitätspflicht" noch immer umstritten ist,[64] wird ihr

---

62 Siehe die Aufzählungen bei *Fleischer*, ZIP 2005, 141, 142 ff., 144; ferner *Meinrad Dreher*, Die kartellrechtliche Bußgeldverantwortlichkeit von Vorstandsmitgliedern. Vorstandshandeln zwischen aktienrechtlichem Legalitätsprinzip und kartellrechtlicher Unsicherheit, in: Dauner-Lieb/Hmmelhoff/Jacobs u.a. (Hrsg.), Festschrift für Horst Konzen zum siebzigsten Geburtstag, 2006, 85, 92; *Ihrig* (Fn. 46), 2103; *Paefgen* (Fn. 47), 251 f.; *Thole* (Fn. 53), 509; *Verse*, ZHR 175 (2011), 401, 403 ff.; *Merkt* (Fn. 49), 713; *Paefgen* (Fn. 52), S. 24 f.; *Abeltshauser*, Leitungshaftung im Kapitalgesellschaftsrecht: Zu den Sorgfalts- und Loyalitätspflichten von Unternehmensleitern im deutschen und US-amerikanischen Kapitalgesellschaftsrecht, 1998, S. 213 f.; *Goette* (Fn. 38), 756; *Wulf Goette*, Leitung, Aufsicht, Haftung – zur Rolle der Rechtsprechung bei der Sicherung einer modernen Unternehmensführung, in: Geiß/Nehm/Brandner/Hagen (Hrsg.), Festschrift aus Anlaß des fünfzigjährigen Bestehens von Bundesgerichtshof, Bundesanwaltschaft und Rechtsanwaltschaft beim Bundesgerichtshof, 2000, 123, 131, 133; *Mertens/Cahn* (Fn. 35), § 93 Rn. 71; *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 74; BGH NZG 2012, 992 (994) = ZIP 2012, 1552 (1554), alle mwN.

63 Ebenso *Ihrig* (Fn. 46), 2105; *Fleischer* (Fn. 62), 149; *Thole* (Fn. 53), 504, 520 f.; *Reichert/Ott*, ZIP 2009, 2173; *Armbrüster*, VersR 2009, 1293, 1294; *ders*., KSzW 2013, 10, 11; anders wohl *Paefgen* (Fn. 52), S. 25: „Gebote, deren Inhalt sich erst unter Einbeziehung und Abwägung der für die Bestimmung des Gesellschaftsinteresses im Einzelfall maßgeblichen Gesichtspunkte genauer bestimmen lässt"; *M. Roth* (Fn. 47), S. 132; im Anschluss daran *W. Müller*, Liber amicorum Happ, 2006, 179, 181.

64 Konsequenterweise wird man ihren Ursprung im Legalitätsinteresse als Teil des Unternehmensinteresses sehen müssen, *Spindler/Gerdemann*, ZIP 2020, 1896, 1903; *Gerdemann*, Transatlantic Whistleblowing, 2018, Rz. 258 ff., 263.

Bestehen mittlerweile von der ganz h.M. mit Recht nicht mehr in Zweifel gezogen.[65] Der Anwendung der Business Judgment Rule nach § 93 Abs. 1 S. 2 AktG auf die Auslegung gesetzlicher Pflichten durch den Vorstand steht jedoch die Begründung des Gesetzgebers entgegen, der „sonstige Pflichten" von § 93 Abs. 1 S. 2 AktG ausnehmen will und dazu ausdrücklich „rechtlich gebundene Entscheidungen", insbesondere „Treuepflichten, Informationspflichten und sonstige allgemeine Gesetzes- und Satzungsverstöße" zählt.[66]

a. Interessenabwägungen und unbestimmte Rechtsbegriffe

Dennoch handelt der Vorstand wie auch bei anderen Tätigkeiten bei der Auslegung von Gesetzen und ihrer Anwendung auf konkrete Sachverhalte tendenziell unter Unsicherheit. Dies gilt auch (oder gerade) im Bereich von IT-Anwendungen und derem rechtlichen Rahmen: So steht etwa die Anwendung von Schranken im Urheberrecht oftmals unter dem Vorbehalt von Interessenabwägungen oder unter der Voraussetzung unbestimmter Rechtsbegriffe („angemessen", etc). Ähnliche Situationen ergeben sich im Datenschutzrecht, wenn Interessenabwägungen vorgenommen werden müssen, oder etwa die angemessene Organisation zum Datenschutz bestimmt werden soll. Die bereits erwähnten Vorgaben zur Sicherheit in der Informationstechnik kritischer Infrastrukturen stellen wiederum auf „angemessene" Sicherheitsvorkehrung gemäß aktuellem „Stand der Technik" ab.[67] In allen diesen Lagen bestehen Entscheidungsspielräume, die eine gewisse Auswahl möglich machen.[68] Dementsprechend werden Durchbrechungen des Legalitätsprinzips für möglich erachtet, wenn das Organmitglied mit erheblichen Rechtsunsicherheiten konfrontiert ist[69] oder die begründete Aussicht auf die Änderung einer bislang gefestigten Rechtspre-

---

65 S. BGH NJW 2011, 88, 92; OLG Karlsruhe NZG 2013, 1177, 1178 f.; *Fleischer* (Fn. 37), § 93 Rn. 29; *Spindler* (Fn. 34), § 93 Rn. 87; *Cichy/Cziupka*, BB 2014, 1482, 1483; *Louven*, KSzW 2016, 241, 246, jew. m.w.N.

66 Begr. RegE UMAG BT-Drucks. 15/5092 S. 11.

67 S. § 8a Abs. 1 S. 1 und 2 BSIG. Hierzu bereits oben unter III.

68 Ähnlich *Katsas*, Die Inhaltskontrolle unternehmerischer Entscheidungen von Verbandsorganen im Spannungsfeld zwischen Ermessensfreiheit und Gesetzesbindung, 2006, S 125 f.; *Holle*, AG 2011, 778, 785.

69 *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 140; *Mertens/Cahn* (Fn. 35), § 93 Rn. 75; *Fleischer* (Fn. 62), 149; *M. Roth* (Fn. 47), S. 132; *Raiser/Veil*, in: Raiser/Veil KapGesR, 6. Aufl. 2015, § 14 Rn. 81; mit Einschränkungen auch *Ihrig* (Fn. 46), 2104 f.

chung besteht.[70] Die dogmatische Begründung divergiert zwar;[71] doch besteht weitgehend Einigkeit, dass der Vorstand nicht ex post für eine falsche Auslegung eines Rechtsbegriffs haften soll.

