Schriften zum IT-Sicherheitsrecht 2

Bittner | Guntermann | Müller | Rostam (Hrsg.)

Cybersecurity als Unternehmensleitungsaufgabe

Nomos

Schriften zum IT-Sicherheitsrecht

Herausgegeben von

Prof. Dr. Gerrit Hornung
Prof. Dr. Ralf Poscher
MinDir a.D. Martin Schallbruch
Prof. Dr. Tobias Singelnstein
Prof. Dr. Gerald Spindler
Prof. Dr. Louisa Specht-Riemenschneider
Prof. Dr. Indra Spiecker gen. Döhmann

Band 2

Marc-Philipp Bittner | Anabel Guntermann
Christoph Benedikt Müller | Darius Rostam (Hrsg.)

Cybersecurity als Unternehmensleitungsaufgabe

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2021

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-8377-9
ISBN (ePDF): 978-3-7489-2767-9

DOI: https://doi.org/10.5771/9783748927679

Onlineversion
Nomos eLibrary

Vorwort

Cybersecurity ist in einer digitalen Wirtschaft eine zentrale Herausforderung nahezu jedes Unternehmens. Die steigende Anzahl an Cyberattacken bezeugt ein massiv zunehmendes Bedrohungspotential. Unternehmen stehen vor Herausforderungen von verschiedenen Seiten: Zum einen geht es um den Schutz der eigenen Handlungs- und Wettbewerbsfähigkeit vor Industriespionage, Hacking und Schadsoftware. Zum anderen tragen Unternehmen in kritischen Infrastrukturen oder im Umgang mit personenbezogenen Daten Pflichten gegenüber Dritten und dem Staat. Diese Verantwortung läuft bei Geschäftsleitern zusammen. Sie müssen wirtschaftliche Aspekte abwägen, Allgemeininteressen berücksichtigen und durch eine Vielzahl gesetzlicher Regelungen navigieren – eine hochkomplexe Aufgabe, die mit erheblichen Schadens- und Haftungsrisiken verbunden ist.

Dieser Tagungsband dokumentiert die virtuelle Tagung „Cybersecurity als Unternehmensleitungsaufgabe", die in Kooperation mit der Friedrich-Naumann-Stiftung für die Freiheit am 23. und 24. Oktober 2020 an der Bucerius Law School in Hamburg stattfand. Die Tagung beschäftigte sich aus einer interdisziplinären Perspektive mit den Problemen und Risiken, denen Unternehmen und ihre Geschäftsleiter im Umgang mit Cyberattacken ausgesetzt sind. Videoaufzeichnungen der einzelnen Vorträge und anschließenden Diskussionen sind im Internet frei abrufbar.[1] Der Band gibt die Referate von *Gerald Spindler*, *Sarah Schmidt-Versteyl*, *Alexander Brüggemeier* und *Dennis-Kenji Kipker* wieder. Zudem enthält er ausgewählte Einsendungen von *Katrin Haußmann*, *Isabella Risini* und *Andreas Beyer*.

Im ersten Beitrag gibt *Gerald Spindler* einen Überblick über Grundlagen, Bedrohungspotentiale und rechtliche Rahmenbedingungen der Cybersecurity. Er beleuchtet die IT-sicherheitsrechtlichen Pflichten der Geschäftsleitung und leitet Anforderungen an ein unternehmensinternes Risikomanagement ab. Welcher Haftungsrahmen sich für Geschäftsleiter daraus ergibt und welche Enthaftungsmöglichkeiten im Wege der Delegation bestehen, ist Gegenstand des folgenden Beitrags von *Sarah Schmidt-Versteyl*. *Alexander Brüggemeier* thematisiert anschließend Auslöser, Inhalt und Verfahren der diversen Melde- und Veröffentlichungspflichten, die Cyberangriffe auslösen können. Im folgenden Beitrag führt *Dennis-Kenji*

1 https://bit.ly/3uinQt5.

Kipker in die bewegte Cybersecurity-Gesetzgebung in China ein und setzt sich mit der Rolle von Systemen Künstlicher Intelligenz als Schlüsseltechnologie des nächsten Jahrzehnts auseinander. Aus arbeitsrechtlicher Perspektive behandelt *Katrin Haußmann* anschließend Fragen der betrieblichen Mitbestimmung bei der Einführung von IT-Sicherheitssystemen und erörtert, welche Handlungsspielräume der Unternehmensleitung offenstehen. Einen verfassungsrechtlichen Zugang für ihren Beitrag wählt *Isabella Risini*, indem sie die Rolle des Staates mit Blick auf die Herausforderungen der IT-Sicherheit hinterfragt und verfassungsrechtlichen Maßstäben dazu nachgeht. Schließlich wirft *Andreas Beyer* abschließend einen Blick auf die Risiken, die sich in der unternehmerischen Praxis des Mittelstandes stellen und entwickelt praxisorientierte Lösungs- und Präventionsmöglichkeiten.

Dieser Band entstand unter Förderung des Liberalen Instituts der Friedrich-Naumann-Stiftung für die Freiheit. Die Publikation im Open Access ermöglichte die Unterstützung durch Knowledge Unlatched. Ihnen gilt unser besonderer Dank. Wir bedanken uns auch bei den Herausgeberinnen und Herausgebern der Schriftenreihe „Schriften zum IT-Sicherheitsrecht“ für die Aufnahme dieses Bandes in ihre Reihe. Schließlich gilt unser Dank unserem Schirmherrn *Prof. Dr. Dr. h.c. mult. Karsten Schmidt*, den Referentinnen und Referenten, Teilnehmerinnen und Teilnehmern der Tagung und allen am Zustandekommen beteiligten Personen.

Hamburg, im Juni 2021

Marc-Philipp Bittner, *Dr. Anabel Guntermann*, *Christoph Benedikt Müller* und *Darius Rostam*

Inhalt

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 (Auwahl)

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.

Cybersecurity als Unternehmensleitungsaufgabe – Neue Aspekte der Organhaftung

Sarah Schmidt-Versteyl

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

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

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

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

2 BGH NJW 1997, 1926.

3 LG München I NZG 2014, 345.

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

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

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

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

I. Haftungsrisiko des Unternehmens

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

---

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

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

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

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

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

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

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

---

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

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

8 Bundesamt für Sicherheit in der Informationstechnik.

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

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

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

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

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

---

11 BGH r+s 2014, 96, 97.

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

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

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

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

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

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

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

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

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

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

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

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

1. Haftungsreduzierung kaum möglich

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

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

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

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

2. Überwälzung des Schadens auf Dritte

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

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

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

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

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

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

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

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

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

---

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

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

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

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

II. Haftungsrahmen der Geschäftsleitung für Cybersecurity

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

1. Haftungsmaßstab

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

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

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

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

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

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

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

---

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

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

32 LG München I NZG 2008, 319.

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

2. Enthaftung möglich?

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

a. Horizontale Delegation

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

b. Enthaftung durch vertikale Delegation

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

34 BGH NZG 2019, 225 Rn. 15.

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

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

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

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

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

c. Enthaftung durch Zertifizierung?

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

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

38 *Spindler* (Fn. 30), § 76 Rn. 18; *Schulze*, NJW 2014, 3484, 3485; *Wentrup* (Fn. 37), § 19 Rn. 35 f.; *Knierim* (Fn. 36), 5. Kap. Rn. 42.

39 Vgl. dazu auch *Spindler*, in diesem Band, E.I.

40 BGH NZG 2018, 1189 Rn. 39.

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

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

d. Enthaftung durch Versicherungslösung?

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

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

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

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

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

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

III. Fazit

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

---

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

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

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

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

Offenlegungspflichten bei Cyberangriffen

Alexander Brüggemeier

I. Einleitung

„Bricht bald der Cyberkrieg los?" titelte vor kurzem die FAZ anlässlich eines Hackerangriffs auf Microsoft.[1] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) meldet eine stetig steigende Zahl an Cyber-Angriffen mit einem immer größeren Gefahrenpotential für Staat, Wirtschaft und Gesellschaft.[2] Für die Leitung von Unternehmen stellt sich eine Vielzahl an Fragen und Problemen. In der akuten Situation eines Cyberangriffs mögen Offenlegungspflichten vielleicht nicht ganz oben auf der Prioritätenliste der Unternehmensleitung stehen. Aufgrund der nicht unerheblichen Bußgelder, möglicher Schadensersatzansprüche und – in besonders gelagerten Einzelfällen – sogar einer Strafbarkeit bei Nichterfüllung der Offenlegungspflichten sollten diese jedoch in jedem Fall penibel eingehalten und nach Möglichkeit Vorsorge getroffen werden. Dieser Beitrag soll einen Überblick über die in Betracht kommenden Melde- und Veröffentlichungspflichten geben und eine erste Handreichung darstellen. Im Zentrum stehen Melde- und Veröffentlichungspflichten nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), der Datenschutz-Grundverordnung (DSGVO) und der Marktmissbrauchsverordnung (MAR).*

1 *Finsterbusch et al.*, Bricht bald der Cyberkrieg los? 09.03.2021, https://www.faz.net/aktuell/wirtschaft/digitec/chinesischer-hackerangriff-auf-microsoft-die-politische-bedeutung-17235983.html.

2 BT-Drs. 19/26106, S. 1.

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag beruht, ist abrufbar unter https://doi.org/10.17176/20210315-161018-0.

II. BSIG

1. Regelungszweck

Die Offenlegungspflichten nach dem BSIG dienen der Gewährleistung der Cyber- und Informationssicherheit und dem Schutz der Funktionsfähigkeit kritischer Infrastruktur sowie – zukünftig – von Unternehmen von besonderem öffentlichen Interesse und der Verfügbarkeit digitaler Dienste. Das BSI soll die IT-Sicherheitslage in Deutschland einschätzen können und ggf. durch eine schnelle Reaktion einen Übergriff bzw. einen vergleichbaren Vorfall bei anderen Systemen verhindern können.

2. Meldepflichtige Unternehmen

Das BSIG statuiert Meldepflichten für die Betreiber Kritischer Infrastrukturen (§ 8b Abs. 4 BSIG) und die Anbieter digitaler Dienste (§ 8c Abs. 3 BSIG). Nach der nunmehr vom Bundestag verabschiedeten Neuregelung des IT-Sicherheitsgesetzes – die Zustimmung des Bundesrates steht noch aus – werden zukünftig voraussichtlich auch Unternehmen von besonderem öffentlichen Interesse gem. § 8f Abs. 7, 8 BSIG-E einer Offenlegungspflicht unterliegen.[3] Diese Offenlegungspflicht erfasst nach § 2 Abs. 14 BSIG-E neben Unternehmen, die Güter nach § 60 Abs. 1 Nr. 1, 3 AWV herstellen oder entwickeln (Rüstungsindustrie und Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen) und bestimmten Unternehmen der Störfall-Verordnung insbesondere auch die Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Welche Unternehmen eine besondere volkswirtschaftliche Bedeutung haben, wird durch eine Rechtsverordnung anhand abstrakt-genereller Kriterien konkretisiert werden, wobei sich die Berechnungsmethodik nach dem Gutachten der Monopolkommission nach § 44 Abs. 1 GWB richten soll.[4]

§ 8b Abs. 4 BSIG verpflichtet Betreiber Kritischer Infrastrukturen bestimmte Störungen unverzüglich über die Kontaktstelle an das Bundesamt

3 BT-Drs. 19/26106, S. 18 f.

4 BT-Drs. 19/26106, S. 31, 58. Die 100 Unternehmen erfassende Liste des Gutachtens der Monopolkommission ist abrufbar unter: https://monopolkommission.de/images/HG23/HGXXIII_Gesamt.pdf, S. 80.

zu melden. Kritische Infrastrukturen sind gem. § 2 Abs. 10 S. 1 BSIG Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören (Nr. 1) und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (Nr. 2). Nähere Bestimmungen zu dieser Legaldefinition sind in der auf Grundlage von § 2 Abs. 10 S. 2, 10 Abs. 1 BSIG erlassenen BSI-KritisV enthalten. Danach sind die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, das Finanz- und Versicherungswesen sowie Transport und Verkehr erfasst, wobei in den Anhängen der BSI-KritisV die Schwellenwerte festgelegt werden, bei deren Erreichen von einer hohen Bedeutung i.S.v. § 2 Abs. 10 S. 1 Nr. 2 BSIG auszugehen ist. Ausgenommen von der Meldepflicht sind gem. § 8d Abs. 3 BSIG Betreiber Kritischer Infrastrukturen, die auf Grund anderer Rechtsvorschriften Veröffentlichungspflichten unterliegen, die mit § 8b Abs. 4 BSIG vergleichbar oder weitergehend sind, wie beispielsweise gem. § 8d Abs. 3 Nr. 1 Alt. 1 BSIG die Betreiber eines öffentlichen Telekommunikationsnetzes, deren Verpflichtung insoweit aus § 109 Abs. 5 TKG folgt. Zudem sind gem. § 8d Abs. 1 BSIG Kleinstunternehmen i.S.d. der Empfehlung 2003/361/EG der Kommission von der Meldepflicht ausgenommen, sodass Unternehmen, die weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2 Millionen Euro nicht überschreitet, nicht zur Meldung an das BSI verpflichtet sind (Art. 2 Abs. 3 des Anhangs zur Empfehlung 2003/361/EG der Kommission).

§ 8c Abs. 3 BSIG verpflichtet die Anbieter digitaler Dienste jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Digitale Dienste erfasst gem. § 2 Abs. 11 BSIG Online-Marktplätze (§ 2 Abs. 11 Nr. 1 BSIG), Online-Suchmaschinen (§ 2 Abs. 11 Nr. 2 BSIG) und Cloud-Computing-Dienste (§ 2 Abs. 11 Nr. 3 BSIG), die nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden und Dienste i.S.v. Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 darstellen.

3. Auslöser der Meldepflicht

a. § 8b Abs. 4 BSIG

Auslöser der Meldepflicht gem. § 8b Abs. 4 BSIG sind Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben (Nr. 1) bzw. erhebliche Störungen, die zu einem Ausfall oder einer erheblichen Störung führen können (Nr. 2). Der Begriff der Störung ist ausweislich der Begründung zum IT-Sicherheitsgesetz 2015 in Anlehnung an die höchstrichterliche Rechtsprechung zu § 100 TKG funktional zu verstehen.[5] Sie liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.[6] Dies erfasst beispielsweise Sicherheitslücken, Schadprogramme und erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug.[7] Hat die Störung bereits zu einem Ausfall oder einer erheblichen Beeinträchtigung geführt, ist eine Erheblichkeit der Störung nicht erforderlich. Ist es hingegen noch nicht zu einem Ausfall oder einer erheblichen Beeinträchtigung gekommen, entsteht eine Meldepflicht nur, wenn es sich um eine erhebliche Störung handelt, die zu einem Ausfall oder einer erheblichen Beeinträchtigung führen kann. Eine erhebliche Störung liegt vor, wenn diese nicht automatisiert oder mit wenig Aufwand behoben werden kann.[8] Eine Beeinträchtigung ist jeweils erheblich, wenn die Infrastruktur nicht mehr in der Lage ist, Versorgungsleistungen wie geplant oder erwartet zu erbringen.[9]

5 BT-Drs. 18/4096, S. 27.
6 BT-Drs. 18/4096, S. 27; BGH, Urteil v.03.07.2014 – III ZR 391/13 = NJW 2014, 2500 Rn. 15.
7 BT-Drs. 18/4096, S. 27 f.
8 *Ritter/Schulte*, CR 2019, 617, 619; *Winter*, CR 2020, 576, 578.
9 *Ritter/Schulte*, CR 2019, 617, 619; *Winter*, CR 2020, 576, 578.

b. § 8c Abs. 3 BSIG

Anbieter digitaler Dienste sind verpflichtet, jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der EU erbrachten digitalen Dienstes zu melden. Ein Sicherheitsvorfall kann in Anlehnung an Art. 4 Nr. 7 der NIS-RL (EU 2016/1148) definiert werden als Ereignis, das tatsächlich negative Auswirkungen auf die Sicherheit von Netz- und Informationssystemen hat. Die Erheblichkeit der Auswirkungen eines Sicherheitsvorfalls bestimmt sich gem. § 8c Abs. 3 S. 2 BSIG i.V.m. Art. 4 der Durchführungsverordnung (EU) 2018/151 auf Grundlage mehrerer Parameter, wie insbesondere der Zahl der betroffenen Nutzer, der Dauer des Sicherheitsvorfalls, dem geographischen Gebiet, dem Ausmaß der Unterbrechung, dem Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten sowie danach, ob der Sicherheitsvorfall zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste geführt hat, von dem mehr als 100.000 Nutzer betroffen sind, ob eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder Menschen ums Leben gekommen sind, oder der Vorfall zu einem Sachschaden in Höhe von mehr als 1.000.000 Euro geführt hat. Kann der Anbieter die Erforderlichkeit mangels Zugang zu den Informationen über diese Parameter nicht einschätzen, entfällt die Meldepflicht gem. § 8c Abs. 3 S. 3 BSIG.