b. Anforderungen an Organmitglieder

Auch wenn die Regel des § 93 Abs. 1 S. 2 AktG nicht unmittelbar anwendbar sein mag, gibt sie doch entscheidende Hinweise darauf, welche Anforderungen an die Organmitglieder im Falle unbestimmter Rechtsbegriffe und Rechtsunsicherheiten zu stellen sind. An den Vorstand wird dabei nicht die hohe Messlatte gelegt werden können, die beispielsweise für rechtsberatende Berufe gilt; umgekehrt wird er gerade im Aktien- bzw. Zivilrecht nicht auf ein individuelles Verständnis wie im Strafrecht hoffen dürfen, das gewissermaßen das Mindestmaß an zu erfüllenden Kriterien für die zu erwartende Sorgfalt bei der Auslegung und Bestimmung von Rechtsbegriffen bildet. Dabei muss berücksichtigt werden, dass den Vorstand in der Regel ein wesentlich höherer Zeit- und Risikodruck trifft als einen Entscheidungsträger in der Verwaltung.[72]

c. Schaffung ausreichender Entscheidungsgrundlage

Grundlage der Entscheidung ist zunächst ähnlich wie in § 93 Abs. 1 S. 2 AktG die Schaffung einer ausreichenden Entscheidungsgrundlage: Je nach Komplexität der Frage und nach Größe des Unternehmens kann der Vorstand sich hierbei auf die Einholung eines internen Rechtsrats beschränken, z.B. zur Lizenzsituation oder zur Auslegung von datenschutzrechtlichen Generalklauseln, wobei er jedoch stets die Gefahr einer „Betriebsblindheit" von untergeordneten Abteilungen im Auge behalten muss. Handelt es sich um Rechtsfragen von besonderer Tragweite, im IT-Sektor etwa bei Auslagerungen ganzer für das Unternehmen wichtiger Work-

70 *Dreher* (Fn. 62), 92 f.; *Strohn*, CCZ 2013, 177, 180.

71 Für Berücksichtigung auf Verschuldensebene (Rechtsirrtum) *Binder*, AG 2012, 885, 888; so auch *Buck-Heeb*, BB 2013, 2247, 2254; zur Darstellung des gesamten Meinungsstandes *Holle*, AG 2016, 270, 271 m.w.N.

72 Näher zur Problematik von Rechtsanwendungsspielräumen in anderen Rechtsgebieten *Gerald Spindler*, Die Haftung von Vorstand und Aufsichtsrat für fehlerhafte Auslegung von Rechtsbegriffen, in: Heldrich/Prölss/Koller (Hrsg.), Festschrift für Claus-Wilhelm Canaris zum 70. Geburtstag, Band II, 2007, 403, 407, 420 ff.

flows in die Cloud, so kann das Organmitglied allerdings gehalten sein, eine zweite Meinung einzuholen, um im Sinne eines Vier-Augen-Prinzips die Rechtslage zu beleuchten.[73] Dies gilt auch, wenn es sich um neue Rechtsmaterien handelt, deren Anwendung etwa durch Behörden höchst ungewiss ist. Eine unbedingte Pflicht zur Einholung eines externen Rechtsrates, wie es mitunter in der Rechtsprechung anklingt, kann indes nicht angenommen werden.[74] Die Auswahl eines externen (Rechts-)Beraters hat entsprechend der allgemeinen Kriterien für die Pflichten bei einer Arbeitsteilung, wie sie etwa in § 831 BGB entwickelt wurden, zu erfolgen; das Vorstandsmitglied kann sich auf die Bestimmung eines qualifizierten Beraters durch Dritte verlassen, wenn diese wiederum allgemein über die Fähigkeiten zur näheren Auswahl verfügen.[75] Ob ein ausgewiesener Experte in dem jeweiligen Spezialgebiet hinzugezogen werden muss, hängt von der Komplexität und Bedeutung der Frage ab.[76] Ferner muss das Vorstandsmitglied eine Plausibilitätsprüfung durchführen. Diese dient einerseits der Vergewisserung, dass die zu beratende Frage ordentlich bearbeitet wurde, und andererseits der Aufdeckung möglicher Interessenkonflikte bei der Beratungsleistung.[77] Kann das Organmitglied auf der Grundlage eines solchermaßen eingeholten Rechtsrates davon ausgehen, dass eine der

---

73 BGH NZG 2011, 1271 (1273); s. für Befragung eines Wirtschaftsprüfers wegen Überschuldung BGH NZG 2007, 545 (547); *Kaulich*, Die Haftung von Vorstandsmitgliedern einer Aktiengesellschaft für Rechtsanwendungsfehler, 2012, S. 226; als empfehlend ansehend *Hölters* (Fn. 37), § 93 Rn. 249; *Selter*, AG 2012, 11, 15; gegen eine Verpflichtung *Peters* (Fn. 51), 816.

74 So der Leitsatz in BGH NZG 2011, 1271, 1273, allerdings handelte es sich um einen besonders gelagerten Fall; s. für Befragung eines Wirtschaftsprüfers wegen Überschuldung BGH NZG 2007, 545, 547; OLG Stuttgart NZG 2010, 141, 143; *Fleischer*, NJW 2009, 2337, 2339; *ders*., ZIP 2009, 1397, 1403 f.; *ders.* (Fn. 37), § 93 Rn. 89; ähnlich *Binder*, AG 2008, 274, 286; *P. Schaub/M. Schaub* (Fn. 51), 659; ebenso für die Inanspruchnahme interner Berater *Holger Altmeppen*, Zur Haftung der Organwalter einer AG bei untauglicher Sacheinlage – zugleich Besprechung von BGH, Urteil vom 20.9.2011 – II ZR 234/09, in: Krieger/Lutter/Schmidt (Hrsg.), Festschrift für Michael Hoffmann-Becking zum 70. Geburtstag, 2013, 1, 9.

75 *Wagner*, BB 2012, 651, 657; *Fleischer*, NZG 2010, 121, 123.

76 *Binder* (Fn. 74), 286; *Fleischer* (Fn. 75), 123; *Wagner* (Fn. 75), 656; *Junker/Biederbick*, AG 2012, 898, 900 f.; *Peters* (Fn. 51), 815; strenger *Selter* (Fn. 73), 15 f.

77 *Walter Bayer*, Legalitätspflicht der Unternehmensleitung, nützliche Gesetzesverstöße und Regress bei verhängten Sanktionen – dargestellt am Beispiel von Kartellverstößen, in: Bitter/Lutter/Priester u.a. (Hrsg.), Festschrift für Karsten Schmidt zum 70. Geburtstag, 2009, 85, 92; *Fleischer* (Fn. 74), 1404; *ders*., Rechtsrat und Organwalterhaftung im Gesellschafts- und Kapitalmarktrecht, in: Kindler, Koch, Ulmer, Winter (Hrsg.), Festschrift für Uwe Hüffer zum 70. Geburtstag,

Gesellschaft günstige Auslegung vertretbar erscheint, handelt er im Rahmen seines unternehmerischen Ermessens, wenn er eine solche Auslegung seiner Entscheidung zugrunde legt, auch wenn später ein Gericht zu einem anderen Ergebnis kommen sollte. In diesem Fall entfällt bereits die Pflichtwidrigkeit.[78]

2. *Beurteilungsspielräume?*

In diesem Zusammenhang spielt auch die Frage, ob der Vorstand eine Art Beurteilungsspielraum genießt, insbesondere bei von der Norm verlangten Interessenabwägungen. Ein Beurteilungsspielraum des Vorstandes würde hier die Norm in ihr Gegenteil verkehren: Denn er kann sich nicht selbst von den Pflichten befreien, indem man ihm einen Beurteilungsspielraum bei den Voraussetzungen der Business Judgment Rule nach § 93 Abs. 1 S. 2 AktG zubilligt; eine andere Frage ist, wie ein Rechtsirrtum dann behandelt wird. Hier gelten die oben aufgezeigten Prinzipien. Die zahlreichen Abwägungsklauseln etwa im Datenschutzrecht eröffnen dem Vorstand keinen „prioritären Beurteilungsspielraum"; die Entscheidungen des Vorstands unterliegen hier vollinhaltlich der richterlichen Überprüfung.

3. *Beachtung ausländischen Rechts*

Die soeben geschilderte Problemlage verschärft sich in der Regel noch einmal, soweit es um die Beachtung ausländischer Rechtsnormen geht, deren Inhalt sich für den Vorstand üblicherweise schwieriger bestimmen lässt als der von Normen des deutschen Rechts.[79] Zu unterscheiden sind in diesem Zusammenhang zudem Fragen der prinzipiellen Maßgeblichkeit des ausländischen Rechts für die Legalitätspflicht des Vorstands und nach seinen hierbei bestehenden Entscheidungsspielräume.

Soweit ausländisches oder internationales Recht in nationales Recht überführt worden ist, kann an seiner Maßgeblichkeit zunächst kein Zweifel bestehen. Relevant sind hier insbesondere Verbote von Schmiergeld-

---

2010, 187, 195; *Peters* (Fn. 51), 816; *Selter* (Fn. 73), 18; *Freund*, GmbHR 2011, 238, 340; *P. Schaub/M. Schaub* (Fn. 51), 659.

78 Ebenso *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 140; *Fleischer* (Fn. 62), 149 f.; *ders.* (Fn. 37), § 93 Rn. 37; *Dreher* (Fn. 62), 93; *Kocher*, CCZ 2009, 215, 217; *U. H. Schneider* (Fn. 45), 100; *Merkt* (Fn. 49), 716.

79 Vgl. für das chinesische Recht *Kipker*, in diesem Band.

zahlungen im Ausland, die mit der Integration der internationalen Konventionen zur Bekämpfung der Korruption in nationales Recht überführt wurden.[80] Die frühere Rechtsprechung des BGH, die Unternehmen Schmiergeldzahlungen insoweit gestatten wollte, wie dies für einen erfolgreichen Wettbewerb mit Konkurrenten in korruptionsgeneigten Ländern erforderlichen schien,[81] ist hierdurch obsolet geworden.[82] Die nunmehr einschlägigen Normen des deutschen Strafrechts, namentlich der § 299 Abs. 1 Nr. 1, Abs. 2 Nr. 1 StGB, die §§ 331 ff. i.V.m. § 11 Abs. 1 Nr. 2a StGB und der § 108e Abs. 3 Nr. 6 StGB, sind daher uneingeschränkt einzuhalten. Hierbei ist unerheblich, ob der Verstoß gegen diese Verbotsnormen für das Unternehmen im Einzelfall als wirtschaftlich nützlich zu beurteilen war.[83] Eine uneingeschränkte Beachtung ausländischen Rechts ist aufgrund der Legalitätspflicht des Vorstands ferner angezeigt, wenn und soweit Rechtsanwendungsnormen des deutschen Kollisionsrechts ausländische Sachnormen für anwendbar erklären[84] – wenngleich dies im hier interessierenden Kontext bei straf- und öffentlich-rechtlichen Normen des ausländischen Rechts aufgrund des geltenden Territorialprinzips eher selten der Fall ist.[85] Sofern der Vorstand (nur) nach ausländischem Kollisionsrecht an bestimmte ausländische Normen gebunden ist, insbesondere in all jenen Fällen, in denen deutsche Unternehmen über Zweigniederlassung im Ausland verfügen, können diese Normen nach deutschem Gesellschaftsrecht jedenfalls über die allgemeine Schadensabwendungspflicht des Vorstands Bedeutung erlangen.[86] Dies bedeutet aber zugleich, dass die Befolgung nicht praktizierten Rechts, das in dem jeweiligen Staat nur auf dem Papier existiert, nicht per se zwingend ist, da die Gesellschaft und ihre

---

80 S. Art. 2 § 1, § 2 Gesetz zu dem Protokoll vom 27. September 1996 zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften (EUBestG), BGBl. 1998 II 2340; Art. 2 § 2 Gesetz zu dem Übereinkommen vom 17. Dezember 1997 über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr (IntBestG), BGBl. 1998 II 2327.

81 BGHZ 94, 268.

82 I.Erg. ebenso *Kort* (Fn. 43), § 76 Rn. 118; *Fleischer* (Fn. 62), 145; *ders.* (Fn. 37), § 93 Rn. 33; *Hölters* (Fn. 37), § 93 Rn. 72; *Jermyn Brooks*, Die Bedeutung der OECD-Konvention gegen internationale Korruption für den Aufsichtsrat, Vorstand und Abschlußprüfer einer deutschen Aktiengesellschaft, in: (Lutter/Scholz/Sigle (Hrsg.), Festschrift für Martin Peltzer zum 70. Geburtstag, 2001, 27, 32.

83 LG München I AG 2014, 332 Rn. 89 – Siemens/Neubürger.

84 *Hopt/Roth* in GroßkommAktG, Band 3, 5. Aufl. 2015, § 93 Rn. 142; *Fleischer* (Fn. 37), § 93 Rn. 34; *Cichy/Cziupka* (Fn. 65), 1483.

85 S. *Spindler* (Fn. 34), § 93 Rn. 110.

86 *Fleischer* (Fn. 37), § 93 Rn. 34; *Cichy/Cziupka* (Fn. 65), 1484; *Louven* (Fn. 65), 246 f.

die Organmitglieder sich nicht gesetzestreuer verhalten müssen als die Rechtssubjekte des ausländischen Staates selbst.[87]

Soweit der Vorstand an Normen des ausländischen Rechts gebunden ist, stellt sich die für die Praxis besonders relevante Frage, inwiefern er sich bei der Interpretation des Inhalts dieses Rechts auf den „sicheren Hafen" der Business Judgment Rule des § 93 Abs. 1 S. 2 AktG berufen kann, insbesondere sofern es sich um die Auslegung unbestimmter Rechtsbegriffe handelt. Im Prinzip gelten hier die obigen Ausführungen zum deutschen Recht entsprechend, so dass dem Vorstand zwar kein eigener Beurteilungsspielraum zugestanden werden kann, im Falle rechtlicher Unsicherheiten aber gleichwohl bereits auf Pflichtenebene ein unternehmerisches Ermessen besteht, sofern der Vorstand seiner Pflicht zur Schaffung einer angemessenen Informationsgrundlage nachkommt. Aufgrund der zusätzlichen Schwierigkeiten, die sich bei der Beurteilung der aktuellen Rechtslage in einer für den Vorstand fremden Rechtsordnung stellen, wird man hier allerdings einen insgesamt großzügigeren Maßstab anlegen können als bei Auslegung unbestimmter Rechtsbegriffe des deutschen Rechts. Das bedeutet zum einen, dass eine Pflicht zur umfassenden Informierung über den Inhalt des ausländischen Rechts nur in Abhängigkeit von der Zugänglichkeit der entsprechenden Informationen und dem Ausmaß der ausländischen Betätigung des Unternehmens anzunehmen ist. Zum anderen führen die bisweilen kaum vermeidbaren Unsicherheiten hinsichtlich des Inhalts ausländischer Rechtsnormen zu einem tendenziell größeren Entscheidungsspielraum.[88] Die Anwendung eines Entscheidungsmaßstabes, der dem des § 93 Abs. 1 S. 2 AktG im konkreten Fall jedenfalls nahe kommen kann, ist somit nicht von vornherein ausgeschlossen.