4. Inhalt der Meldepflicht

§ 8b Abs. 4 BSIG verpflichtet die Betreiber Kritischer Infrastruktur zur unverzüglichen Meldung der Störungen. Der Inhalt der Meldung, für welche das BSI ein Meldeformular zur Verfügung stellt,[10] wird durch § 8 Abs. 4 S. 2 BSIG vorgegeben und umfasst Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung. Eine namentliche Nennung des Betreibers ist gem. § 8b Abs. 4 S. 3 BSIG lediglich erforder-

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=1.

lich, wenn die Störung zu einem Ausfall oder einer Beeinträchtigung führt. Zudem soll das BSI zukünftig gem. § 8b Abs. 4a BSIG-E berechtigt sein, die zur Bewältigung der Störung erforderlichen Daten einschließlich personenbezogener Daten herausverlangen zu können. Die Meldung muss unverzüglich, mithin ohne schuldhaftes Zögern, erfolgen[11] und das BSI geht von dem Grundsatz „Schnelligkeit vor Vollständigkeit" aus.[12] Ein Aufschub bis zur Ausermittlung des Sachverhaltes ist nach Auffassung des BSI nicht zulässig.[13] Stattdessen sind die bislang bekannten Informationen als Erstmeldung zu kennzeichnen und durch spätere Folgemeldungen zu ergänzen.

Der Inhalt der Meldung nach § 8c Abs. 3 BSIG richtet sich nach § 8b Abs. 4 BSIG.[14] Das BSI stellt wiederum ein Meldeformular zur Verfügung[15] und gibt auf seiner Webseite im Rahmen von FAQ nähere Hinweise.[16] Hiervon gem. § 8c Abs. 3 S. 4 BSIG abweichende Durchführungsakte der Kommission nach Art. 16 Abs. 9 der NIS-RL existieren aktuell nicht.

5. Sanktionen

Die Sanktionen sind bislang insbesondere im Vergleich zu den drohenden Rechtsfolgen eines Verstoßes gegen die Vorschriften der DSGVO und der MAR zahnlos. § 14 Abs. 2 BSIG stellt lediglich ein Bußgeld von bis zu 50.000 Euro in Aussicht. Nach der vom Bundestag verabschiedeten Neuregelung ist in § 14 Abs. 2 Nr. 7, Abs. 5 BSIG-E nunmehr ein Bußgeld von bis zu 500.000 Euro vorgesehen.

---

11 BSI, KRITIS-FAQ, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Meldepflicht/faq-zur-meldepflicht_node.html; *Buchberger* in: Schenke/Graulich/Ruthig, 2. Aufl. 2019, § 8b BSIG Rn. 6.

12 BSI, KRITIS-FAQ.

13 BSI, KRITIS-FAQ.

14 Der bisherige Verweis auf § 8b Abs. 3 BSIG stellt ein Redaktionsversehen dar und soll durch Art. 1 Ziff. 14 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme korrigiert werden, BT-Drs. 19/26106, S. 17.

15 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/meldungen_8c3BSIG_vorlage_pdf.pdf?__blob=publicationFile&v=1.

16 BSI, FAQ zur Regulierung von Anbietern digitaler Dienste, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/Anbieter_digitaler_Dienste/FAQ/Meldepflicht/faq_dsp_meldepflicht_node.html.

III. DSGVO

1. Regelungszweck

Die DSGVO enthält mehrere Offenlegungspflichten, die im Falle eines Cyberangriffs einschlägig sein können. Zunächst verpflichtet Art. 33 Abs. 1 DSGVO die Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden. Zudem ist der Verantwortliche gem. Art. 34 Abs. 1 DSGVO verpflichtet, in bestimmten Fällen die von der Verletzung betroffenen Personen unverzüglich zu benachrichtigen. Schließlich verpflichtet Art. 33 Abs. 2 DSGVO Auftragsverarbeiter, einem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten zu melden. Diese Offenlegungspflichten dienen dem möglichst effektiven Schutz personenbezogener Daten natürlicher Personen durch einen präventiven Anreiz zur Stärkung der Datensicherheit. Zudem stellen sie die Grundlage für Maßnahmen gem. Art. 58 DSGVO dar.[17]

2. Personeller Anwendungsbereich

Die Meldepflicht gegenüber der zuständigen Aufsichtsbehörde gem. Art. 33 Abs. 1 DSGVO und die Benachrichtigungspflicht gem. Art. 34 Abs. 1 DSGVO treffen die Verantwortlichen. Verantwortlicher ist gem. Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die DSGVO enthält anders als das BSIG keine Einschränkung auf bestimmte Sektoren oder Unternehmen mit besonderer Kritikalität.

Die Pflicht zur Meldung einer Verletzung an den Verantwortlichen trifft Auftragsverarbeiter. Auftragsverarbeiter ist gem. Art. 4 Nr. 8 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

17 *Paal*, ZD 2020, 119.

3. Auslöser der Meldepflicht

a. Art. 33 DSGVO

Auslöser der Meldepflicht gem. Art. 33 Abs. 1 DSGVO ist die Verletzung des Schutzes personenbezogener Daten. Diese liegt gem. Art. 4 Nr. 12 DSGVO bei einer Verletzung der Sicherheit vor, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Es sind vielfältige Cyberangriffe denkbar, die diese Merkmale erfüllen. Beispielhaft kann die Verschlüsselung von Daten durch eine Erpressungssoftware (Verlust) genannt werden. Die Meldepflicht entfällt gem. Art. 33 Abs. 1 Hs. 2 DSGVO, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es handelt sich um eine Prognoseentscheidung unter Berücksichtigung aller Umstände des Einzelfalls, wobei insbesondere die Eintrittswahrscheinlichkeit und die voraussichtlich betroffenen Rechtsgüter zu berücksichtigen sind.[18] Anders als im Rahmen der Ad-hoc-Publizitätspflicht aus Art. 17 MAR, bei der eine einmal eingetretene Veröffentlichungspflicht nicht wieder entfällt, können Gegenmaßnahmen, die dazu führen, dass das Risiko für die Rechte und Freiheiten der betroffenen Personen nachträglich entfällt, zu einem Entfallen der Meldepflicht führen.[19]

b. Art. 34 DSGVO

Führt die eine Meldepflicht nach Art. 33 DSGVO auslösende Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, sind diese gem. Art. 34 Abs. 1 DSGVO unverzüglich zu benachrichtigen. Anders als bei Art. 33 Abs. 1 Hs. 2 DSGVO ist eine Risikoabwägung bereits zur Begründung der Benachrichtigungspflicht erforderlich. Das Bestehen eines hohen Risikos kann sowohl durch eine hohe Wahrscheinlichkeit eines geringen Schadens als auch durch eine geringe Wahrscheinlichkeit ei-

18 *Paal*, ZD 2020, 119, 121; *Winter*, CR 2021, 576, 579.
19 *Winter*, CR 2021, 576, 579.

nes hohen Schadens begründet werden.[20] Maßgeblich ist – wie bei Art. 33 DSGVO – ein *probability/magnitude*-Test. In bestimmten Fällen entfällt die Benachrichtigungspflicht gem. Art. 34 Abs. 3 DSGVO, insbesondere, wenn durch nachfolgende Maßnahmen das Bestehen eines hohen Risikos ausgeräumt werden kann. Die Benachrichtigungspflicht entfällt zudem, wenn der Verantwortliche bezüglich der betroffenen Daten – zum Schutz der Rechte und Freiheiten der betroffenen Personen – geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat – auch wenn in diesen Fällen bereits das Bestehen eines hohen Risikos fraglich sein dürfte – oder wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat allerdings eine öffentliche Bekanntmachung oder ähnliche Maßnahme zu erfolgen. Besteht Unsicherheit, ob die Voraussetzungen des Art. 34 Abs. 3 DSGVO vorliegen, bietet es sich an, einen Beschluss nach Art. 34 Abs. 4 DSGVO herbeizuführen, mit welchem festgestellt wird, dass die Voraussetzungen für ein Entfallen der Benachrichtigungspflicht gegeben sind.

4. Verfahren und Inhalt der Meldung

a. Art. 33 DSGVO

Der Verantwortliche hat die Verletzung unverzüglich – mithin ohne schuldhaftes Zögern – und möglichst binnen 72 Stunden, nachdem sie dem Verantwortlichen bekannt wurde, zu melden. Wird diese 72-Stunden-Frist nicht eingehalten, muss die Verzögerung gegenüber der Behörde begründet werden. Insgesamt gilt das Prinzip „Schnelligkeit vor Vollständigkeit", was sich deutlich in der Möglichkeit der Abschichtung der Meldung in Abhängigkeit von den zur Verfügung stehenden Informationen gem. Art. 33 Abs. 4 DSGVO zeigt.

Der Mindestinhalt der Mitteilung ergibt sich aus Art. 33 Abs. 3 DSGVO. Erforderlich sind Informationen über die Art der Verletzung [lit. a)], die Angabe einer Anlaufstelle für weitere Informationen [lit. b)], eine Beschreibung der wahrscheinlichen Folgen [lit. c)] und eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen [lit. d)]. Von den zuständigen Behörden zur Verfügung gestellte Meldeformulare strukturieren

20 *Martini* in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 34 Rn. 30. Lediglich auf eine hohe Wahrscheinlichkeit abstellend: *Winter*, CR 2021, 576, 579.

und vereinheitlichen die jeweils zu meldenden Informationen.[21] Benötigt die zuständige Behörde weitere Informationen, kann sie diese jedenfalls auf Grundlage von Art. 58 Abs. 1 DSGVO anfordern.

b. Art. 34 DSGVO

Die unverzügliche Benachrichtigung der betroffenen Personen nach Art. 34 Abs. 2 DSGVO orientiert sich inhaltlich an Art. 33 Abs. 3 DSGVO, reduziert die Verpflichtung aus Art. 33 Abs. 3 lit. a) DSGVO allerdings auf die Art der Verletzung. Die Benachrichtigung hat gem. Art. 34 Abs. 2, 12 Abs. 1, 2 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher, schriftlicher oder anderer, ggf. elektronischer Form in einer klaren und einfachen Sprache zu erfolgen.

5. Sanktionen

Die Erfüllung der Pflichten aus der DSGVO wird mit erheblichen Sanktionen abgesichert. Nach Art. 83 Abs. 4 DSGVO können aufgrund eines Verstoßes gegen Art. 33, 34 DSGVO Bußgelder von bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Bei einem Verstoß gegen Art. 58 Abs. 1 DSGVO (ergänzende Informationspflicht) drohen sogar Geldbußen von bis zu 20 Millionen Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

21 S. bspw. https://www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/Inhalt2/Meldeformular---Verletzung-des-Schutzes-personenbezogener-Daten/formular_art33.pdf.

IV. MAR

1. Regelungszweck

Die Ad-hoc-Publizität ist ein wesentlicher Baustein des europäischen Kapitalmarktrechts zum Schutz der Funktionsfähigkeit der Kapitalmärkte.[22] Sie flankiert das Verbot des Insiderhandels aus Art. 8 MAR,[23] stärkt dadurch das Vertrauen in die Integrität der Kapitalmärkte und fördert die Informationseffizienz und Allokationseffizienz der Kapitalmärkte.[24]

2. Meldepflichtige Unternehmen

Art. 17 MAR erfasst lediglich Emittenten, die für ihre Finanzinstrumente eine Zulassung zum Handel an einem geregelten Markt in einem Mitgliedsstaat beantragt oder erhalten haben, sowie gem. Art. 17 Abs. 1 UAbs. 3 MAR Emittenten, die für ihre Finanzinstrumente eine Zulassung zum Handel auf einem multilateralen (MTF) oder organisierten Handelssystem (OTF) erhalten oder eine Zulassung zum Handel auf einem MTF beantragt haben.[25] Freiverkehrs-Emittenten werden hingegen nicht erfasst.

3. Auslöser der Meldepflicht

a. Insiderinformation gem. Art. 7 Abs. 1 lit. a) MAR

Art. 17 Abs. 1 MAR verpflichtet einen Emittenten, Insiderinformationen, die unmittelbar den Emittenten betreffen, zu veröffentlichen. Der Begriff der Insiderinformation wird definiert durch Art. 7 Abs. 1 lit. a) MAR. Danach sind Insiderinformationen „nicht öffentlich bekannte präzise Infor-

22 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1.

23 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1.

24 *Fleischer/Zimmer* in: dies. Effizienz als Regelungsziel im Handels- und Wirtschaftsrecht, 9, 14 ff.; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 6 ff.

25 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 29 ff.

mationen, die direkt oder indirekt einen oder mehrere Emittenten oder ein oder mehrere Finanzinstrumente betreffen und die, wenn sie öffentlich bekannt würden, geeignet wären, den Kurs dieser Finanzinstrumente oder den Kurs damit verbundener derivativer Finanzinstrumente erheblich zu beeinflussen". Der Emittentenleitfaden der BaFin enthält eine Reihe an Umständen, die potentiell eine Ad-hoc-Pflicht auslösen können. Mögliche Cyberangriffe auf Emittenten werden jedoch nicht diskutiert.[26]

Wann eine Information als präzise anzusehen ist, ergibt sich aus Art. 7 Abs. 2 S. 1 MAR. Erfasst werden sowohl Umstände bzw. Ereignisse, die bereits eingetreten sind, als auch Umstände bzw. Ereignisse, von denen vernünftigerweise erwartet werden kann, dass sie in Zukunft eintreten werden. Eine hinreichende Eintrittswahrscheinlichkeit liegt vor, wenn die Wahrscheinlichkeit, dass der Umstand eintritt, größer als 50 % ist.[27] Die voraussichtlichen Auswirkungen des Ereignisses auf den Börsenkurs sind hingegen nicht bei der Bestimmung der notwendigen Eintrittswahrscheinlichkeit zu berücksichtigen (kein *probability/magnitude*-Test).[28] Zu berücksichtigen ist, dass im Rahmen von gestreckten Sachverhalten sowohl die bereits eingetretenen Zwischenschritte, als auch die zukünftigen Zwischenschritte und das Endereignis mögliche Anknüpfungspunkte darstellen.[29] Selbst wenn ein Cyberangriff also noch nicht zu einem Schaden geführt hat, dieser aber hinreichend wahrscheinlich ist und auch die übrigen Voraussetzungen von Art. 17 MAR vorliegen, kann bereits ein ad-hoc-publizitätspflichtiger Sachverhalt gegeben sein, dessen Nichtveröffentlichung lediglich auf Grundlage eines Aufschubs gem. Art. 17 Abs. 4 MAR möglich ist. Diese Umstände bzw. Ereignisse müssen zudem hinreichend spezifisch sein, um bei der Bildung des Marktpreises berücksichtigt werden zu können.

Die Information darf zudem nicht bereits öffentlich bekannt sein. Dies ist der Fall, wenn sie nicht von einer unbestimmten Anzahl von Perso-

26 BaFin, Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 22.

27 EuGH, Urteil v. 28.06.2021 – Rs. C-19/11 = NJW 2012, 2787 Rn. 49; BGH, Beschluss v. 23.04.2013 – II ZB 7/09 = NZG 2013, 708 Rn. 29; *Krause* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 6 Rn. 63; *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 97.