E. Pflicht zur Einrichtung eines IT-Riskmanagementsystems

Wie beschrieben, können IT-Risiken das Unternehmen existentiell gefährden – daher liegt es nahe, aus den Pflichten nach § 91 Abs. 2 AktG auch

---

87 *Spindler* (Fn. 34), § 93 Rn. 110; *Hopt/Roth* (Fn. 84), § 93 Rn. 142 f.; *Mertens/Cahn* (Fn. 35), § 93 Rn. 73; *Klaus Hopt*, Recht und Geschäftsmoral multinationaler Unter- nehmen. Unlautere Finanztransaktionen und Geldzuwendungen im internationalen Wirtschaftsrecht, in: Gernhuber (Hrsg.), Tradition und Fortschritt im Recht: Festschr., 1977, 279, 279 ff.; *Bicker*, AG 2014, 8, 12; krit. aber *Cichy/Cziupka* (Fn. 65), 1484 f.; *Fleischer* (Fn. 37), § 93 Rn. 34; *Koch* (Fn. 35), § 93 Rn. 6a.

88 A.A. wohl *Cichy/Cziupka* (Fn. 65), 1485.

eine Pflicht zur Einrichtung eines IT-Riskmanagementsystems abzuleiten. Eine solche Pflicht würde mutatis mutandis auch für GmbHs bzw. deren Geschäftsführung gelten, da das GmbHG zwar keine § 91 Abs. 2 AktG entsprechende Regelung kennt, dennoch aber § 91 Abs. 2 AktG als allgemein gültiger Gedanke und Konkretisierung der Geschäftsführungspflichten auch im GmbH-Recht für vergleichbare Unternehmen anzuwenden ist.[89] Maßstab für eine solche Pflicht ist das Ausmaß der potentiellen Gefährdung des Unternehmens durch IT-Risiken bzw. Cyberangriffe, insbesondere etwa durch Erpressungssoftware (Ransomware); je mehr ein Unternehmen von seiner IT abhängt, je stärker es derartigen Risiken ausgesetzt ist, umso wichtiger wird ein umfassendes IT-Riskmanagementsystem als Unterfall des Riskmanagements nach § 91 Abs. 2 AktG.[90]

I. Organisations- und Überwachungspflichten, insbesondere Compliance

1. Grundsätze

Den Vorstand treffen ferner Organisations- und Überwachungspflichten, wobei zwischen vertikaler und horizontaler Arbeitsteilung, also innerhalb des Organs selbst, zu differenzieren ist. Die Pflichten hinsichtlich der vertikalen Arbeitsteilung als Bestandteil seiner allgemeinen Sorgfaltspflicht zur Leitung eines Unternehmens stehen in einem engen Zusammenhang mit der Pflicht zur Einrichtung eines Systems zur Früherkennung von Risiken nach § 91 Abs. 2 AktG und entsprechenden Tendenzen zur Standardisierung von Organisationen.

Ein wesentliches Element der Organisationspflicht der Unternehmensleitung besteht heute anerkanntermaßen in der Einrichtung eines Compliance-Systems zur Unterbindung von Rechtsverstößen und Einhaltung

89 *Paefgen* in Habersack/Casper/Löbbe GKGmbHG, 3. Aufl. 2020, § 43 Rn. 134; *Beurskens* in Baumbach/Hueck GmbHG, 22. Aufl. 2019, § 43, Rn. 34; *Theusinger/Jung* in MAH GmbH-Recht, 4. Aufl. 2018, § 24 Rn. 9; zuletzt *Löschhorn/Fuhrmann*, NZG 2019, 161, 163; i.Erg. ähnlich *Fleischer* in MüKo GmbHG, 3. Aufl. 2019, § 43 Rn. 61 (Übertragbarkeit für größere, risikobehaftetere Unternehmen); Auch der Gesetzgeber des KonTraG, das § 91 II AktG einführte, ging bereits von einer „Ausstrahlungswirkung" auf andere Gesellschaftsformen aus: Begr RegE KonTraG, BT-Drs. 13/9712, 15.

90 Ebenso *Schmidt-Versteyl* (Fn. 25), 1640; zuvor *Spindler*, CR 2017, 715, 722; *Beucher/Utzerath*, MMR 2013, 362, 366.

der Legalitätspflicht.[91] Deren Intensität hat sich an der jeweils drohenden Gefahr von Rechtsverstößen,[92] der Größe und dem Gegenstand des Unternehmens sowie der Bedeutung der Geschäfte zu orientieren, ebenso an der Art der übertragenen Aufgaben, der Risikoträchtigkeit einer Funktion oder eines Produktes (bei Spartenorganisation) sowie der persönlichen Befähigung des Vorstandsmitglieds, seiner Erfahrung und Bewährung auf dem jeweiligen Gebiet.[93] Dabei greift grundsätzlich der allgemein im Zivilrecht für arbeitsteilige Prozesse anerkannte Vertrauensgrundsatz ein;[94] ähnlich der vertikalen Delegation im Zivilrecht[95] genügt es auch auf der Ebene der Geschäftsführung regelmäßig, wenn der Vorstand nach sorgfältiger Überlegung ein sachkundiges Mitglied mit der Aufgabe betraut.[96] Eine Verletzung der allgemeinen Aufsichtspflicht sowohl in vertikaler wie horizontaler Sicht ist erst zu bejahen, wenn für einen ordentlichen und gewissenhaften Geschäftsleiter ein Verdacht[97] bestehen musste, dass die Geschäfte nicht ordnungsgemäß geführt werden und die Interessen der Gesellschaft gefährdet sind.[98] Bei Krisensituationen ergeben sich intensivere Überwachungspflichten.[99] Insbesondere für die Compliance gilt,

---

91 LG München I NZG 2014, 345, 347; dazu *Meyer*, DB 2014, 1063, 1065; ausführlich zum ganzen Komplex *Spindler* (Fn. 34), § 91 Rn. 52 ff.

92 *C. Goette/M. Goette*, DStR 2016, 815, 816.

93 *Fleischer*, NZG 2003, 449, 453 ff.; *ders.* (Fn. 37), § 91 Rn. 54 ff.; *Spindler* (Fn. 37), § 91 Rn 64 ff.

94 *Fleischer* (Fn. 37), § 77 Rn. 63 ff.; *Froesch*, DB 2009, 722, 725; ähnlich *Armbrüster*, KSzW (Fn. 63), 13.

95 Zu den Anforderungen im Rahmen von § 831 BGB s. *Förster* (Fn. 57), § 831 Rn. 27 ff.

96 Für die vertikale Delegation im Rahmen von § 92 (Erkundigung bei einem WP wegen Überschuldung) BGH NJW 2007, 2118 = ZIP 2007, 1265; für das Steuerrecht (Delegation auf einen Steuerberater) grundlegend BFHE 175, 209 = BStBl. 1995 II, 278 = GmbHR 1995, 239 (Tz. 21 ff.) m.w.N.; s. dazu *H. P. Westermann/Mutter*, DZWiR 1995, 184, 185.

97 Die Quelle des Verdachtsmoments ist ohne Belang, vgl. *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 376; *Fleischer* (Fn. 58), 454.