28 EuGH, Urteil v. 28.06.2021 – Rs. C-19/11 = NJW 2012, 2787 Rn. 50; *Krause* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 6 Rn. 63 m.w.N.

29 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 73.

nen zur Kenntnis genommen werden kann.[30] Die Kenntnis nur einer Bereichsöffentlichkeit, d.h. der unmittelbaren Marktteilnehmer, ist nicht ausreichend.[31]

Die Information muss außerdem geeignet sein, den Kurs des Finanzinstruments erheblich zu beeinflussen. Dies ist gem. Art. 7 Abs. 4 MAR der Fall, wenn „ein verständiger Anleger [sie] wahrscheinlich als Teil der Grundlage seiner Anlageentscheidung nutzen würde."[32] Dafür ist aus einer objektiven ex-ante-Perspektive festzustellen, ob sich die Information auf den Fundamentalwert des Unternehmens auswirkt.[33] Anders als bei der Prüfung, ob für einen zukünftigen Umstand überhaupt eine hinreichende Eintrittswahrscheinlichkeit besteht, sind im Rahmen der Prüfung der Kursrelevanz die erwartete Auswirkung der Information auf den Kurs sowie die Eintrittswahrscheinlichkeit des Umstandes zu berücksichtigen (*probability/magnitude*-Test).[34] Dass sich ein Cyberangriff auf den Fundamentalwert eines Unternehmens auswirkt, ist in einer Vielzahl von Fällen – bspw. bei einer erheblichen Beeinträchtigung der Produktion oder dem Bekanntwerden von wichtigen Geschäftsgeheimnissen – denkbar, kann aber nicht generell festgestellt werden. Vielmehr ist die Beurteilung auf Grundlage sämtlicher Informationen und Besonderheiten des Einzelfalls vorzunehmen.

b. Unmittelbare Betroffenheit

Zudem muss der Emittent unmittelbar betroffen sein, um eine Ad-hoc-Publizitätspflicht zu begründen. Dies ist in Anlehnung an § 15 Abs. 1 S. 3 WpHG a.F. insbesondere der Fall, wenn die Information im Tätigkeitsbereich des Emittenten selbst eintritt, also bei unternehmensinternen Ereignissen. Allerdings kann auch bei Ereignissen, die von außen stammen, ein hinreichend konkreter Zusammenhang zu dem Emittenten bestehen, sodass ein verständiger Anleger die Veröffentlichung der Information durch

30 BaFin, Emittentenleitfaden, Modul C, S. 10; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 77.

31 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 77; *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 126 ff.

32 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 78.

33 *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 190 ff.

34 *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 198.

den Emittenten berechtigterweise erwarten darf.[35] Bei Cyberangriffen wird die Information in der Regel im Tätigkeitsbereich des Emittenten selbst eintreten, diesen also unmittelbar betreffen.

c. Keine Saldierung

Anders als im Rahmen der Meldepflicht nach Art. 33 DSGVO, bei welcher auch nachträgliche Maßnahmen zu einem Entfall der Veröffentlichungspflicht führen können, wenn dadurch Risiken für die Rechte und die Freiheit natürlicher Personen vermieden werden, kann eine einmal eingetretene Ad-hoc-Pflicht nicht aufgrund nachträglicher Umstände entfallen. Die Veröffentlichungspflicht entfällt nicht, wenn nach dem Entstehen einer veröffentlichungspflichtigen Insiderinformation – bspw. eines erfolgreichen Cyberangriffs, der voraussichtlich zu einem erheblichen Abfluss von Geschäfts- und Betriebsgeheimnissen führt – im Zeitraum eines Aufschubs nach Art. 17 Abs. 4 MAR Maßnahmen getroffen werden können, um diesen Abfluss zu verhindern. Auch können zwei Insiderinformationen, die voraussichtlich einen gegenläufigen Einfluss auf den Kurs haben, nicht saldiert werden.[36]

4. Aufschubbefugnisse gem. Art. 17 Abs. 4 MAR

Von höchster Relevanz sind die Befugnisse des Emittenten, die Veröffentlichung der Insiderinformation aufzuschieben. Ein solcher Aufschub kommt nach Art. 17 Abs. 4 MAR in Betracht, wenn eine unverzügliche Offenlegung geeignet wäre, die berechtigten Interessen des Emittenten zu beeinträchtigen, die Aufschiebung nicht geeignet wäre, die Öffentlichkeit irrezuführen und der Emittent die Geheimhaltung der Information sicherstellen kann. Die Möglichkeit eine Veröffentlichung nach Art. 17 Abs. 4 MAR aufzuschieben, wird konkretisiert durch ein Zusammenspiel der Durchführungsverordnung (EU) 2016/1055, der Leitlinien der ESMA über den Aufschub der Offenlegung von Insiderinformationen und der Verord-

35 BaFin, Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 33 f.; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 49 ff.

36 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 79.

nung zur Konkretisierung von Anzeige-, Mitteilungs- und Veröffentlichungspflichten nach dem Wertpapierhandelsgesetz (WpAV).[37]

a. Berechtigte Interessen des Emittenten

Entgegen der Auffassung der ESMA[38] ist der Begriff der berechtigten Interessen tendenziell nicht eng auszulegen.[39] Vielmehr bedarf es eines transparenzrechtlichen Korrektivs zur Ausdehnung des Tatbestands der Insiderinformation zur Vermeidung von Insiderhandel.[40] Nach Art. 6 WpAV liegt ein berechtigtes Interesse vor, wenn die Interessen des Emittenten an der Geheimhaltung der Information die Interessen des Kapitalmarktes an einer vollständigen und zeitnahen Veröffentlichung überwiegen. Diese von § 6 WpAV vorgesehene Abwägung kann dogmatisch am Begriff der *berechtigten* Interessen festgemacht werden.[41] Ein Interesse des Emittenten kann angenommen werden, wenn die Veröffentlichung zu negativen Konsequenzen für den Emittenten, d.h. für dessen Fundamentalwert, führen kann. Allein der Kursverlust, der mit einer negativen Ad-hoc-Mitteilung in der Regel einhergeht, oder ein durch die Veröffentlichung drohender Reputationsverlust stellen allerdings typischerweise kein berücksichtigungsfähiges berechtigtes Interesse des Emittenten dar.[42] Typische Fallgruppen eines berechtigten Interesses, welche auch in einigen Fällen von Cyberangriffen relevant werden können, sind laufende Verhandlungen, deren Ergebnis oder Gang durch eine Veröffentlichung negativ beeinträchtigt würde.[43]

---

37 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 95.

38 ESMA/2016/1130 Rn. 52.

39 *Kumpan/Schmidt* in: Schwark/Zimmer, Kapitalmarktrechts-Kommentar, 5. Aufl. 2020, Art. 17 MAR Rn. 199; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 173 f.

40 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 96 m.w.N.

41 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 97 m.w.N. Allein die Interessen des Emittenten für maßgeblich erachtend bspw.: *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 167 ff.; *Klöhn*, AG 2016, 423, 430 f.; *Kumpan*, DB 2016. 2039 2043; *Poelzig* NZG 2016, 761, 764.

42 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 99.

43 ESMA/2016/1478 DE Rn. 8 lit. a. S. 4; ESMA/2016/1130 Rn. 55 f.; EW 50 lit. a) MAR; § 6 Nr. 1 WpAV.

b. Keine Irreführung der Öffentlichkeit

Die Aufschiebung der Offenlegung darf gem. Art. 17 Abs. 4 UAbs. 1 lit. b) MAR nicht geeignet sein, die Öffentlichkeit irrezuführen. Eine Eignung zur Irreführung besteht, wenn im Markt, d.h. bei einem breiten Anlegerpublikum, eine Fehlvorstellung über die Information besteht.[44] Das alleinige Bestehen einer Informationsasymmetrie ist allerdings nicht ausreichend, da diese dem Bestehen einer Insiderinformation immanent ist.[45] Drei von der ESMA genannte, nicht abschließende Beispiele[46] lassen sich zu dem Grundsatz verdichten, dass insbesondere eigene Kommunikation eine entsprechende Fehlvorstellung im Markt verursachen kann. Auch hinreichend konkrete Informationen, die nicht auf den Emittenten zurückzuführen sind, können eine entsprechende Fehlvorstellung begründen. Solange im Markt allerdings lediglich Gerüchte kursieren, die nicht auf Kommunikation des Emittenten zurückzuführen sind und die nicht aus anderen Gründen hinreichend konkret sind, ist eine *no comment policy* dringend anzuraten.[47]

c. Sicherstellung der Geheimhaltung

Schließlich muss der Emittent gem. Art. 17 Abs. 4 UAbs. 1 lit. c) MAR die Geheimhaltung der Information sicherstellen.

Neben den stets zu berücksichtigenden Grundsätzen für die Sicherstellung der Geheimhaltung ist im Falle von Cyberangriffen insbesondere das Zusammenspiel mit den im Einzelfall parallel eingreifenden Publizitätspflichten nach dem BSIG und der DSGVO zu berücksichtigen. Aus Art. 4 Abs. 1 lit. c) i) DurchführungsVO (EU) 2016/1055 ergibt sich, dass Emittenten sicherstellen müssen, dass lediglich Personen, denen gegenüber eine Offenlegung der Insiderinformation nach Art. 10 MAR erfolgen darf, Zugang zu der Information haben. Nach Art. 10 MAR ist eine Offenlegung insbesondere erlaubt, wenn die Offenlegung im Zuge der normalen Ausübung einer Beschäftigung oder eines Berufs oder der normalen Erfül-

44 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 251.
45 *Kumpan* in: Baumbach/Hopt, HGB, Art. 17 MAR Rn. 18.
46 ESMA/2016/1130 Annex V Nr. 3.2.5 Rn. 80.
47 ESMA, Questions and Answers on the Market Abuse Regulation (MAR), Version 14, 29. März 2019, ESMA70–145–111, S. 13; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 129; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 259.

lung von Aufgaben geschieht. Dies erfasst insbesondere die Erfüllung anderer gesetzlicher Publizitätspflichten. Auch wenn grundsätzlich zu prüfen ist, ob auch die jeweilige Informationspflicht Vorrang gegenüber dem insiderrechtlichen Weitergabeverbot genießt,[48] kann jedenfalls für die Pflichten nach dem BSIG und der DSGVO festgehalten werden, dass diese zur Weitergabe berechtigen. Zwar dient die Benachrichtigungspflicht nach Art. 34 DSGVO nicht der normalen Ausübung einer Beschäftigung oder eines Berufes, allerdings verfolgt Art. 34 DSGVO mit dem Schutz der persönlichen Rechte und Freiheiten von natürlichen Personen ein wichtiges Regelungsziel. Der Schutz der Funktionsfähigkeit des Kapitalmarktes muss in diesem Fall über die unverzügliche Veröffentlichung der Insiderinformation gewährleistet werden. Auch die weiteren Veröffentlichungspflichten nach dem BSIG und DSGVO berechtigen zur Weitergabe an die jeweils zuständige Behörde. Die Pflichten enthalten – anders als bspw. das Informationsrecht des Aktionärs gem. § 131 Abs. 1, 3 Nr. 5 AktG – keinen Vorbehalt hinsichtlich etwaiger entgegenstehender Pflichten. Zudem erfüllen auch sie mit dem Schutz der Funktionsfähigkeit kritischer Infrastruktur und dem Schutz personenbezogener Daten wichtige Regelungszwecke, die im Rahmen einer Abwägung Vorrang vor dem insiderrechtlichen Weitergabeverbot haben. Eine Veröffentlichungspflicht gem. Art. 17 Abs. 8 MAR wegen nach Art. 10 Abs. 1 MAR erfolgter Offenlegung greift allerdings in der Regel wegen § 67 BBG, § 30 VwVfG und den landesspezifischen Äquivalenten nicht ein.

Während die Erfüllung der Benachrichtigungspflicht nach Art. 34 DSGVO deshalb im Ergebnis zum Entfallen der Aufschubbefugnis führt, da die Geheimhaltung nicht mehr sichergestellt werden kann, führen die Pflichten nach dem BSIG und nach Art. 33 DSGVO in der Regel nicht zu einem Entfallen der Aufschubbefugnis. Allerdings ist auch das BSI nach § 7 Abs. 1 S. 1 Nr. 1 BSIG berechtigt, Warnungen an die Öffentlichkeit oder an die betroffenen Kreise zu richten. Enthält eine solche Warnung keinen konkreten Bezug zum IT-Sicherheitsvorfall des Emittenten, besteht keine Gefahr, dass die Geheimhaltung nicht sichergestellt werden kann. Insbesondere wenn die Warnung allerdings gem. § 7 Abs. 1 S. 1 Nr. 1 lit. c) BSIG über den Verlust von oder den unerlaubten Zugriff auf Daten informiert und insoweit ein erkennbarer Zusammenhang zu der aufgeschobenen Insiderinformation besteht, kann die Sicherstellung der Geheimhaltung im Einzelfall gefährdet sein.

48 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 10 Rn. 98.

Schließlich können erfolgreiche Cyberangriffe auch Auswirkungen auf die Pflicht zur Veröffentlichung anderer Insiderinformationen haben, wenn deren Veröffentlichung gem. Art. 17 Abs. 4 MAR bislang aufgeschoben wurde, der Cyberangriff allerdings zu einem Abfluss von Daten geführt hat und nicht ausgeschlossen werden kann, dass auch die Insiderinformation hiervon betroffen ist. In diesem Fall ist die Information unverzüglich zu veröffentlichen.

5. Verfahren und Inhalt der Mitteilung

Die Ad-hoc-Mitteilung muss gem. Art. 17 Abs. 1 UAbs. 1 MAR unverzüglich, d.h. ohne schuldhaftes Zögern,[49] erfolgen. Dies erfordert, dass der Emittent alle erforderlichen und zumutbaren Vorkehrungen trifft, um die Information zu erkennen, ggf. den Sachverhalt weiter aufzuklären und die Information weiterzuleiten sowie zu analysieren und zu veröffentlichen.[50] Die Berücksichtigung einer Frist auch für die weitere Aufklärung der Information ist nicht gleichzusetzen mit der Möglichkeit, den Sachverhalt zunächst „auszuermitteln". Denn der Emittent muss auch das Interesse des Marktes an einer zügigen Veröffentlichung berücksichtigen. Er muss abwägen, ob der Nutzen, den er von der weiteren Ermittlung für den Kapitalmarkt erwartet, das Interesse des Marktes an der Veröffentlichung der Information in der aktuellen Form überwiegt.[51]

Der Inhalt der Mitteilung ergibt sich aus Art. 17 Abs. 1 UAbs. 2 MAR i.V.m. Art. 2 Abs. 1 lit. b) VO (EU) 2016/1055 und § 26 Abs. 4 WpHG i.V.m. § 4 WpAV. Erforderlich sind sowohl Angaben zum Emittenten als auch zur Insiderinformation. Weitere Erläuterungen finden sich im Modul C des Emittentenleitfaden der BaFin.[52] Die Information muss gem. Art. 2, 3 VO (EU) 2016/1055 über öffentlich zugängliche Medien verbreitet werden. Sind die Wertpapiere zum Handel an einem geregelten Markt zugelassen, ist die Information in einem amtlich bestellten System zu veröffentlichen.

---

49 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 116. Für ein objektives, nicht an § 121 BGB angelehntes Verständnis: *Kumpan/Schmidt* in: Schwark/Zimmer, Kapitalmarktrechts-Kommentar, 5. Aufl. 2020, Art. 17 MAR Rn. 72.

50 ESMA/2016/162 Rn. 64, 67; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 129; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 116 ff.

51 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 125.

52 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 43 ff.