98 BGHZ 133, 370 (378 f.); BGH NJW 2019, 1067; BGH ZIP 1987, 1050; BGH NJW 1986, 54 (55); *Hoffmann-Becking,* ZGR 1998, 497, 512 f.; *Kleindiek,* in: Lutter/Hommelhoff GmbHG, 19. Aufl. 2019, § 37 Rn. 32; *Hoffmann-Becking,* in: MHdB GesR, Band 4, 5. Aufl. 2020, § 22 Rn. 28; *Sieg/Zeidler,* in: Hauschka/Mossmayer/Lösler Corporate Compliance, 3. Aufl. 2016, § 3 Rn. 69; *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 376; *Mertens/Cahn* (Fn. 35), § 93 Rn. 81 f.; *Fleischer* (Fn. 37), § 77 Rn. 63; *Zöllner/Noack,* in: Baumbach/Hueck GmbHG § 35 Rn. 33; *Koppensteiner/Gruber,* in: Rowedder/Schmidt-Leithoff GmbHG, 6. Aufl. 2017, § 43 Rn. 10.

99 OLG Hamburg AG 2001, 141, 144; OLG Bremen ZIP 1999, 1671, 1678; vgl. für die GmbH BGH NJW 2019, 1067, 1068 ff.; BGHZ 133, 370. 379; BGH DStR

dass entsprechende Stellen mit Informationsbefugnissen und Ressourcen ausgestattet sein müssen, sowie entsprechende unmittelbare Meldewege an die Geschäftsleitung bestehen. Auch wenn es ratsam erscheint, ist die Unabhängigkeit einer Compliance-Abteilung im Sinne einer Weisungsunabhängigkeit bis hin zum Kündigungsschutz gesellschaftsrechtlich nicht (wohl aber kapitalmarktrechtlich) vorgeschrieben.

Die Erfüllung von IT-spezifischen Pflichten macht hier keine Ausnahme, sondern wird eher durch bestimmte Vorgaben akzentuiert, von denen hier nur einige vorgestellt werden können.

2. *IT-spezifische Compliance-Felder*

a. Datenschutzrechtliche Compliance

Die Verabschiedung der EU-DSGVO mit ihren zahlreichen Weiterungen gegenüber dem bisherigen Datenschutzrecht,[100] vor allem aber den erheblich verschärften Sanktionen, die konzernweit bis zu 4 % des globalen Umsatzes betragen können (Art. 83 Abs. 5 DSGVO, Erwägungsgrund 150), hat das Bewusstsein für die Notwendigkeit der Berücksichtigung datenschutzrechtlicher Vorschriften im Unternehmen gestärkt, und damit auch für Datenschutz-Compliance sensibilisiert.[101] Die potentielle Existenzgefährdung für ein Unternehmen liegt bei derartig hohen Bußgeldern auf der Hand und ist mit kartellrechtlichen Risiken durchaus vergleichbar, so dass heute von einer Pflicht zur Einrichtung solcher Organisationen ausgegangen werden muss – sofern es sich um größere Unternehmen handelt.[102] Bei Lichte besehen wirft die datenschutzrechtliche Compliance-Organisation aber – abgesehen von der Einbindung des Datenschutzbeauftragten – keine Besonderheiten gegenüber anderen sensiblen Rechtsgebieten auf, so-

---

2001, 633, 634; BGH WM 2008, 1403 (1404, Rn. 11) = NJW-RR 2008, 1253 (1254, Rn. 11); *Armbrüster* (Fn. 63), 12; *Hopt/Wiedemann* (Fn. 37), § 93 Rn. 381; *Fleischer* (Fn. 37), § 77 Rn. 64; strenger wohl *Ernst T. Emde*, Gesamtverantwortung und Ressortverantwortung im Vorstand der AG, in: Burgard/Hadding/Mülbert u.a. (Hrsg.), Festschrift für U. H. Schneider zum 70. Geburtstag, 2011 295, 319, der unabhängig von der Ressortverteilung eine volle Verantwortlichkeit jedes Vorstandsmitglieds in Krisensituationen annimmt.

100 S. *Spindler*, DB 2016, 937 ff.

101 Dazu etwa *Behling*, ZIP 2017, 697 ff.; *Wybitul*, CCZ 2016, 194, 194 ff.; *König* (Fn. 30), 267 ff.

102 *Behling* (Fn. 101), 698 f.; s. auch *König* (Fn. 30), 268.

fern es sich nicht um die Wiedergabe von Pflichten (Informations-, Dokumentations-, Auskunftspflichten etc.) und die Festlegung von Datenverarbeitungszwecken und z.B. Speicherfristen handelt;[103] insbesondere die Delegationsgrundsätze einschließlich des Vertrauensgrundsatzes können herangezogen werden. Hinzu kommt, dass schon vor der DSGVO aus § 9 BDSG umfangreiche Pflichten zur datenschutzsichernden Organisation folgten.

b. IT-Sicherheit

Jenseits der Kommunikation hat die Digitalisierung auch Auswirkungen auf andere Bereiche des Gesellschaftsrechts, hier namentlich die Organhaftung. Wie bereits angedeutet, bringt die zentrale Rolle der IT und der Digitalisierung für praktisch alle Geschäftsprozesse mit sich, dass die IT-Sicherheit eine völlig andere Bedeutung als noch vor ca. 10–15 Jahren hat. Da heute das Schicksal des Unternehmens von einer funktionierenden und gegenüber dem Zugriff Dritter sicheren IT abhängt, vom Vertrieb über die finanzielle Steuerung bis hin zu Einkauf oder Fertigung, liegt es auf der Hand, dass die IT-Sicherheit „Chefsache" geworden ist.[104]

Natürlich kann (und muss) der Vorstand oder die Geschäftsführung die konkreten Aufgaben der IT-Sicherheit delegieren, um entsprechende Fachleute zu engagieren; essentiell ist jedoch die direkte Anbindung an die Geschäftsführung, da es sich um existentielle Risiken im Sinne von § 91 Abs. 2 AktG im Rahmen des Risikomanagements handelt. Vorstand bzw. Geschäftsführung sind daher persönlich gehalten, die entsprechende Abteilung zu leiten und regelmäßig zu überwachen.[105] In horizontaler Hinsicht sind auch die fachfremden Geschäftsführungsmitglieder verpflichtet, zumindest rudimentär das für IT-Sicherheit zuständige Mitglied zu überwachen.[106] In diesem Rahmen kann es sinnvoll sein, eine sog. Cyber-Risk-Governance-Gruppe aus verschiedenen Vorstandsmitgliedern zu bilden, die die in Frage kommenden Ressorts leiten, wie Human Resources, IT,

---

103 Darauf laufen auch letztlich die Ausführung von *Behling* (Fn. 101), 700 ff. hinaus; ähnlich *Wybitul* (101), 194 ff.; ähnlich auch *König* (Fn. 30), 268 ff.

104 *Schmidt-Versteyl* (Fn. 25), 1640; *Habbe/Gergen* (Fn.), 282; *Noack*, ZHR 2019, 105, 124; v. *Holleben/Menz* (Fn. 22), 65; *Schmidl* (Fn. 32), § 28 Rn. 47 ff.; s. auch *Kiefner/Happ*, BB 2020, 2051, 2054.

105 *Kiefner/Happ* (Fn. 104), 2054.

106 *Schmidt-Versteyl* (Fn. 25), 1640, *Habbe/Gergen* (Fn.), 282 f.; *Noack* (Fn. 104), 125; allgemein s. BGH, NJW 2019, 1067.