Nach der Veröffentlichung ist der Emittent nicht verpflichtet, die Ad-hoc-Mitteilung zu aktualisieren, es sei denn, der neu eingetretene Umstand erfüllt für sich genommen den Tatbestand einer Insiderinformation.[53] Ist die Information hingegen so unvollständig oder fehlerhaft veröffentlicht worden, dass die Bewertung der Information durch den Kapitalmarkt beeinträchtigt wird, besteht eine Pflicht des Emittenten, die Ad-hoc-Mitteilung nach Maßgabe von § 4 Abs. 3 WpAV zu korrigieren.[54]

6. Sanktionen

Die in Betracht kommenden Sanktionen bei Verstößen gegen die Pflicht zur Veröffentlichung von Insiderinformationen sind mannigfaltig. Eine Strafbarkeit kommt grundsätzlich nur bei gleichzeitigem Verstoß gegen das Verbot der Marktmanipulation in Betracht (§ 119 Abs. 1 WpHG).[55] Allerdings können nach § 120 Abs. 15 Nr. 6–11, Abs. 18 WpHG Bußgelder[56] von bis zu einer Million Euro, gegenüber juristischen Personen dem höheren der Beträge von bis zu zweieinhalb Millionen Euro oder bis zu 2 Prozent des Gesamtumsatzes verhängt werden. Zudem kann der Verstoß nach § 120 Abs. 18 S. 3, 4 WpHG mit dem dreifachen des geschätzten gezogenen wirtschaftlichen Vorteils geahndet werden.[57] Die Bußgeldandrohung richtet sich sowohl an die Leitung des Emittenten als auch an den Emittenten selbst. Schließlich ist auch auf die Bekanntmachung von Sanktionen (sog. *naming and shaming*) und auf die zivilrechtliche Haftung des Emittenten aus §§ 97, 98 WpHG und aus § 826 BGB hinzuweisen.[58]

---

53 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 46; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 179.

54 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 46; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 182.

55 *Rönnau/Wegner* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 28.

56 *Rönnau/Wegner* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 29.

57 S. auch BaFin, WpHG, Bußgeldleitlinien II, Stand: Februar 2017.

58 *Wolf/Wink* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 30.

V. Schlussfolgerungen

Cyberangriffe können diverse Offenlegungspflichten auslösen. Diese sind inhaltlich nicht deckungsgleich, da sie unterschiedliche Regelungszwecke verfolgen, haben aber eine gemeinsame Schnittmenge. Insbesondere nach Zustimmung des Bundesrates zum geänderten IT-Sicherheitsgesetz steigt die Wahrscheinlichkeit für ein börsennotiertes Unternehmen, sowohl einer Publizitätspflicht nach Art. 17 MAR als auch nach § 8f BSIG zu unterliegen, deutlich. Sind von dem Ereignis personenbezogene Daten betroffen, greifen zudem die Vorgaben der DSGVO.

Jedenfalls aus kapitalmarktrechtlicher Perspektive besteht keine aufsichtsrechtliche Pflicht, eine Compliance-Organisation zu etablieren, um die Ad-hoc-Publizitätspflicht zu erfüllen.[59] Allerdings lässt sich jedenfalls aus gesellschaftsrechtlicher Perspektive für alle der diskutierten Offenlegungspflichten aus der Legalitätspflicht der Geschäftsleitung die Pflicht ableiten, Vorkehrungen zu treffen, potentiell offenlegungspflichtige Informationen zu erkennen, zu bewerten und entsprechend der jeweiligen Offenlegungspflicht zu veröffentlichen.[60] Zu diesem Zweck bietet es sich an, die für die Erfüllung aller Offenlegungspflichten erforderlichen Informationen zentral zusammenzustellen und den jeweils für die Erfüllung der Offenlegungspflichten zuständigen Personen regelbasiert zur Verfügung zu stellen.

59 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 25.

60 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 26.

Unternehmerische IT-Compliance in China: Cybersecurity und Künstliche Intelligenz

Dennis-Kenji Kipker

A. Einführung

Wirtschaftsbeziehungen machen nicht an Landesgrenzen halt – ebenso wenig die transnationalen Datenströme. Ganz im Gegenteil: Wo einerseits weltwirtschaftlich immer mehr an Vernetzung stattfindet, so spiegelt sich diese denknotwendigerweise auch im internationalen und digitalen Informationsaustausch wider. Dabei ist der Informationsaustausch aber mit nicht unerheblichen Risiken für die Cybersicherheit verbunden, und so werden nicht nur der deutsche und der europäische Gesetzgeber tätig, um den zunehmend gefährdeten Cyberraum abzusichern, sondern ebenso die Rechtssetzungsorgane anderer Staaten weltweit. Dies bedeutet folglich auch, dass international tätige Unternehmen – gleichgültig, ob Großkonzern oder KMU – sich im Rahmen ihrer IT-Compliance nicht nur darauf beschränken können, die gesetzlichen Regelungen ihres jeweiligen Herkunftslandes zu beachten, sondern sich genauso auf die Vielzahl an neuen Rechtsvorschriften in der Cybersicherheit einstellen müssen, die aktuell weltweit verabschiedet werden. Das ist nicht selten aufgrund der kulturellen, aber auch der sprachlichen Barrieren, eine erhebliche Herausforderung. Der vorliegende Beitrag widmet sich im Speziellen der Cybersicherheitsgesetzgebung in der Volksrepublik China, und hier mit einem Schwerpunkt auf dem Thema der Künstlichen Intelligenz (KI) als einer Schlüsseltechnologie, die nicht nur für die Cybersicherheit, sondern auch für die globale politische und wirtschaftliche Entwicklung des nächsten Jahrzehnts eine herausragende Relevanz besitzt.*

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag beruht, ist abrufbar unter https://doi.org/10.17176/20210315-161623-0.

B. Regelungssystematik und politische Strategien

Mit einem Blick auf die rechtliche Entwicklung der Cybersicherheit in China wird recht schnell deutlich: China besitzt schon seit Jahrzehnten eine mehrschichtige Gesetzgebung zur IT-Sicherheit, und dürfte auf diesem Feld damit zu den globalen Vorreitern zählen. Das erste IT-sicherheitsrelevante Gesetz, die „Computer Information System Security Protection Regulations of the People's Republic of China", wurde in der Volksrepublik schon 1994 verabschiedet. In den letzten Jahren ist die chinesische IT-Sicherheitsgesetzgebung auch in westlichen Staaten immer wieder in den Fokus der öffentlichen Wahrnehmung gelangt. Das ist vor allem auf die Tatsache zurückzuführen, dass eine Vielzahl westlicher Unternehmen geschäftliche Niederlassungen in China betreibt, die dementsprechend von der neuen chinesischen Gesetzgebung zur IT-Sicherheit betroffen sind. Erschwerend hinzu tritt die unübersichtliche Behörden- und Zuständigkeitsstruktur auf mehreren Verwaltungsebenen sowie die Tatsache, dass viele Gesetze eher generalklauselartig formuliert sind und so weite begriffliche Interpretationsspielräume in ihrer konkreten Anwendung bestehen lassen.

Ein eigenständiges KI-Gesetz, das die IT-Sicherheit umfassend aufgreift und reguliert, existiert in China gegenwärtig dennoch nicht. Gleichwohl enthalten verschiedene andere chinesische Gesetze durch die Regulierung von technisch-organisatorischen Einsatzszenarien Bezugspunkte zur KI und zu möglichen (zukünftigen) Anwendungsfeldern, die sich hieraus entwickeln können. Trotz noch fehlender bereichsspezifischer KI-Gesetzgebung zur IT-Sicherheit bedeutet dies nicht, dass die Volksrepublik im Bereich der allgemeinen KI-Gesetzgebung nicht schon umfassend tätig ist.[1] Die Relevanz, die Peking dem Thema KI beimisst, wird außerdem durch die Strategie des Staatsrats deutlich, bis zum Jahr 2025 die weltweite Führungsposition bei KI zu übernehmen, und bis zum Jahr 2030 die weltweite Vormachtstellung zu erlangen, sowohl politisch wie auch wirtschaftlich.[2] Außerdem benennt der „Next Generation Artificial Intelligence Development Plan" (AIDP) aus Juli 2017 KI als eine zentrale Maßnahme zur Förderung der nationalen, wirtschaftlichen und sozialen Sicherheit von

1 Weiterführend dazu Roberts *et al.*, The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation, AI & Society 2020, https://doi.org/10.1007/s00146-020-00992-2 (abgerufen am 05.10.2020).

2 Konrad Adenauer Stiftung (Hrsg.), Vergleich nationaler Strategien zur Förderung von Künstlicher Intelligenz – Teil 1, 2018, S. 18 ff. mwN., so auch *Roberts et al.* (Fn.), ausdrücklich Bezug nehmend auf den Zehnjahresplan „Made in China 2025".

China.[3] In dem Dokument wird auf Sicherheitsaspekte von KI-Entwicklung nicht unter dem Aspekt der „Security", sondern auf die „Safety" verwiesen. Die Gefahren bei der KI-Nutzung werden folglich vorrangig nicht im Schutz des KI-Systems vor dem Menschen, sondern im Schutz des Menschen bzw. der durch ihn betriebenen Einrichtungen vor einer fehlgeleiteten KI und den dadurch eintretenden Schäden gesehen. Die IT-Sicherheit als solche rückt bei der gesetzgeberischen Betrachtung somit (zurzeit noch) in den Hintergrund.

Im Folgenden werden drei zentrale und aktuelle gesetzgeberische Maßnahmen zur IT-Sicherheit in China in einem Überblick vorgestellt: das Chinese Cybersecurity Law (CSL) aus 2016, das New Chinese Cryptography Law aus 2019 und das Chinese Data Security Law (DSL), das gegenwärtig noch in einer Entwurfsfassung aus 2020 vorliegt. Relevant ist unter Gesichtspunkten der Datensicherheit daneben das Personal Information Protection Law, das sich ebenfalls noch im Gesetzgebungsverfahren befindet. Wichtig ist, dass die chinesischen Rechtsgrundlagen zur IT- und Datensicherheit stets im Zusammenhang betrachtet werden, da sich die Regulierungsbereiche von einzelnen Gesetzen durchaus überschneiden können.

C. *Chinese Cybersecurity Law*

Das 2016 verabschiedete und im Juni 2017 in Kraft getretene CSL enthält sowohl Vorschriften zur IT-Sicherheit als auch zum Datenschutz – womit es eine der ersten gesetzlichen Regelungen in China gewesen ist, die explizit datenschutzrechtliche Anforderungen adressierte.[4] Hierzulande gelangte das Gesetz durch die Themen Regulierung von VPN-Verbindungen, Produktzulassung und Datenlokalisierung in das Blickfeld der öffentlichen Wahrnehmung zahlreicher Wirtschaftsunternehmen.[5] Als Hauptziele des CSL beschrieben werden die Sicherstellung der Netzwerksicherheit (im

3 China Association for International Science and Technology Cooperation, Next Generation Artificial Intelligence Development Plan Issued by State Council, http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf (abgerufen am 01.10.2020).

4 Zur Analyse der Entwurfsfassung des CSL aus 2015 siehe *Kipker*, MMR-Aktuell 2015, 370972, hierzu aktuell weiterführend *Chen/Han/Kipker*, An Introduction into the New Chinese Data Protection Legal Framework, DuD 2020, 52.

5 Vgl. *Kipker*, Chinese Cybersecurity Law: Neue rechtliche Wege und Umwege nach China, Tagungsband des BSI-Kongresses 2019, S. 475.

Wesentlichen gleichzusetzen mit der IT-Sicherheit), die Aufrechterhaltung der Souveränität im Cyberspace, der Schutz der nationalen Sicherheit und des öffentlichen Interesses, der Schutz der Rechte und Interessen von Bürgern, Rechtspersonen und sonstigen Einrichtungen, und eine Förderung der wirtschaftlichen und sozialen Entwicklung der Gesellschaft. Insbesondere die Kapitel 2 „Support and Promotion of Network Security", 3 „Network Operations Security" und 5 „Monitoring, Early Warnings, and Emergency Responses" enthalten zentrale Vorgaben zur IT-Sicherheit. Auf KI wird dabei jedoch nicht unmittelbar Bezug genommen, jedoch lässt sich über folgende Vorschriften des Gesetzes ein KI-Bezug herstellen:

- Art. 5: Der Staat hat die Aufgabe, IT-Sicherheitsrisiken zu überwachen und ihnen vorzubeugen, kritische Infrastrukturen zu schützen und rechtswidrige bzw. kriminelle Netzwerkaktivitäten zu erkennen, und auf diese Weise die Sicherheit und Ordnung im Cyberspace zu gewährleisten.
- Art. 7: Der Staat beteiligt sich an internationalem Austausch und Kooperation in der Entwicklung und Nutzung von Netzwerktechnologien, und formuliert entsprechende Standards.
- Art. 10: Es sind Maßnahmen vorzuhalten, die die Netzwerksicherheit und operationelle Stabilität des Netzwerks gewährleisten, und Maßnahmen umzusetzen, die effektiv auf Sicherheitsvorfälle reagieren, und Cyberkriminalität vorbeugen.
- Art. 15: Der Staat begründet, unterhält und verbessert ein System von Netzwerksicherheitsstandards.
- Art. 18: Der Staat fördert die Entwicklung von IT-Sicherheitstechnologien, und unterstützt innovative Maßnahmen zur Netzwerksicherheit. Hierzu können auch neue Netzwerktechnologien eingesetzt werden.
- Art. 21: Ein System der Netzwerksicherheit ist zu etablieren, das entsprechende technische Maßnahmen zum Schutz vor Computerviren, Netzwerkangriffen, und sonstigen schädlichen Eingriffen enthält. Die Maßnahmen umfassen ebenfalls die Überwachung und Aufzeichnung des Netzwerkstatus und von IT-Sicherheitsvorfällen.
- Art. 51: Der Staat richtet Systeme zur Netzwerküberwachung ein, sowie zu Frühwarnungen.

Auf der Grundlage des CSL wurden und werden überdies verschiedene untergesetzliche Regelwerke sowie technische Normen und Standards verfasst, bzw. sind in Bearbeitung, die ebenfalls ein Einfallstor für KI und

IT-Sicherheit bilden.[6] Hier dürfte in den kommenden Jahren am ehesten eine weitere konkrete Ausgestaltung des CSL zu verorten sein. Auffällig ist dabei aber, dass IT-Sicherheit in Bezug auf KI gegenwärtig nicht zu den Schlüsseltechnologien gezählt wird, die Entwicklung ist hier vielmehr noch allgemeiner gehalten bzw. bezieht sich auf andere Anwendungsfelder, so werden genannt: Machine Learning, knowledge graphs, natural language processing, human-computer interaction, computer vision, biometric feature recognition und virtual reality/augmented reality – in dem Zusammenhang wird jedoch der Ausblick gegeben, dass die chinesische KI-Entwicklung zukünftig nicht von bereichsspezifischen, sondern von allgemeinen Anwendungsfeldern ausgeht, die eine Vielfalt möglicher Einsatzszenarien abdecken, sodass hiervon zwangsläufig auch IT-Sicherheit umfasst ist.[7]

D. Chinese Cryptography Law

Das neue chinesische Kryptografiegesetz wurde im Oktober 2019 verabschiedet und trat zum 1.1.2020 in Kraft (vgl. Art. 44 des Gesetzes).[8] Ziel des Gesetzes ist die Entwicklung neuer kryptografischer Verfahren, Dienste und Produkte in China, womit auch die Stärkung der IT-Sicherheit einhergeht – explizit wird dies in Art. 1 des Gesetzes hervorgehoben. Die IT-Sicherheit steht dabei im Fokus der öffentlichen und nationalen Sicherheitsinteressen Chinas.[9] Insoweit bestehen von der rechtspolitischen Zielsetzung deutliche Parallelen zum CSL. Auch das Kryptografiegesetz enthält aber keine ausdrückliche Bezugnahme auf KI, sodass auch hier der Bezug mittelbar durch die Auslegung des Gesetzes herzustellen ist. Dies ist aufgrund der generalklauselartigen Formulierung vieler chinesischer Rechtsvorschriften aber nicht unbedingt als Hinweis dahingehend zu in-

6 Im Überblick dazu *Kipker/Scholz*, Cybersicherheit und Datenschutz in China – TC 260 stellt neue Normungsentwürfe vor, DuD 2018, 768.

7 China Electronics Standardization Institute (CESI)/Standardization Administration of China (SAC), Artificial Intelligence Standardization White Paper (2018 Edition), S. 20 f., http://www.cesi.cn/images/editor/20180124/20180124135528742.pdf (abgerufen am 01.10.2020).

8 Für die vollständige englische Sprachfassung des Cryptography Law of the People's Republic of China: https://www.chinalawtranslate.com/en/cryptography-law/ (abgerufen am 01.10.2020).

9 Zum Entwurf und zur rechtspolitischen Debatte zum chinesischen Kryptografiegesetz siehe *Kipker/Scholz*, China: Neue Vorgaben zur Cybersicherheit – Entwurf des Kryptografiegesetzes veröffentlicht, MMR-Aktuell 2019, 419468.

terpretieren, dass das Gesetz eine KI-Regulierung ausschließt. Wie auch für das EU-Recht erweist sich die Technologieoffenheit des chinesischen Rechts insoweit als signifikanter Vorteil, wenn es um Flexibilität und Anpassungsoffenheit im Hinblick auf die Einbindung neuer Technologien geht.

Systematisch untergliedert sich das Chinese Cryptography Law in die fünf Kapitel „General Provisions", „Core Cryptography, Common Cryptography", „Commercial Cryptography", „Legal Responsibility" und „Supplementary Provisions". Den Kern der Regelungen bildet die Unterscheidung zwischen verschiedenen kryptografischen Verfahren, an die stufenmäßig unterschiedliche Nutzungsanforderungen angelegt werden: „Core Cryptography", „Common Cryptography" sowie „Commercial Cryptography". Die beiden erstgenannten Verfahren sollen zum Schutz von Staatsgeheimnissen eingesetzt werden, demgemäß unterfallen sie als Staatsgeheimnis selbst einem entsprechenden Schutz. Die drittgenannte Kategorie kryptografischer Verfahren, die „Commercial Cryptography", wird für den Schutz jeglicher Information herangezogen, die kein Staatsgeheimnis ist – im Umkehrschluss ist sie somit zur Verschlüsselung sämtlicher herkömmlicher Daten nutzbar, um die IT-Sicherheit von Unternehmen und Privatpersonen zu gewährleisten. Insbesondere bei der Entwicklung und Anwendung kryptografischer Verfahren ist sicherzustellen, dass diese informationstechnisch nicht kompromittiert werden, vgl. Art 17 (für „Core Cryptography" und „Common Cryptography") und Art. 24 (für „Commercial Cryptography") des chinesischen Kryptografiegesetzes. Ein direkter Bezug zum CSL ergibt sich für die Überprüfung kryptografischer Produkte überdies aus Art. 26 und Art. 27 des Kryptografiegesetzes.

E. Chinese Data Security Law

Die hohe Bedeutung, die die chinesische Regierung der IT- und Datensicherheit bemisst, wird durch das umfängliche gesetzgeberische Tätigwerden der vergangenen Jahre besonders deutlich. So wurde Anfang Juli 2020 der Entwurf für ein neues chinesisches Datensicherheitsgesetz (Data Security Law, DSL) vom Standing Committee of the National People's Congress (NPC) veröffentlicht, der bis zum 16. August 2020 zu öffentlichen

Kommentierung zur Verfügung stand.[10] Das Gesetz betrifft die Datenverarbeitungsaktivitäten in Mainland China (vgl. Art. 2). Da es sich bei dem veröffentlichten Entwurf um eine frühe erste Entwurfsfassung handelt, ist im weiteren Verlauf des Gesetzgebungsverfahrens noch mit Änderungen zu rechnen. Das DSL wird systematisch als gleichrangige Regelung neben dem CSL stehen, und regelt über die IT- und Datensicherheit hinaus in erster Linie den Umgang mit Daten als Wirtschaftsgut, die Modalitäten von Datenverarbeitungsvorgängen, die Regelung von Zugriffsmöglichkeiten, und Möglichkeiten zu Open Data. Der Entwurf des Gesetzes untergliedert sich in insgesamt sieben Kapitel, die vom Allgemeinen zum Speziellen hin aufgebaut sind. Unter KI- und IT-Sicherheitsgesichtspunkten relevant sind das Kapitel 2 („Data Security and Development"), das Kapitel 3 („Data Security Systems"), das Kapitel 4 („Data Security Protection Responsibilities") und das Kapitel 5 („Government Data Security and Openness"). Folgende Vorschriften des Gesetzentwurfs sind im Einzelnen auch unter Gesichtspunkten von KI-Entwicklung besonders hervorzuheben:

- Art. 12: Der Staat ergreift Maßnahmen, um einerseits die Datensicherheit zu befördern, andererseits aber auch die Datennutzung zu ermöglichen. IT-Sicherheit wird als zentrales Kriterium der industriellen Entwicklung in China genannt.
- Art. 13: Der Staat verabschiedet eine Big Data-Strategie. Zur Datennutzung im Rahmen von Big Data sind innovative Technologien notwendig, wie beispielsweise sichere KI-gestützte Methoden der Datenauswertung.
- Art. 14: Der Staat fördert die wissenschaftliche Forschung im Bereich der Datenentwicklung und Datennutzung. Dabei wird ebenfalls die Datensicherheit genannt. In diesem Zusammenhang ist Art. 18 des Gesetzes zu sehen, der vorschreibt, dass der Staat personelle Ressourcen zur Datennutzung und Datensicherheit entwickelt.
- Ein Kernelement des DSL sind die Vorgaben in den Art. 19 ff. (Kapitel 3: „Data Security Systems"). Demnach werden die Datenbestände in unterschiedliche Schutzklassen unterteilt, jeweils in Abhängigkeit der Bedeutung für die wirtschaftliche und soziale Entwicklung, und gemessen an den Auswirkungen auf die nationale Sicherheit, das öffentliche Interesse und die Rechtsordnung. Hierzu baut der Staat u. a. ein zentralisiertes System der Risikoüberwachung auf, das ebenfalls ein Früh-

10 Data Security Law of the People's Republic of China (draft version), https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf (abgerufen am 01.10.2020).

warnsystem enthalten kann – ein klassisches Einfallstor für KI in der IT-Sicherheit (vgl. Art. 20). Basierend auf detektierten Sicherheitsvorfällen sind die staatlichen Einrichtungen befugt, im Rahmen eines Notfallmanagements entsprechende Gegenmaßnahmen zu ergreifen (Art. 21).

- Art. 25: In dieser Bestimmung wird festgelegt, dass für die Datenverarbeitung Verantwortliche ein compliancegerechtes Management zur Datensicherheit etablieren müssen, das sich auf den gesamten Arbeitsablauf der Organisation erstreckt. Entsprechende technische Maßnahmen zur Datensicherheit müssen etabliert werden. Solche technischen Maßnahmen können letztlich auch KI umfassen.
- Art. 27: Soweit Daten verarbeitet werden, sollte eine Risikoüberwachung etabliert werden, die auch die IT- bzw. Datensicherheit betrifft. Eine solche Risikoüberwachung kann KI-gesteuert erfolgen.
- Art. 36: Staatliche Einrichtungen, die Daten verarbeiten, müssen ein Management zur Datensicherheit implementieren. Art. 37 DSL bestimmt weitergehend, dass sich staatliche Einrichtungen ihrer Pflicht zur Datensicherheit nicht dadurch entledigen können, indem sie die Datenverarbeitung an Dritte auslagern. Die Einhaltung entsprechender technisch-organisatorischer Maßnahmen ist weiterhin zu überwachen.
- Art. 41: Die IT- und Datensicherheit ist in einem fortlaufenden Prozess sicherzustellen – dies gilt sowohl für Aufsichtsbehörden als auch für datenverarbeitende Stellen.

F. Fazit und Ausblick

Bei einem Blick auf die chinesische Cyber-Sicherheitsgesetzgebung wird schnell deutlich, dass es nicht um ein einzelnes Gesetz geht, sondern eine Vielzahl unterschiedlichster Rechtsquellen, aber auch untergesetzliche Regelwerke sowie außerhalb des Rechts liegende technische Normen und Standards ausschlaggebend sind, um den regulatorischen Rahmen des Themas in China zu bestimmen. Das Zusammenspiel dieser unterschiedlichen Erkenntnisquellen mit jeweils verschiedener Granularität und Ansprüchen, aber auch das Fehlen einer transparenten und zentralisierten Kommunikationsstruktur erschwert den Umgang mit Compliance-Anforderungen zur Cybersecurity für Unternehmen in China enorm. Hinzu tritt, dass für weite Bereiche der chinesischen Cybersicherheitsgesetzgebung die Konkretisierung durch untergesetzliche Rechtsvorschriften und technische Normen und Standards noch nicht vollständig abgeschlossen ist bzw. zurzeit noch fortdauert und das Ende dieser Übergangsphase zur-

zeit nicht absehbar ist. Ausländische Unternehmen stehen hier aufgrund der undurchsichtigen chinesischen Behördenstruktur außerdem vor dem Problem, geeignete Ansprechpartner zu finden. Und selbst wenn ein solcher gefunden sein sollte, ist unklar, ob dieser eine rechtsverbindliche Auskunft erteilen kann oder darf. Kompetenzkonflikte zwischen den unterschiedlichen zuständigen Behörden und die sprachliche sowie kulturelle Barriere verschärfen diese Problematik. Die unklare Gesetzeslage tangiert dabei nicht nur betroffene Unternehmen selbst, sondern auch rechtsberatende Einrichtungen, die im Ausland tätig sind, weshalb verlässlicher und hinreichend verbindlicher (rechtssicherer) juristischer Rat im Hinblick auf das chinesische Recht der Cybersicherheit nicht leicht zu finden ist.

Angesichts der zahlreichen Unklarheiten von gesetzgeberischer Seite bleibt deshalb zumindest vorerst nur der Weg, die Implementierung der chinesischen Rechtsvorschriften zur Cybersicherheit weitestgehend über Best Practices voranzutreiben, die vor allem auch durch mittelständische deutsche Unternehmen entwickelt werden, die auf dem chinesischen Markt tätig sind. Nicht selten haben diese aufgrund jahrelanger Erfahrungen mit chinesischen Behörden und Providern einen Erfahrungsschatz gesammelt, der zwar keine klassische „Rechtssicherheit", wie wir sie hierzulande kennen, vermittelt, aber doch bei der Einschätzung, Kalkulierbarkeit und Prognose der rechtspolitischen Entwicklung und des behördlichen Handelns in China unterstützt. Zudem verfügen entsprechende Firmen zumeist über die notwendigen Kontakte zu Behörden und Geschäftspartnern, die essenzielle Voraussetzung für eine erfolgreiche unternehmerische Tätigkeit auf dem chinesischen Markt sind. Hier ist es wünschenswert, unter den betroffenen deutschen Unternehmen ein entsprechendes nationales Netzwerk für den Informations- und Erfahrungsaustausch zu etablieren. Soweit es die Kommunikation mit den chinesischen Behörden anbelangt, bleibt zu hoffen, dass auf absehbare Zeit konsolidierte Kommunikationskanäle und zentrale Ansprechstellen geschaffen werden, die bei der Beantwortung wesentlicher Fragestellungen zur Implementierung der Vorgaben des chinesischen Rechts der Cybersecurity unterstützen und insoweit auch über die notwendige Kompetenz zur Rechtsverbindlichkeit – und damit Rechtssicherheit – verfügen.

Dass für eine derartige Rechtsverbindlichkeit und Rechtssicherheit dringender Bedarf besteht, wird mit einem Blick auf die künftige politische und wirtschaftliche Schlüsseltechnologie Künstliche Intelligenz besonders deutlich, denn auch wenn die Volksrepublik China im kommenden Jahrzehnt die weltweite Technologieführerschaft für diesen Bereich für sich beansprucht, so befinden sich dennoch viele der in diesem Beitrag vorgestellten und diskutierten Regulierungsansätze in den unterschiedlichen

Cybersecurity-Gesetzen noch im Anfangsstadium. Für die KI-Regulierung im Zusammenhang mit der IT-Sicherheit ist ferner auffällig, dass es sich um einen klassischen Fall handelt, in dem das Recht den Risiken folgt, die sich aus der technologischen Entwicklung heraus ergeben – und es nicht umgekehrt das Recht ist, das zunächst die Rahmenbedingungen für sichere Technologieentwicklung und Einsatzszenarien setzt.

Die IT-Sicherheit von KI ist stets aus zwei unterschiedlichen Perspektiven zu betrachten: Einerseits sind die möglichen Einsatzszenarien zu berücksichtigen, die sich zur Verbesserung und Förderung der IT-Sicherheit durch KI-Maßnahmen ergeben können, andererseits sind die Risiken zu ermitteln und einzuschätzen, die eine fehlerhaft entwickelte KI für die IT-Sicherheit mit sich bringen kann. Dieser Dualismus findet sich in der gegenwärtigen Rechtslage noch kaum wieder – geht es doch in vielen IT-sicherheitsbezogenen Rechtsvorschriften der Volksrepublik nur darum, dass diese bewusst entwicklungsoffen und damit gleichermaßen unbestimmt formuliert sind, um die Möglichkeit zu bieten, KI als technisch-organisatorische Vorkehrung in die weiteren Rahmenbedingungen des chinesischen IT-Rechts aufzunehmen. Mit erheblicher Wahrscheinlichkeit wird man jedoch davon ausgehen können, dass die chinesische Gesetzgebung hier in den kommenden Jahren nach und nach weitere und auch konkretere Vorgaben zur sicheren KI-Nutzung entwickelt – nicht zuletzt auch deshalb, weil China die Entwicklung von KI-Technologien zu einer Hauptfrage der gegenwärtigen und zukünftigen technologischen Stoßrichtung des Landes gemacht hat. Nichtsdestotrotz dürfte gerade China mit Blick auf die KI-Gesetzgebung keine globale „model role“ einnehmen, da chinesische Gesetze ihrer Natur nach bereits unbestimmt formuliert sind, unabhängig davon, ob es um KI, Cybersecurity oder um andere Themen geht – sie haben vielmehr den Charakter einer rechtspolitischen „Blaupause“ für weitere und konkretere Maßnahmen in naher Zukunft. Umso mehr ergibt sich hier im internationalen Kontext auch die Chance für den EU-Gesetzgeber, transparente, verlässliche und einheitliche gesetzgeberische Vorgaben zu KI und Cybersecurity für den europäischen Binnenmarkt zu schaffen, um Unternehmen, Behörden und Verbraucher bei der (IT-) sicheren Entwicklung und Verwendung dieser neuen Technologie bestmöglich zu unterstützen. Schon für die EU DS-GVO hat sich nämlich in der Vergangenheit gezeigt, dass auch China den Blick auf Europa richtet.