Datenschutz etc.[107] Im Finanzmarktbereich ist dies bereits durch die BAIT definiert, die dort formulierten Anforderungen können jedoch aufgrund der umfassenden Digitalisierung heute fast in jedem Bereich eines größeren Unternehmens Geltung beanspruchen.[108] So führt die BaFin hier aus:[109] „Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte der IT-Strategie sind:

a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie der Auslagerungen von IT-Dienstleistungen
b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT
c) Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation
d) Strategische Entwicklung der IT-Architektur
e) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange
f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)".

Auch wenn die BAIT detaillierte Vorgaben nur für den nach KWG regulierten Bankensektor enthält, bleibt dennoch die Frage nach einer weiteren Konkretisierung der erforderlichen Maßnahmen offen: Hier ist zwischen organisatorischen einerseits und technischen Maßnahmen andererseits zu unterscheiden. Für die organisatorischen Anforderungen kann auf den Grundschutzkatalog des BSI[110] zurückgegriffen werden, was schon über § 9 BDSG a.F. und Art. 24 DSGVO im Datenschutzrecht weitgehend galt bzw. weiter gelten wird. Für technische Maßnahmen muss dagegen im jeweiligen Einzelfall überprüft werden, welche IT zum Einsatz kommt. Stets ist indes daran zu erinnern, dass auch hier für die Einrichtung und Ausgestaltung der Organisation die Business Judgment Rule nach § 93 Abs. 1 S. 2 AktG zum Tragen kommt, da es sich ganz überwiegend (außerhalb der be-

107 S. dazu *Kiefner/Happ* (Fn. 104), 2054 unter Bezugnahme auf *NACD*, Director's Handbook Series, Cyber-Risk Oversight, 2017, S. 17; *FERMA*, At the junction of corporate governance & cybersecurity, 2019, S. 18 f.

108 S. auch *Schmidt-Versteyl* (Fn. 25), 1641.

109 *BaFin* (Fn. 33), Rn. 2.

110 BSI-Grundschutzkatalog, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/Zip_Datei_Edition_2021.html;jsessionid=7340A73AFDDC91D7A3F609E4373D5764.internet081 (abgerufen am 05.07.2021).

sonders regulierten Bereiche) um unternehmerische Entscheidungen handelt.[111]

aa. Risikoanalyse

Eines der essentiellen Handlungsfelder, das sich aus dem Grundsatz der Business Judgment Rule nach § 93 Abs. 1 S. 2 AktG unmittelbar im Sinne der angemessenen Information zur Entscheidungsvorbereitung ergibt, besteht in der Beurteilung der Gefährdungslage und der Risikoanalyse für das gesamte Unternehmen.[112] Die BAIT fordert hierzu, dass regelmäßige Überprüfungen und Anpassungen etwa bei Veränderungen der Bedrohungsszenarien oder der Sicherheitstechnologien vorzunehmen sind.[113] Da es sich hier um einen allgemeinen Grundsatz handelt, gilt dies mutatis mutandis auch für Branchen bzw. Unternehmen, die nicht dem KWG bzw. der Aufsicht durch die BaFin unterliegen. Die letztliche Risikobeurteilung obliegt nach entsprechender Vor- und Aufbereitung durch IT-Fachleute immer der Geschäftsleitung.[114]

Bestandteil dieser Risikoanalyse ist unter anderem die Sicherung der Daten des Unternehmens und seiner Vertragspartner, insbesondere wie die Sicherungsmechanismen des Zugangs zu ihnen ausgestaltet sind und welche Risiken aus der Vernetzung des Unternehmens resultieren können. Aber auch der derzeit geltende Sicherheitsstandard als „Stand der Technik" ist zu ermitteln. Dazu soll auch gehören, dass die Geschäftsleitung nachzuvollziehen habe, „ob alle Daten tatsächlich gespeichert werden müssen und wenn ja, wie lange. Je weniger Daten das Unternehmen sammelt, desto weniger Angriffsmasse entsteht."[115] Dies ist zwar vor dem Hintergrund der DSVGO und ihrem Prinzip der Datensparsamkeit richtig, wirft allerdings auch Zweifel im Hinblick auf die Analysefähigkeit von Angriffen auf, die u.U. auch ein „Mehr" an Daten erfordern können.

Dabei kann (aber nicht muss) sich die Geschäftsleitung auch an einem Ordnungsrahmen orientieren, wie er vom Weltwirtschaftsforum

---

111 *Kiefner/Happ* (Fn. 104), 2053; *Mehrbrey/Schreibauer*, MMR 2016, 75, 80.

112 S. dazu spezifisch für Cybersecurity *Kiefner/Happ* (Fn. 104), 2052; allgemein *Spindler* (Fn. 34), § 91 Rn. 20; *R. Koch*, ZGR 2006, 184, 208.

113 *BaFin* (Fn. 33), Rn. 16; s. allgemein auch *OECD*, Digital Security Risk Management for Economic and Social Prosperity, 2015, S. 8; *Kiefner/Happ* (Fn. 104), 2053.

114 Ebenso *Schmidt-Versteyl* (Fn. 25), 1641.

115 So *Schmidt-Versteyl* (Fn. 25), 1641.

entwickelt wurde, und der in Anwendung allgemeiner Kriterien[116] die Auswirkungen eines Vorfalls im Sinne der Schädigung und Bedrohung von unternehmensrelevanten Daten und Aktivitäten bis hin zur Reputation und dessen Eintrittswahrscheinlichkeiten ermittelt, etwa der möglichen Angriffe.[117] Andere Kriterien, anhand derer die Risiken ermittelt werden können, beziehen sich auf die Kategorien der „Vertraulichkeit", „Verfügbarkeit" und „Integrität".[118]

bb. Maßnahmen

Ferner obliegt es der Geschäftsleitung, Pläne und Maßnahmen zu entwickeln, die Angriffsrisiken minimieren können, aber auch Notfallpläne im Falle erfolgreicher Angriffe enthalten, wozu die Zusammenstellung eines Notfallteams (Response-Team) gehören kann.[119] Die Zusammenstellung des Response Teams gehört allerdings wiederum zu den unternehmerischen Entscheidungen, die von dem Zuschnitt des Unternehmens und seiner IT-Risiko-Exposition abhängen.[120]

Theoretisch kann die Geschäftsleitung auch aufgrund einer Kosten-Nutzen-Analyse zu dem Ergebnis kommen, dass die Risiken zu akzeptieren sind oder umgekehrt, dass die gefährdenden Aktivitäten (z.B. Verbindung zum Internet) einzustellen sind.[121] In aller Regel dürften aber risikoadäquate Maßnahmen im Vordergrund stehen, da außer in Ausnahmefällen kein Unternehmen mehr IT-Risiken ohne Weiteres akzeptieren oder seine Geschäftsfelder einstellen kann.

---

116 Jenseits des einfachen probabilistischen Produkts aus Eintrittswahrscheinlichkeit und Schadensausmaß sind hierbei insbesondere (Rest-)Risiken mit besonderes schwerem, ggf. unternehmensgefährdenden Schadensverlauf angemessen zu berücksichtigen. Vgl. zur Risikoanalyse im Kontext der Atomkraftdiskussion etwa *Breuer* NVwZ 1990, 211, 212 ff.; zu unterschiedlichen Risikosignaturen und Begrifflichkeit im Recht *Jaeckel* JZ 2011, 116.