IT-Sicherheitssysteme und Mitbestimmung des Betriebsrats

Katrin Haußmann

A. Der Mitbestimmungstatbestand: „technische Einrichtungen"

Die Einführung und Anwendung technischer Einrichtungen, die geeignet sind, Mitarbeiterverhalten oder -leistung zu kontrollieren, sind mitbestimmungspflichtig. Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG ist darauf gerichtet,

> *„Arbeitnehmer vor Beeinträchtigungen ihres Persönlichkeitsrechts durch den Einsatz technischer Überwachungseinrichtungen zu bewahren, die nicht durch schutzwerte Belange des Arbeitgebers gerechtfertigt und unverhältnismäßig sind".*[1]

Regelungszweck dieses Mitbestimmungstatbestandes ist es, den Einsatz eines Systems mitzugestalten, so dass Arbeitnehmer nicht *„beliebig zum Objekt einer Überwachungstechnik gemacht"* werden können, die personen- oder leistungsbezogene Informationen verarbeitet.[2] Der Tatbestand wurde eingeführt, als es außer der klassischen Stechuhr und Überwachungskameras wenige technische Einrichtungen gab, die den Begriff erfüllten. Der Begriff der „Überwachung" wird weit ausgelegt und schon dann bejaht, wenn durch einen technische Vorgang Informationen über das Verhalten oder die Leistung von Arbeitnehmern erhoben und aufgezeichnet werden, um sie auch späterer Wahrnehmung zugänglich zu machen. Das Bundesarbeitsgericht dehnt in ständiger Rechtsprechung den Mitbestimmungstatbestand über die Grenzen des Wortlauts („*(…) zur Überwachung (…) bestimmt*") auf alle zur Kontrolle geeigneten Systeme aus.[3] Dazu zählt nahezu jede Software sowie deren spätere Änderung oder Aktualisierung.[4]

---

1 BAG NZA 2018, 673, 674 Rn. 15.
2 BAG NZA 2018, 673, 674 Rn. 15.
3 BAG NJW 1976, 261; zuletzt BAG NZA 2017, 657.
4 LAG Hamm BeckRS 2005, 31048701 Rn. 54 (Zit. ausgelassen): „Auch wenn die Software Windows 2000 lediglich die Vorgängerversion ersetzt hat, schließt dieser Neueinsatz das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG nicht aus. Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG ist nämlich nicht nur bei der Einführung und erstmaligen Anwen-

IT-Sicherheitssysteme sind grundsätzlich geeignet, Mitarbeiterverhalten zu kontrollieren. Zeitgemäße Systeme vergleichen z.B. Aktivitäten eines Benutzerkontos mit dessen Normalverhalten, markieren Anomalien und bewerten Risiken, die sich daraus für die IT-Sicherheit ergeben können, ggf. zusammen mit anderen Risikofaktoren. Ist das Benutzerkonto einem Mitarbeiter eindeutig zugeordnet, liegen die Tatbestandsmerkmale des Mitbestimmungstatbestandes vor. Dem lässt sich zwar entgegenhalten, dass gerade die sicherheitsrelevanten Anomalien die konkrete Frage aufwerfen, ob ein Mitarbeiter selbst gerade den ihm zugeordneten Account nutzt, oder die Anomalie eher darauf hindeutet, dass ein anderer sich des individualisierten Zugangs bedient. Gleichwohl wird sich damit nicht begründen lassen, dass eine Verhaltensbeobachtung mit diesen Systemen nicht (auch) möglich wäre. Jedes System schreibt mindestens die sogenannten Log-Daten mit und erfasst damit das Nutzerverhalten. Im Regelfall lässt sich eine Nutzerkennung einer bestimmten Person zuordnen. Diese Daten können in sogenannten Security Information and Event Management-Systemen (kurz: „SIEM“) ausgewertet und mit dem üblichen Nutzerverhalten eines Accounts verglichen werden. Soweit die Technik der User/Entity Behavior Analytics eingesetzt wird (kurz: „UEBA“) wird der Normalwert, an dem das aktuelle Nutzerverhalten gemessen wird, individualisiert und variabilisiert.[5]

B. Reformvorschläge

Die derzeitige Auslegung des Mitbestimmungstatbestands zu technischen Systemen ist offensichtlich praxisfern. Sie wird den zeitlichen Abläufen von IT-Projekten nicht gerecht und berücksichtigt nicht die Geschwindigkeit, mit der generell Softwareanwendungen aktualisiert und speziell IT-Sicherheitssysteme dem Stand der Technik und der Sicherheitslage angepasst werden müssen. Es mehren sich die Vorschläge zu einer Reform des Mitbestimmungstatbestands.[6] Seit vielen Jahren wird vorgeschlagen, den Tatbestand auf seinen Wortlaut „*zur Überwachung (…) bestimmt*“ zurückzu-

---

dung von EDV-Anlagen betroffen, sondern auch bei der Einführung eines neuen Programms oder bei der Änderung von vorhandenen Programmen.“

5 Beispiel: Ein System dieser Art bieten Software-Anbieter wie Securonix oder SPLUNK an.

6 *Günther/Böglmüller*, NZA 2015, 1024, 1027; *Grimm*, ArbRB, 2015, 336, 339; *Ludwig/Rancke*, BB 2016, 2293; *Karthaus*, NZA 2017, 558, 561; *Wisskirchen/Schiller/Schwindling*, BB 2017, 2105.

führen.[7] Dann ließe sich bezogen auf IT-Sicherheitssysteme hervorheben, dass ihr primärer Zweck nicht die Mitarbeiterkontrolle selbst ist, sondern die IT-Sicherheit. Die Systeme kontrollieren als oberstes Suchkriterium typischerweise nicht namentlich identifizierte Mitarbeiter in ihrem Nutzerverhalten, sondern sie beobachten und bewerten sicherheitsrelevante Ereignisse („*incidents*" oder „*events*"). Bei der Aufklärung solcher Ereignisse ist u.U. die Einsicht in individualisierbare Nutzeraccounts erforderlich. Mit einer Rückführung des Mitbestimmungstatbestandes auf seinen Wortlaut ist derzeit nicht zu rechnen. Die Reduktion der Vorschrift auf den wesentlichen Regelungszweck ist dennoch dringend erforderlich. Da die Mitbestimmung kollektive Tatbestände erfassen soll, ist nicht einzusehen, warum schon die Möglichkeit der einzelfallbezogenen Einsichtnahme in personenbezogene Verhaltensdaten mit dem Betriebsrat geregelt werden sollte. Rechtfertigen lässt sich die Mitbestimmung bezogen auf solche technischen Systeme, die den Arbeitgeber in die Lage versetzen, automatisch Verhaltens- oder Leistungsdaten mehrerer Mitarbeiter vergleichend auszuwerten.[8] Außerdem könnte der Tatbestand mit dem Datenschutzrecht synchronisiert werden, indem an die Datenverarbeitung angeknüpft wird, und nicht an den Einsatz einer technischen Einrichtung. Weitere Reformvorschläge beziehen sich auf Verfahrensregelungen und schlagen Fristen für die Verhandlungen vor.[9] Erörtert wird auch die Einführung einer Erheblichkeitsschwelle.[10] Das Bundesarbeitsgericht lehnt eine – wie auch immer im Einzelnen verfasste – „Geringfügigkeitsschwelle" jedoch ab.[11] Nur vereinzelt hat das Bundesarbeitsgericht technische Systeme ausgenommen. Dies betraf zuletzt den Datenabgleich im Sanktionslistenscreening. In seiner Entscheidung vom 19. Dezember 2017[12] hat das Bundesarbeitsgericht den Abgleich von Terrorlisten und Mitarbeiterlisten mit Hilfe technischer Systeme von der Mitbestimmung ausgenommen. Die Begründung dazu lautet:

---

7 *Günther/Böglmüller*, NZA 2015, 1024, 1027; *Ludwig/Rancke*, BB 2016, 2293; *Wisskirchen/Schiller/Schwindling*, BB 2017, 2105.

8 *Haußmann/Thieme*, NZA 2019, 1612, 1618: Mitbestimmungspflichtig ist „[Nr. 6:] die automatisierte Verarbeitung personenbezogener Arbeitnehmerdaten zum Zwecke der vergleichenden Überwachung des Verhaltens oder der Leistung von Arbeitnehmern".

9 *Mengel*, NZA 2017, 1494, 1497 ff. für interne Untersuchungen.

10 *Kania,* in: Müller-Gloge et. al. (Hrsg.), ErfK zum Arbeitsrecht, 20. Aufl. 2020, § 87 BetrVG Rn. 57.

11 BAG BeckRS 2018, 27856.

12 BAG NZA 2018, 673.

> *„Die aufgrund des Datenabgleichs generierten Ergebnisse bilden weder ein konkretes Verhalten oder eine konkrete Leistung eines Arbeitnehmers ab, noch lassen sie auf solche schließen. Eine Identität dieser Statusdaten eines Arbeitnehmers, der auf einer „Terrorliste" geführten Person gibt Auskunft darüber, dass sich gegen diese eine Verbotsmaßnahme i.S.d. Bereitstellungsverbots richtet. Eine Aussage über ein tatsächliches betriebliches oder außerbetriebliches Verhalten des Arbeitnehmers, das einen Bezug zum Arbeitsverhältnis hat, ist damit nicht verbunden."*

Hier differenziert das Gericht also danach, ob tatsächlich Rückschlüsse auf das Verhalten eines Arbeitnehmers möglich sind. Auf andere Systeme bezogen ist diese Rechtsprechung übertragbar, wenn zwar mitarbeiterbezogene oder -beziehbare Daten verarbeitet werden, diese Daten aber keine Aussagen über das Verhalten oder die Leistung eines Mitarbeiters enthalten. Werden z.B. zur Korruptionsbekämpfung die letzten Ziffern der IBAN von Mitarbeiter-Lohnkonten einerseits und Bankkonten von Lieferanten oder Dienstleistern andererseits abgeglichen, ließe sich das Argument übertragen.

Allerdings ist in der arbeitsgerichtlichen Praxis und in Einigungsstellenverfahren zu beobachten, dass die Möglichkeit der Verhaltenskontrolle bejaht wird, soweit Nutzungs- oder Administratorenzugriffe von Mitarbeitern in Logdaten aufgezeichnet werden, die punktuell Informationen über Nutzerverhalten (wer hat wann lesend, schreibend oder ändernd auf Daten im System zugegriffen?) enthalten. Dann müsste sich aber jedenfalls die Betriebsvereinbarung nach § 87 Abs. 1 Ziff. 6 BetrVG auf diese konkrete Kontrollmöglichkeit beschränken. Solche eingeschränkten Vereinbarungen lassen sich in der Praxis gelegentlich durchsetzen, wenn nur technische Daten, z.B. zu den übertragenen Datenmengen durch E-Mail-Anhänge und dem Zeitpunkt der Übertragung ohne Nutzerkennung, aber keine mitarbeiterbezogenen Informationen verarbeitet werden. Dann sollte sich der Arbeitgeber jedoch mindestens das Recht zur Kontrolle der schreibenden und ändernden Zugriffe der Nutzer und Administratoren vorbehalten, um die Systemsicherheit zu gewährleisten und zugleich die Qualität der Datenverarbeitung zu sichern und z.B. eventuellen Rechenfehlern nachgehen zu können. Entsprechendes gilt für Test-Systeme und die Zugriffe der Tester, soweit noch keine Mitarbeiter-Daten, sondern nur „Dummys" verarbeitet werden. Auch hier muss der Arbeitgeber ggf. das Verhalten der Tester auswerten können, um Fehler nachverfolgen und das System weiterentwickeln zu können. Zugleich wäre die Speicherung von Logdaten in dem Umfang mitbestimmungsfrei, wie sie gesetzlich geboten ist.

C. Gesetzliche Vorgaben begrenzen die Mitbestimmung

Nur ausnahmsweise ist also eine technische Einrichtung, die Verhalten und Leistung von Arbeitnehmern erfasst, nicht dazu geeignet, diese auch zu „überwachen" im oben beschriebenen Sinne der Rechtsprechung zu § 87 Abs. 1 Ziff. 6 BetrVG. Der lesende Zugriff auf IT-Systeme dokumentiert, wann welcher Arbeitnehmer welche Informationen eingesehen hat. Dies gilt auch für IT-Administratoren von IT-Sicherheitssystemen. Soweit die regulatorischen Vorgaben des IT-Sicherheitsrechts und des Datenschutzrechts oder branchenspezifische Vorgaben im Bankaufsichtsrecht den Gestaltungsspielraum bei der Speicherung von Logdaten einengen, ist das Mitbestimmungsrecht des Betriebsrats ausgeschlossen, vgl. § 87 Abs. 1 Hs. 1 BetrVG. Dies gilt jedenfalls, soweit es keine für Arbeitnehmer weniger einschneidende, gleich wirksame Maßnahmen gibt und der Gestaltungsspielraum dadurch auf Null reduziert ist, weil es zu der Frage „ob" Administratorenzugriffe gespeichert werden, keine datenschutzrechtlich zulässige Alternative gibt. Dann bleibt nur zu prüfen, ob speziell bezogen auf das „Wie" der Verarbeitung gestaltende Entscheidungen noch verbleiben, auf die sich die Mitbestimmung beziehen könnte. Daher könnte zumindest das „Ob" der Speicherung von Zugriffsdaten der Administratoren von der Mitbestimmungspflicht ausgenommen sein, so dass die Mitbestimmung auf verbleibende gestaltbare Entscheidungen zum Einsatz und der Anwendung technischer Einrichtungen begrenzt wäre, in denen der Umfang der Speicherung und der Weiterverarbeitung von Zugriffsdaten gestaltet wird.

D. Entscheidungsspielraum für die Unternehmensleitung als Korridor für mitbestimmungspflichtige Entscheidungen

Einzelne Verarbeitungsvorgänge können vom Mitbestimmungsrecht ausgenommen sein (§ 87 Abs. 1 Hs. 1 BetrVG), wenn und soweit sie gesetzlich vorgegeben sind und dem Arbeitgeber kein eigener Gestaltungsspielraum zusteht.[13] Gesetz im Sinne dieser Bestimmung ist jedes zwingende förmliche oder materielle Gesetz und gesetzesvertretende Richterrecht, das den

13 *Richardi*, in: Richardi (Hrsg.), BetrVG, 16. Aufl. 2018, § 87 Rn. 148; *Kania*, in: Müller-Gloge et. al. (Hrsg.), ErfK zum Arbeitsrecht, 20. Aufl. 2020, § 87 Rn. 10.

Arbeitgeber bindet.[14] Ausreichend ist auch ein bindender Verwaltungsakt, der den Arbeitgeber zu bestimmten Maßnahmen verpflichtet.[15]

Verbleibt dem Arbeitgeber trotz gesetzlicher Regelung ein Gestaltungsspielraum, den er durch sein Direktionsrecht ausfüllen kann, darf der Betriebsrat im gleichen Umfang mitbestimmen:[16]

> *„Nach § 87 Abs. 1 Eingangshalbs. BetrVG hat der Betriebsrat u. a. nicht nach § 87 Abs. 1 BetrVG mitzubestimmen, soweit die betreffende Angelegenheit gesetzlich geregelt ist. Das beruht auf der Erwägung, dass für die Erreichung des Mitbestimmungszwecks kein Raum mehr verbleibt, wenn eine den Arbeitgeber bindende und abschließende gesetzliche Vorschrift vorliegt. Wird der Mitbestimmungsgegenstand durch diese inhaltlich und abschließend geregelt, fehlt es an einer Ausgestaltungsmöglichkeit durch die Betriebsparteien. Verbleibt dem Arbeitgeber dagegen trotz der bestehenden normativen Regelung ein Gestaltungsspielraum, ist ein darauf bezogenes Mitbestimmungsrecht des Betriebsrats eröffnet […].“*[17]

E. Einschätzungsprärogative des Arbeitgebers zu regulatorischen Vorgaben und technischen Details?

Während das Unternehmen als Arbeitgeber nebeneinander die Sicherheit informationstechnischer Systeme und den Arbeitnehmerdatenschutz gewährleisten muss, konzentriert sich das Engagement der Betriebsräte als Interessenvertreter in Verhandlungen über technische Einrichtungen auf den Arbeitnehmerdatenschutz und die Begrenzung der Mitarbeiterkontrolle. Dieses Ungleichgewicht prägt den Verlauf der Verhandlungen. Dadurch werden die Verhandlungen der Personalabteilung mit dem Betriebsrat zum Nadelöhr für die Umsetzung von IT-Sicherheitskonzepten. Für den erfolgreichen Abschluss der Verhandlungen kann daher ausschlaggebend sein, dass der Arbeitgeber den Betriebsrat schon in der Informationsphase gründlich darüber aufklärt, welche gesetzlichen und behördlichen Vorgaben zur IT-Sicherheit seinen eigenen Gestaltungsspielraum einschränken. Entsteht Streit über die Reichweite solcher Vorgaben, muss

14 *Richardi* (Fn. 13), § 87 Rn. 145 f., 148.
15 *Richardi* (Fn. 13), § 87 Rn. 149 m.w.N.
16 *Kania* (Fn. 13), § 87 Rn. 13; BAG NZA 2014, 1152 Rn. 14 zu Nr. 4 (Arbeitsentgelt); BAG NZA 2013, 913, 914 Rn. 19 zu Nr. 6 (Verhaltens- und Leistungskontrolle); BAG NZA 2002, 995 zu Nr. 7 (Arbeitsschutz).
17 BAG NZA 2014, 1151, 1152 Rn. 14.

den Fachabteilungen zu regulatorischen Vorgaben und zu der technischen Umsetzung und eventuellen Alternativlösungen, die dem Stand der Technik entsprächen, im Zweifel eine Einschätzungsprärogative zugestanden werden. Die Verantwortung des Unternehmens, sich so zu organisieren, dass Gesetze beachtet werden, liegt in der Aktiengesellschaft beim Vorstand, § 93 AktG.[18] Die Fachabteilungen tragen in der Organisation des Unternehmens die fachliche Verantwortung für die Einhaltung der gesetzlichen Vorgaben zur Datensicherheit und zur Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und bewahren das Unternehmen vor behördlichen Sanktionen oder Schadensersatzansprüchen Dritter.

F. Verfahrensablauf in der Mitbestimmung

I. Innerbetriebliche Verhandlungen

Einigen sich Arbeitgeber und Betriebsrat auf den Einsatz eines Systems und den Umfang der Nutzung, ist für das Unternehmen damit nicht zuverlässig gesichert, dass es damit zugleich auch den regulatorischen Anforderungen an die Datensicherheit genügt. Der Betriebsrat gestaltet die Regeln zur Anwendung des Systems mit, er trägt aber nicht die Verantwortung im Interessenausgleich zwischen Arbeitnehmerdatenschutz einerseits und Datensicherheit, Integrität, Verfügbarkeit und Vertraulichkeit der Systeme andererseits. Wählt das Unternehmen hier den vorsichtigen Weg möglichst umfangreicher IT-Sicherheitssysteme, lässt sich eine Einigung mit dem Betriebsrat schwer erzielen. Dann kann im Einigungsstellenverfahren unter Umständen nur durch Spruch eine Regelung gefunden werden. Die Einigungsstelle hat dabei den Stand der Technik zu berücksichtigen, der durch Industriestandards (ISO 27000, 27001, 27002) und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (IT-Grundschutz) konkretisiert wird, vgl. § 8 BSiG, Art. 32 DSGVO.

II. Spruch der Einigungsstelle und dessen gerichtliche Überprüfung

Die Verhandlungen über die Mitbestimmung bei der Anwendung technischer Einrichtungen dauert nicht selten mehrere Monate: Zunächst tauschen sich die Betriebsparteien schriftlich über die Besetzung der Eini-

18 LG München I NZG 2014, 345.

gungsstelle aus. Im nächsten Schritt müssen gemeinsame Termine gefunden werden. Ein erster Termin dient meist dazu, dem Einigungsstellenvorsitzenden einen Überblick über den Gegenstand der Einigungsstelle zu verschaffen. Im zweiten Termin sind meist offene Fragen der Arbeitnehmervertreter zu den Funktionen der technischen Einrichtungen zu beantworten. In diesem und je nach Komplexität mindestens ein bis drei Anschlussterminen werden dann Regelungen zur Begrenzung der Leistungs- und Verhaltenskontrolle erörtert. Im Rahmen dieser Diskussion beantwortet der Arbeitgeber typischerweise auch Fragen des Betriebsrates dazu, ob der Einsatz des Systems den Arbeitnehmerdatenschutz wahrt. Dazu stehen dem Betriebsrat Informations- und Kontrollrechte gemäß § 80 BetrVG zu. Damit zwischen den Terminen Fragen beantwortet werden können und in Abhängigkeit von der Verfügbarkeit des Vorsitzenden und der Beisitzer liegen die Termine meist in einem Abstand von zwei bis sechs Wochen. Das passt nicht zu den zeitlichen Abläufen in typischen IT-Sicherheitsprojekten. Entscheidet die Einigungsstelle durch Spruch, ist der Spruch anfechtbar und kann in mindestens zwei Instanzen der Arbeitsgerichtsbarkeit auf Ermessens- und Rechtsfehler überprüft werden, § 2a Abs. 2, § 80 ArbGG, § 76 Abs. 5 BetrVG. Dieses Verfahren dauert über zwei Instanzen erfahrungsgemäß häufig 15 bis 18 Monate. Für die praktische Umsetzung der Sicherheitskonzepte bedeutsam ist, dass der Spruch betriebsverfassungsrechtlich bis zur rechtskräftigen Entscheidung über die Wirksamkeit des Einigungsstellenspruchs angewandt werden kann und der Betriebsrat, der einen Spruch zur Einführung und Anwendung eines technischen Systems anficht, nur ausnahmsweise im Wege des einstweiligen Rechtsschutzes die Anwendung stoppen kann.[19]

Mit der förmlichen Entscheidung der Einigungsstelle und der Zustellung des vom Vorsitzenden unterschriebenen Textes ist der Spruch der Einigungsstelle zunächst verbindlich, § 87 Abs. 2 S. 2 BetrVG. Es muss nicht im Nachgang noch eine von beiden Seiten unterschriebene Betriebsvereinbarung geschaffen werden. Der Spruch gilt als Betriebsvereinbarung, die unmittelbar gilt und umzusetzen ist, § 87 Abs. 2 S. 2 BetrVG. Das gilt zunächst einmal unabhängig davon, ob sie gerichtlich angegriffen wird. Diese betriebsverfassungsrechtliche und prozessuale Zwischenlösung schützt das Unternehmen allerdings nicht zuverlässig vor abweichenden eigenständigen Bewertungen der Datenschutzaufsichtsbehörde. Hält die Einigungsstelle ein System und die Art seiner Anwendung für datenschutzkonform und kann auf der Grundlage eines Spruchs der Einigungsstelle das

19 LAG Baden-Württemberg BeckRS 2016, 73644.

System zunächst betriebsverfassungsrechtskonform eingesetzt werden, ist damit jedenfalls theoretisch noch nicht beantwortet, ob die Datenschutzaufsicht später Datensicherheitsdefizite feststellen wird oder aber die arbeitnehmerdatenschutzrechtlichen Grenzen des Einsatzes anders bewertet. Dies wäre nur dann zuverlässig ausgeschlossen, wenn die Betriebsvereinbarung selbst zugleich als datenschutzrechtliche Rechtsgrundlage der Verarbeitung gestaltet wäre. In der Regel wird die Einigungsstelle aber nur prüfen, ob einer der datenschutzrechtlichen Erlaubnistatbestände (§ 26 BDSG oder Art. 6 DSGVO) die Verarbeitung der Arbeitnehmerdaten rechtfertigt, und dann durch Spruch über die Grenzen der Mitarbeiterkontrolle i. S. d. § 87 Abs. 1 Ziff. 6 BetrVG entscheiden.

Hat der Arbeitgeber durch Spruch der Einigungsstelle den Weg für den Einsatz eines IT-Sicherheitssystems gebahnt, bleibt dem Betriebsrat der Weg, den Einigungsstellenspruch im arbeitsgerichtlichen Beschlussverfahren anzufechten. Wenn er nicht nur Rechtsfehler, sondern auch Ermessensfehler geltend macht, muss die Anfechtung innerhalb von zwei Wochen nach Zuleitung des Beschlusses beim Arbeitsgericht eingereicht und begründet werden, § 76 Abs. 5 S. 4 BetrVG. Auch nach Ablauf der Zwei-Wochen-Frist bleibt der Rechtsweg offen für eine Anfechtung mit der Begründung, dass der Spruch gegen Rechtsvorschriften verstoße. Insbesondere die Behauptung des Betriebsrats, dass das Arbeitnehmer-Datenschutzrecht mit einem Spruch, der die Einführung eines technischen Systems unter bestimmten Bedingungen gestattet, nicht hinreichend beachtet würde, kann Gegenstand der Rechtskontrolle sein. Auch der Vorwurf, dass rechtliches Gehör nicht gewährt worden wäre, könnte nach Ablauf der Zwei-Wochen-Frist noch geltend gemacht werden, § 2a Abs. 2 ArbGG, § 80 ArbGG.

Die Arbeitsgerichtsbarkeit muss dann die Interessenabwägung zwischen Datensicherheit und Arbeitnehmerdatenschutz überprüfen und dabei ggf. auch fachgesetzliche Vorgaben anwenden. Sowohl die technischen Sachverhalte als auch die nicht-arbeitsrechtlichen Rechtsquellen sind dabei für Arbeitsrichter unter Umständen Neuland. Zu der Frage, ob ein System dem Stand der Technik entspricht und wie die IT-Sicherheitsrisiken branchen- und unternehmensspezifisch zu bewerten sind, können ggf. ergänzend zu den veröffentlichten ISO-Standards und Katalogen des BSI technische Gutachten einzuholen sein. Gutachten zur Auslegung deutscher Gesetze, insbesondere des § 25 KWG oder § 8a BSiG, lassen sich mit der Prozessordnung aber nur ausnahmsweise vereinbaren. Die Frage der Zulässigkeit der Einholung eines Rechtsgutachtens zu inländischen Rechtsfragen durch ein deutsches (Zivil-)Gericht wird nicht einheitlich beurteilt. Der BGH hielt in einer Entscheidung zum Steuerrecht die Einholung eines Rechtsgutachtens eines Steuerfachmanns für möglich, sofern das Gericht

dessen Meinung in vollem Umfang überprüft.[20] Bei außerordentlich speziellen oder entlegenen Rechtssätzen wird eine analoge Anwendung des § 293 ZPO in erwogen.[21] Die überwiegende Meinung im Schrifttum lehnt dagegen eine analoge Anwendung der Vorschrift bei außerordentlich „speziellen" oder „entlegenen" Rechtssätzen ab.[22] Bezogen auf den Strafprozess hat das OLG Celle festgestellt, dass Bestand und Auslegung des inländischen Rechts sowie seine Anwendung auf den Entscheidungsfall einer Beweiserhebung nicht zugänglich seien.[23]

III. Einstweiliger Rechtsschutz

Der Betriebsrat könnte während der gerichtlichen Auseinandersetzung über die Wirksamkeit des Einigungsstellenspruchs die Einführung eines IT-Sicherheitssystems nur aufhalten, wenn er beim Arbeitsgericht eine einstweilige Verfügung erwirken könnte, die sich gegen die Anwendung eines Einigungsstellenspruches während der gerichtlichen Auseinandersetzung über die Wirksamkeit des Einigungsstellenspruchs richtet. Eine solche einstweilige Verfügung könnte bei „besonders krassen und offensichtlichen Rechtsverstößen" erlassen werden.[24]

1. Verfügungsanspruch

Einigungsstellensprüche sind grundsätzlich unmittelbar umzusetzen. Anfechtungsverfahren, unabhängig davon, welche Seite den Angriff gegen den Spruch der Einigungsstelle betreibt, haben keinen Suspensiveffekt.[25] Dies gilt nicht nur in Fällen, in denen der Betriebsrat oder Gesamtbetriebsrat das Interesse an der Durchführung einer durch Spruch der Einigungs-

20 BGH NJW 1999, 638.

21 *Thole,* in: Stein/Jonas, Kommentar zur ZPO, 23. Aufl. 2013, § 293 Rn. 17.

22 Vgl. *Sanger*, in: Saenger (Hrsg.), Zivilprozessordnung, 8. Aufl. 2019, § 293 Rn. 6; *Prütting*, in: MüKoZPO, 6. Aufl. 2020, § 293 Rn. 22; so auch der hessische Staatsgerichtshof LKRZ 2012, 14 oder im Steuerrecht vgl. *Tipke* NJA 1976, 2200; *Nickl*, NJW 1989, 2093.

23 OLG Celle BeckRS 2015, 11588 Rn. 9 m.w.N.

24 So zusammenfassend zur Instanzrechtsprechung Fitting, BetrVG, 30. Aufl. 2020, § 76 Rn. 165, insbesondere LAG Köln NZA 2000, 334.

25 *Korinth*, Einstweiliger Rechtsschutz im Arbeitsgerichtsverfahren, 3. Aufl. 2015, Abschnitt K, Rz. 175 mit Verweis auf LAG Berlin v. 6.12.1984 – 4 TaBV 2/84; LAG Hessen v. 16.12.2004 – 4 Ta 165/04; LAG Köln v. 20.4.1999 – 13 Ta 243/98.

stelle zustande gekommenen Regelung hat, sondern auch dann, wenn die Durchführung des Einigungsstellenspruchs im Interesse des Arbeitgebers liegt oder vom Arbeitgeber sogar für zwingend erforderlich gehalten wird.[26] Einstweilige Verfügungen, die die Durchführung eines Einigungsstellenspruchs verhindern sollen, sind nur ausnahmsweise zulässig, wenn der Spruch der Einigungsstelle krasse Rechtsverstöße enthält und dies zudem offensichtlich ist.[27] Für diese restriktive Handhabung gibt es auch eine vollstreckungsrechtliche Begründung: Mit dem Streit über eine einstweilige Verfügung werden für die Dauer des Anfechtungsverfahrens durch die Instanzen die Risiken zwischen den Betriebsparteien verteilt. Diese Risikoverteilung findet im Urteilsverfahren einen Ausgleich durch den Schadensersatzanspruch des § 945 ZPO.[28] Eine Zwischenregelung durch einstweilige Verfügung, die sich nach einer Entscheidung in der Hauptsache als von Anfang an ungerechtfertigt erweist, verpflichtet im Urteilsverfahren den Gegner zum Schadensersatz (§ 945 ZPO). Dieser Schadensersatz steht dem Arbeitgeber im Beschlussverfahren nicht zur Verfügung, da die Vorschriften über das Beschlussverfahren nicht auch auf die Bestimmung verweisen, die einen Ausgleich für die gerichtliche Risikoverteilung schafft.[29] Erweist sich im Beschlussverfahren in der zweiten oder dritten Instanz eine vorläufige Regelung als von Anfang an ungerechtfertigt, hat allein der Arbeitgeber die Risiken daraus zu tragen.[30] Er hat keinen Schadensersatzanspruch gegen den Betriebsrat nach § 945 ZPO und auch keine anderen Regressansprüche gegen handelnde Personen.[31]

Bezogen auf den Einsatz notwendiger IT-Sicherheitssysteme wären die Folgen einer Unterlassungsverfügung bis zum rechtskräftigen Abschluss des Streits um die Wirksamkeit des Einigungsstellenspruchs nicht hinnehmbar. Der Arbeitgeber wäre nicht nur unternehmerischen Risiken ausgesetzt, sondern auch dem aufsichtsbehördlichen Vorwurf, seine Aufgaben in der Gefahrenabwehr nicht beachtet zu haben und damit dem Risiko, dass Sanktionen gegen ihn verhängt werden:

Je länger sich die Einführung eines IT-Sicherheitssystems verzögert, desto größer wäre die Wahrscheinlichkeit, dass bestehende Sicherheitslücken tatsächlich für einen Cyberangriff genutzt würden. Dies würde für das Unternehmen ein unternehmerisches Risiko darstellen. Vertrauliche Informa-

26 LAG Köln NZA 2000, 334.
27 LAG Köln NZA 2000, 334.
28 BGH NJW 1996, 198; *Drescher*, in: MüKoZPO, 6. Aufl. 2020, § 945 Rn. 2.
29 LAG Baden-Württemberg NZA 1990, 286; *Olderog* NZA 1985, 753, 756.
30 LAG Baden-Württemberg NZA 1990, 286.
31 LAG Baden-Württemberg NZA 1990, 286.

tionen könnten an Wettbewerber gelangen, Kundendaten könnten gestohlen werden oder Arbeitsabläufe gefährdet werden. Zudem wäre damit die Reputation des Unternehmens beschädigt, wenn Sicherheitslücken öffentlich bekannt werden.[32] Darüber hinaus hätte das Unternehmen oder dessen Organe[33] auch (behördliche) Sanktionen zu befürchten: In einer Aktiengesellschaft haben die Vorstandsmitglieder gemäß § 93 Abs. 1 AktG bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Zu den Pflichten des Gesamtvorstands gehört die Einrichtung eines funktionierenden Compliance-Systems.[34] Ein gesetzeskonformes System der IT-Sicherheit ist ein notwendiger Bestandteil davon. Ungenügende organisatorische Vorkehrungen stellen eine Pflichtverletzung dar und können zur Schadensersatzpflicht gegenüber der Gesellschaft führen.[35] Eine Schadensersatzpflicht kann den Vorstand darüber hinaus auch dann treffen, wenn er es gemäß § 91 Abs. 2 AktG unterlässt, geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Früherkennung eines Cyber-Angriffs lässt sich unter diesen Begriff fassen.[36]

Jedenfalls seit der Anwendbarkeit der DSGVO können auch Datenschutzverstöße zu bestandsgefährdenden Bußgeldern führen. Bußgelder sind in der DSGVO in Art. 83 vorgesehen. Nach dessen Absatz 4 können Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden. Auch der Verstoß gegen Art. 32 DSGVO ist gem. Art. 83 Abs. 4 lit. a bußgeldbewehrt. Die Norm gibt technische und organisatorische Maßnahmen vor, die im Unternehmen ergriffen werden müssen, um ein angemessenes Schutzniveau in Bezug auf die Datensicherheit zu erzielen. Genügt ein bisher verwendetes IT-System diesen Anforderungen nicht und verzögert sich die Einführung des neuen datenschutzkonformen IT-Sicherheitssystems, kann es zur Verhängung eines Bußgeldes kommen.