117 Näher *Kiefner/Happ* (Fn. 104), 2052, unter Verweis auf *World Economic Forum*, Advancing Cyber Resilience, 2017, 3.3 Board Cyber Risk Framework, S. 15 ff.

118 *Habbe/Gergen* (Fn.), 283 unter Bezugnahme auf *BSI*, Cyber-Sicherheits-Exposition v. 11.07.2018, S. 2, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_013.pdf?__blob=publicationFile&v=4 (abgerufen am 15.01.2021).

119 Näher dazu *Kiefner/Happ* (Fn. 104), 2055; s. auch *Neufeld/Schemmel*, DSB 2017, 209, 209.

120 Zutr. *Kiefner/Happ* (Fn. 104), 2056.

121 *Kiefner/Happ* (Fn. 104), 2053 unter Bezugnahme auf *OECD* (Fn. 113), S 52.

Zu den notwendigen Maßnahmen gehören entsprechend dem Grundschutzkatalog des BSI Mitarbeiter-Schulungen,[122] Virenschutz und Kontrollmechanismen, die eindeutige Zuordnung von Verantwortlichkeiten und die Einbindung der Behörden und externer Berater.[123] Hierzu kann ferner die Ausarbeitung der IT-Netzwerkstrukturen, der verfügbaren Hard- und Software sowie der Schutzvorrichtungen gehören.[124] Auch die Erarbeitung von IT-Richtlinien zum Umgang mit der im Unternehmen eingesetzten Informationstechnik ist erforderlich, die Maßnahmen zum Schutz des Unternehmens-Knowhows und der Verfügbarkeit der IT-Systeme bei Cyberangriffen zur Verhinderung von Betriebsunterbrechungen enthalten.[125] So verlangt die BaFin in den BAIT, dass die Geschäftsleitung eine Informationssicherheitsleitlinie zu beschließen und zu kommunizieren hat, die sich an dem Stand der Technik ausrichtet.[126] Gleiches gilt für das Krisenmanagement im Falle erfolgter Angriffe.[127]

Im Bereich des Notfall- oder auch Response-Managements wird zu Recht dafür plädiert, dass bei einer Gefährdung der wesentlichen Unternehmenswerte („crown jewels“) das jeweilige zuständig Vorstandsmitglied einbezogen werden muss, ohne dass die Möglichkeit einer Delegation bestünde, wozu auch die Benennung eines kurzfristig erreichbaren Ersatz-Vorstandsmitglieds gehört.[128] Im Übrigen gilt es, auch im Rahmen der Erarbeitung der Notfallpläne die Kompetenzen und Berichtswege klar zu definieren, einschließlich der Benennung der im Unternehmen involvierten Stellen und Bereiche.[129] Von zentraler Bedeutung ist im Rahmen der Notfallreaktion und späteren Beseitigung von Schäden die ausreichende Protokollierung der Vorfälle, etwa durch Log-Files.[130]

---

122 Hierzu auch *Kiefner/Happ* (Fn. 104), 2053.
123 *BSI*, Leitfaden IT-Grundschutz, 2016, S. 71; s. ferner *Habbe/Gergen* (Fn.), 283 f.
124 S. dazu *BSI*, BSI-Standard 200–2 – IT-Grundschutz-Methodik, 2017, 8.1.4 Netzplanerhebung, S. 87, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html (abgerufen am 05.07.2021); *Habbe/Gergen* (Fn.), 284.
125 *Schmidl* (Fn. 32), § 28 Rn. 48.
126 *BaFin* (Fn. 33), Rn. 16.
127 Zum Ganzen auch *Aufderheide/Fischer,* CCZ 2017, 138, 140.
128 *Kiefner/Happ* (Fn. 104), 2056.
129 Statt vieler *Habbe/Gergen* (Fn.), 284 m.w.N.
130 *Habbe/Gergen* (Fn.), 285, unter Bezugnahme auf Allianz für Cyber-Sicherheit, Massnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle, 2019, S. 3.

cc. Überwachung

Last but not least bedarf die Umsetzung der Maßnahmen einer engmaschigen Überwachung durch die Geschäftsleitung, die sich selbst ein Bild hiervon machen muss, einschließlich der Risikokontrolle durch die jeweiligen Stabsmitarbeiter und deren ständige Berichterstattung. So führt die BaFin in den BAIT aus, dass die Geschäftsleitung quartalweise über Risikoanalyse und Veränderungen der Risikosituation zu unterrichten ist.[131]

c. Rolle von Zertifizierungen

Für beide Bereiche der (datenschutzrechtlichen) Compliance und IT-Sicherheit stellt sich immer wieder die Frage nach der Rolle von Zertifizierungen, insbesondere ob diese haftungsentlastend wirken.[132] Diese Frage ist keineswegs IT-spezifisch, sondern taucht oft bei Organisationspflichten und einschlägigen Compliance- oder Risikomanagementsystemen auf. Da auch im IT-Bereich die Ausgestaltung einer sicheren Organisation höchst individuell ist, kann aus der Befolgung von bestimmten Vorgaben, auch des BSI-Grundschutzkatalogs, nicht *per se* die Einhaltung der nach § 93 Abs. 1 AktG bzw. § 43 GmbHG geforderten Sorgfalt abgeleitet werden; stets bedarf es noch einer Prüfung des Einzelfalls. Auch die Zertifizierung entlastet eine Geschäftsführung noch nicht von vornherein von ihren Pflichten, zumal sie immer nur eine Momentaufnahme darstellt.[133] Dies gilt umso mehr, wenn es sich bei der Zertifizierung nur um eine sog. Systemprüfung handelt, die sich auf die Prüfung der Kohärenz der vorgelegten Managementsysteme etc. beschränkt, aber keine (stichprobenartigen) Prüfungen vor Ort durchführt.[134]

131 *BaFin* (Fn. 33), Rn. 14.
132 Siehe dazu *Schmidt-Versteyl*, in diesem Band, II.2.c.
133 Zust. *Schmidt-Versteyl* (Fn. 25), 1642.
134 Ausführlich dazu *Spindler,* Unternehmensorganisationspflichten, 2001, S. 809 ff.

II. Handlungsfelder in concreto (Auswahl)

Besondere Maßnahmen werden im Folgenden kurz beleuchtet:

1. Pflicht zur Einrichtung eines CISO (Chief Information Security Officer)?

In Betracht kommt die Einrichtung eines besonders mit IT-Sicherheitsfragen befassten Unternehmensbeauftragten – eines Chief Information Security Officers (CISO), der nicht identisch mit dem Chief Information Officer ist, wie er jetzt schon verschiedentlich in Unternehmen anzutreffen ist.[135] Dieser CISO soll „wesentliche Richtlinien und Standards (formulieren), auf deren Grundlage die weiteren Zwischenschritte hin zu den finalen Umsetzungsmaßnahmen basieren" und ggf. „als Schnittstelle zwischen den verschiedenen Geschäftseinheiten agieren".[136] Die BaFin sieht ebenfalls, allerdings nur „nur bei größeren Unternehmen oder spezifisch IT-ausgerichteten Unternehmen die Einrichtung eines organisatorisch und prozessual unabhängigen Informationssicherheitsbeauftragten" vor.[137] Schon daraus wird ersichtlich, dass die Schaffung eines solchen CISO keineswegs verpflichtend ist, geschweige den seine besondere Ausgestaltung, etwa ob er unabhängig gegenüber Weisungen zu sein hat etc. Nur in Ausnahmefällen wie den besonders gegenüber IT-Risiken anfälligen Unternehmen kann hier eine Pflicht zur Einrichtung eines solchen CISO angenommen werden – einer Weisungsunabhängigkeit bedarf es hier aber nicht.

2. Pflicht zum Abschluss von Cyberrisk-Versicherungen?

Diskutiert wird ferner, ob es eine Pflicht zum Abschluss einer Cyberversicherung für den Vorstand bzw. die Geschäftsführung geben kann.[138] Auch dies lässt sich pauschal nicht beantworten, sondern hängt auch hier vom Einzelfall ab; allerdings kann eine Ermessenreduzierung auf Null vorliegen, wenn es sich wiederum um Unternehmen handelt, die in beson-

---

135 Dazu *Kiefner/Happ* (Fn. 104), 2054 unter Verweis auf *NACD* (Fn. 107), S. 38 ff.; *FERMA* (Fn. 107), S. 14, 23; s. auch *Habbe/Gergen* (Fn.), 284.

136 So *Kiefner/Happ* (Fn. 104), 2054.

137 *BaFin* (Fn. 33), Rn. 18.

138 Siehe dazu *Schmidt-Versteyl*, in diesem Band, II.2.d.

derem Maße IT-Risiken ausgesetzt sind.[139] Zumindest muss ein geschäftsführendes Organmitglied die Möglichkeit einer Versicherung prüfen,[140] allerdings auch hier die jeweiligen Bedingungen.[141]

3. Technische Maßnahmen

Auch die technischen Vorkehrungen gehören selbstverständlich zum Katalog der von der Geschäftsleitung mit Unterstützung der jeweiligen IT-Stabsstellen und -funktionen zu ergreifenden Maßnahmen, wiederum unter Geltung der Business Judgment Rule, so dass die jeweiligen Maßnahmen vom Einzelfall abhängen. Generell wird man aber einen aktualisierten Virenschutz für alle Geräte fordern können, ebenso wie ein Patch-Management, um die nötigen Updates stets einzuspielen.[142] Ebenso gehört ein angemessenes Passwortmanagement, das möglichst starke Passwörter verwendet, hierzu.[143] Schließlich muss das Unternehmen für regelmäßige Backups sorgen, ebenso wie für die Protokollierung (Logfiles), um Angriffe nachvollziehen zu können.[144] Unter Umständen kann auch der Einsatz von kryptographischen Lösungen bis hin zur Blockchain in Betracht kommen.

---

139 *Fortmann*, r+s 2019, 429, 443; Achenbach VersR 2017, 1493, 1497.

140 *Fortmann* (Fn. 139), 443.

141 S. dazu näher *Spindler,* in: Beckmann/Matusche-Beckmann, Handbuch Versicherungsrecht, 4. Aufl. erscheint 2021.

142 *BSI*, Ransomware – Bedrohungslage, Prävention & Reaktion 2019, S. 14 ff.; *Habbe/Gergen* (Fn.), 284; s. auch bereits *v. Hollenen/Menz* (Fn. 22), 67.

143 *Habbe/Gergen* (Fn.), 284.

144 *BSI*, Basismaßnahmen der Cyber-Sicherheit, 2021, 8. Logdatenerfassung und -auswertung, S. 6, https://www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.pdf;jsessionid=6D1EF7BCF5AD03E06B9-FE4160285053B.internet082?__blob=publicationFile&v=1 (abgerufen am 05.07.2021); näher dazu *BSI*, Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen, Version 1.0a, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf?__blob=publicationFile&v=5 (abgerufen am 05.07.2021).

F. Anforderungen an Überwachungsorgane (Aufsichtsrat)

Die Pflichten der Geschäftsleitung bzw. des Vorstands spiegeln sich in den diesbezüglichen Überwachungspflichten des Aufsichtsrats als Teil der Überwachung der Vorstandstätigkeit gem. § 111 AktG. Die konkret erforderlichen Überwachungsmaßnahmen richten sich – wie stets – insbesondere sowohl nach der individuellen Risikoexposition des Unternehmens als auch nach den getroffenen Organisationsmaßnahmen des Vorstands.[145] Entscheidet sich der Vorstand beispielsweise zur Bestimmung eines CISO, werden die Überprüfung von dessen Aufgabenzuschnitt und -erfüllungen einen nicht unwesentlichen Teil der IT-bezogenen Aufsichtsratsarbeit einnehmen, einschließlich etwaiger Befragungen des CISO im Rahmen von Aufsichtsratssitzungen.

Ob hier der Aufsichtsrat indes verpflichtet ist, einen eigenen IT-bezogenen Ausschuss zu gründen und mit entsprechenden fachkundigen Mitgliedern zu besetzen, kann gemäß den allgemeinen Kriterien zum Ermessen des Aufsichtsrats zur internen Organisation nicht pauschal beantwortet werden;[146] wiederum hängt es von der Risikoexposition des Unternehmens und seiner Ausrichtung ab, ob ein derartiger Ausschuss erforderlich ist. So dürfte ein solcher Ausschuss eher bei einem IT-Unternehmen ratsam sein, sowie ggf. auch bei einem am Finanzmarkt tätigen Unternehmen, nicht jedoch allgemein.

Gleiches gilt für die Frage, ob der Aufsichtsrat Zustimmungsvorbehalte anordnen muss: Auch hier kommt es auf den Einzelfall und die Risikoexposition des Unternehmens an.[147] Allerdings dürfte angesichts der wachsenden Bedeutung der IT-Strategie eines Unternehmens dieser Punkt inzwischen zu denjenigen gehören, die auf jeden Fall einem Zustimmungsvorbehalt unterliegen sollten.

---

145 *Spindler,* in: BeckOGK AktG, 19.10.2020, § 111 Rn. 25 ff; *Habersack,* in: MüKo AktG, 5. Aufl. 2019, § 111 Rn. 55.

146 S. auch *Meckl/J. Schmidt*, BB 2019, 131, 134; *Kiefner/Happ* (Fn. 104), 2054; allgemein: *Habersack* (Fn. 145), § 107 Rn. 94; *Spindler* (Fn. 145), § 107 Rn. 93.

147 S. auch *Schmidt-Versteyl* (Fn. 25), 1642; zu den allgemeinen Kriterien, wann ein Zustimmungsvorbehalt anzuordnen ist: *Habersack* (Fn. 145), § 111 Rn. 125 ff.; *Spindler* (Fn. 145), § 111 Rn. 79.

G. Fazit

In summa ergibt sich ein disparates Bild: Während die Pflichten für die Unternehmen selbst noch eher gleich einem Flickenteppich über verschiedene Gesetze hinweg gewoben sind, schält sich für das interne Riskmanagement und die Compliance ein weitgehender Konsens heraus, der IT-spezifisch die verschiedenen Anforderungen aus den allgemeinen Kriterien heraus konkretisiert, insbesondere im Rahmen der Business Judgment Rule zur Ausformung der geforderten Organisation. Dabei spielen die von den verschiedenen Institutionen verabschiedeten Normungen und Empfehlungen eine gewichtige Rolle. Es bleibt abzuwarten, wie weit der neue Referenzrahmen des sog. Cybersecurity Acts der EU hier neue Impulse geben wird.