---

32 Vgl. die Berichtserstattung zum Cyber-Angriff auf die Funke-Mediengruppe im Dezember 2020 (etwa *Finanznachrichten.de* vom 4.1.2021, „Cyberangriff auf Funke-Mediengruppe hält weiter an“) oder die Berichterstattung zum Cyber-Angriff auf die British Airways 2018 (etwa *Der Tagesspiegel* vom 7.9.2018, „Hacker erbeuten 380.000 Kundendaten bei British Airways“) zu nennen.

33 Dazu unter Ziffer V.

34 *Bicker*, AG 2012, 542; *Fleischer*, in: BeckOGK, 15.1.2020, AktG, § 91 Rn. 47 ff.

35 LG München I NZG 2014, 345.

36 *Behling*, ZIP 2017, 697, 698.

Betreiber Kritischer Infrastrukturen (vgl. zur Legaldefinition § 1 Abs. 10 BSIG), wie etwa Banken, trifft darüber hinaus auch die Verpflichtung aus § 8a BSIG, 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. Kommen sie dieser Verpflichtung nicht nach, etwa durch Implementierung eines den Anforderungen genügenden IT-Sicherheitssystems, rechtfertigt auch dies die Verhängung eines Bußgeldes gem. § 14 BSIG.

2. Anforderungen an den Verfügungsgrund

Da die Durchführung des Einigungsstellenspruchs während eines Anfechtungsverfahrens der Regelfall ist und nur höchst ausnahmsweise ein Verfügungsanspruch überhaupt in Betracht kommt, sind besonders hohe Anforderungen an den Verfügungsgrund zu stellen. Eine nicht rechtskräftige Entscheidung des Arbeitsgerichts ist kein Verfügungsgrund; sie kann mit ihrer Begründung aber in die Bewertung des Verfügungsanspruchs einbezogen werden. Der Antragsteller muss für den Verfügungsgrund vielmehr darlegen, dass ihm bei – auch bloß zeitweiliger – Durchführung des Einigungsstellenspruchs Nachteile drohen, gegenüber denen die Interessen des Antragsgegners zweifelsfrei zurückzutreten haben.[37] Der Einsatz eines Systems der IT-Sicherheit müsste also in der Verarbeitung von Mitarbeiterdaten offensichtlich eine nicht mehr reversible Verletzung deren Persönlichkeitsrechts begründen. Diese Voraussetzungen liegen im Zweifel nicht vor. Wäre der Eingriff durch Verarbeitung von Verhaltensdaten über die Nutzeraktivitäten zu intensiv, könnten die Daten gelöscht werden. Der Eingriff wäre nicht irreversibel.

3. Keine Ausnahme von den Anforderungen an Verfügungsanspruch und -grund

Für den besonderen Fall von Überstunden von Verkäuferinnen in einem Kaufhaus hatte das LAG Hamburg im Jahr 2000[38] ausnahmsweise eine einstweilige Verfügung erlassen, die dem Arbeitgeber die Durchführung

37 LAG Baden-Württemberg NZA 1990, 286.
38 3 TaBV 6/00 mit Anm. *Bertelsmann*, AIB 2001, 51.

eines Einigungsstellenspruchs untersagen sollte, der die Überstunden gestattete. Dies wurde ausdrücklich auf die einzelfallbezogene Begründung gestützt, dass ohne den einstweiligen Rechtsschutz die Hauptsache in der Sache vollständig erledigt wäre. Diese Überlegung ist hier nicht übertragbar, da eine vorläufige Durchführung des Einigungsstellenspruchs zum Einsatz und zur Anwendung eines IT-Sicherheitssystems die Hauptsache nicht erledigt. Das System wird in der Regel über Monate und Jahre eingesetzt. Die Entscheidung in der Hauptsache könnte die Rahmenbedingungen für den Einsatz bestimmen für den Zeitraum nach Abschluss des Verfahrens im einstweiligen Rechtsschutz.

G. Fazit

Mitbestimmungsrechte des Betriebsrates bei der Einführung von IT-Sicherheitssystemen sollten im Projektplan für die Einführung technischer Systeme von Anfang an eingeplant werden. Andernfalls kann es zu erheblichen Verzögerungen kommen, bis durch Abschluss einer Betriebsvereinbarung oder Spruch der Einigungsstelle der Einsatz des Systems betriebsverfassungsrechtlich legitimiert ist. Gelingt eine Einigung nicht und muss das Einigungsstellenverfahren durch Spruch beendet werden, können sich aus Folgestreitigkeiten über die Wirksamkeit des Einigungsstellenspruchs im Beschlussverfahren durch zwei oder drei Instanzen über längere Zeiträume Rechtsunsicherheiten ergeben.

IT-Sicherheit: ein verfassungsrechtlicher Zugang

Isabella Risini

A. Die verfassungsrechtliche Relevanz von IT-Sicherheit

Der Beitrag beleuchtet Fragen der IT-Sicherheit aus einer verfassungsrechtlichen Perspektive. Besonderes Augenmerk liegt auf der möglichen Verantwortung des Staates im Bereich der IT-Sicherheit. Begrifflich verknüpft er die traditionell staatliche Aufgabe der Gewährleistung von Sicherheit, einschließlich der IT-Sicherheit, mit der faktischen und rechtlichen Verantwortung von Unternehmen für IT-Sicherheit. Dieser Ansatz soll den Blick darauf ermöglichen, dass die Rückbindung von IT-Sicherheit in das Verfassungsrecht bisher unzureichend dogmatisch durchdrungen ist.

Das Sicherheitsrecht ist traditionell eines der am stärksten verfassungsrechtlich determinierten Rechtsgebiete.[1] Das Verständnis von Sicherheit und Sicherheitsrecht gibt Auskunft zum Verhältnis zwischen Staat und seinen Bürgern; die Risikotoleranz indiziert die Freiheitsgrade, die sich eine Gesellschaft bewusst bewahren möchte.

Mit Blick auf die zunehmende Abhängigkeit von Datenverarbeitung quer durch alle Lebensbereiche, oft verschlagwortet mit dem Begriff der „Digitalisierung", ist eine sichere IT-Umgebung eine wichtige Vorbedingung für die Ausübung der meisten Grundrechte geworden. Die Sicherheit von Datensystemen ist auch die Grundbedingung für einen Großteil der wirtschaftlichen Wertschöpfung. Die Zukunft in einer Welt mit autonomen Fahrzeugen zu Lande[2] und in der Luft sowie allerlei künstlich intelligenten Maschinen und Robotern[3], die unseren Alltag begleiten und erleichtern sollen, ist ohne IT-Sicherheit undenkbar.[4] Bislang bleibt das

1 *Gärditz*, Sicherheitsrecht als Perspektive, GSZ 2017, S. 1.

2 *Roßnagel/ Hornung*, (Hrsg.) Grundrechtsschutz im Smart Car, Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, 2019.

3 *Eberstaller/Forgó*, KI-spezifische Rechtsfragen der Cybersicherheit, in: Ebers/Heinze/Krügel/Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik, Rechtshandbuch, 2020, S. 441; Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021 (im Erscheinen).

4 *Müller-Quade* u.a., AG IT-Sicherheit, Privacy und Ethik, Whitepaper Künstliche Intelligenz und IT-Sicherheit, Bestandsaufnahme und Lösungsansätze, 4.4.2019,

Verfassungsrecht noch schuldig, wie der überragende, aus rechtswissenschaftlicher Sicht verhältnismäßig neue Zielwert der IT-Sicherheit optimal zu verwirklichen ist.

Dieser Beitrag gibt zunächst eine begriffliche Orientierung zum Topos „IT-Sicherheit" (B.). Im darauffolgenden Abschnitt (C.) erfolgt eine Rekonstruktion dessen, was das Grundgesetz in Bezug auf IT-Sicherheit ausdrücklich und qua richterlicher Rechtsfortbildung regelt. Insbesondere wird die Aufteilung von Verantwortungen für Universaldienste zwischen Staat und Unternehmen im Rahmen des Privatisierungsfolgenrechts beleuchtet. Sodann werden der grundrechtliche Schutz von IT-Sicherheit und seine Grenzen in den Blick genommen.

In Abschnitt D. wird der Blick auf den inter- und intradisziplinären Mehrwert gelegt, der in besonderem Maße für Fragen der IT-Sicherheit vorhanden ist. Insbesondere wird anhand von Beispielen aus verschiedenen Fachsäulen der Rechtswissenschaft herausgearbeitet, wo ein klarerer verfassungsrechtlicher Maßstab zum Oberthema IT-Sicherheit wünschenswert wäre. Im Fazit wird hervorgehoben, dass es über den Selbstzweck der Dogmatik hinaus einen Gewinn an Rechtssicherheit bedeuten würde, wenn das deutsche Verfassungsrecht einen Kompass für Fragen der IT-Sicherheit bereithielte.

B. Der Begriff der IT-Sicherheit – ein Zugang über Schutzziele

IT-Sicherheit, auch Cybersicherheit, Cybersecurity oder Information Security, ist ein technischer Idealzustand, in dem ein IT-System vor Angreifern von innen und von außen geschützt ist. Cyber-Sicherheit ist indes kein statisches Ziel. Eine besondere Eigenschaft aller Fragen der IT-Sicherheit ist die Notwendigkeit, der ständigen Anpassung und Weiterentwicklung der Schutzmechanismen und Abwehrstrategien. Diese zeitliche Dimension der IT-Sicherheit, mit schnell fortschreitenden technischen Anforderungen, macht die rechtliche Einhegung über schwerfällige Gesetzgebungsmechanismen jedenfalls herausfordernd.

Wegen der Vielgestaltigkeit von Fragen der Sicherheit von Daten ist eine übergreifende rechtliche Definition von IT-Sicherheit Desiderat.[5] Er-

---

https://www.plattform-lernende-systeme.de/publikationen-details/id-1-broschuere.html (abgerufen am 10.1.2020).

5 *Kipker*, Grundlagen und Strukturen, in: Kipker (Hrsg.), Cybersecurity, 2020, Rn. 4 ff.; *Hornung/Schallbruch*, Einführung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 25.

schwerend für den Prozess einer einheitlichen Begriffsbildung kommt hinzu, dass die Begrifflichkeiten rund um die IT-Sicherheit inter- und intradisziplinär mit vielen verschiedenen Konnotationen belegt sind.

I. Fragmentiertheit rechtlicher Anforderungen an die IT-Sicherheit

Bisher zeichnen sich die rechtlichen Anforderungen an IT-Sicherheit als Querschnittsmaterie vor allem durch ihre Fragmentiertheit aus. Eine Bestandsaufnahme des Rechts der der IT-Sicherheit darf nicht nur entlang der vorgefundenen Rechtsgebietsgrenzen und Fachsäulen verlaufen. Ohne Anspruch auf eine vollständige Auflistung von Rechtssätzen und Materien, die sich mit IT-Sicherheit befassen, reicht diese vom Recht der Produkthaftung[6] über das klassische zivile Haftungsrecht[7] bis hin zum Urheber- und Lauterkeitsrecht.[8] Am Beispiel des Rechtes des Datenschutzes kann außerdem abgelesen werden, wie sehr das Zusammenspiel von verschiedenen Ebenen entscheidend war und wohl auch in Zukunft sein wird.[9]

Beispielhaft für das öffentliche Recht sei hier aufgeführt, dass die Betreiber von sogenannten kritischen Infrastrukturen (Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen) sektoral besondere Anforderungen erfüllen müssen.[10] Diese Diskriminierung zwischen Unternehmen, die in gewissen Sektoren agieren und „normalen" Unternehmen wird bislang allgemein hingenommen.

Die Fragmentiertheit des Rechts der IT-Sicherheit lässt sich nicht zuletzt auf die Gesetzgebungs- und Verwaltungszuständigkeiten im föderalen Ver-

---

6 *Spindler*, Verantwortung der IT-Hersteller (produktbezogene Pflichten), in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 248.

7 *Voigt*, IT-Sicherheitsrecht, Pflichten und Haftung im Unternehmen, Otto Schmidt Verlag, 2018.

8 *Barudi*, Urheber- und Lauterkeitsrecht, Know-How-Schutz, in Kipker (Hrsg.), Cybersecurity, 2020, S. 273.

9 *T. Streinz*, The Evolution of European Data Law, in: Caig/de Búrca, The Evolution of EU Law, 2021 im Erscheinen; *Voskamp*, Datenschutz, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 151; siehe auch *Conrad/Eckhardt/Fleischhauer/Huppertz/Streitz*, Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Auer-Reinsdorff / Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2019, S. 1637.

10 § 2 Abs. 9 und 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).

fassungsstaat zurückführen.[11] Art. 91 c Abs. 2 GG, der in einem gewissen Teilbereich eine Kooperation von Bund und Ländern ermöglicht, lässt erahnen, wie schwierig ein übergreifender Ansatz für das Recht der IT-Sicherheit umzusetzen wäre.[12] Ein solcher übergreifender Ansatz geht weit über die Ambition des vorliegenden Beitrages hinaus.

Die Auffächerung des Rechts der IT-Sicherheit geht einher mit einer höher werdenden Regelungsdichte, bisweilen ist auch die Rede von einem „Normenzoo".[13] Außerdem fließen in die Standardisierung bzw. Normgebung vielfältige Interessen ein. Flankiert wird diese Entwicklung von steigender Komplexität von informationstechnischen Systemen im Zeitalter des Internets der Dinge (Internet of Things) und entsprechend höheren Anforderungen an die Absicherung vor Angriffen.

II. Ein Zugang über Schutzziele

IT-Sicherheit verfolgt verschiedene Schutzziele.[14] Diese verschiedenen Ziele müssen jeweils bedarfsorientiert durch Priorisierung miteinander in Einklang gebracht werden. Die Schutzziele werden durch verschiedene technische Methoden verfolgt. Die Ziele überschneiden sich vielfach; eine abschließende Aufzählung ist schwer möglich. In der Verfolgung dieser Ziele kommt zum Ausdruck, dass es sich um einen sehr dynamischen Prozess handelt, der stets einen Idealzustand anstrebt. Regelungstechnisch wird diese Dynamik mit unbestimmten Rechtsbegriffen abgefedert, insbesondere dem „Stand der Technik".[15]

1. Vertraulichkeit

Zu den Zielen der IT-Sicherheit gehört die Vertraulichkeit, die trotz der Benutzung von IT-Systemen gewahrt werden soll. Vertraulichkeit wird

11 Z.B. Art. 74 Nr. 11 GG „Recht der Wirtschaft".
12 *Spiegel*, IT im Grundgesetz, NvWZ 2009, S. 1128.
13 Siehe dazu etwa den „Cybersecurity-Navigator", https://cybersecurity-navigator.de.
14 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23, 26ff.
15 Siehe *Ekrot/Fischer/Müller*, Stand der Technik, in: Kipker, (Hrsg.), Cybersecurity, 2020, S. 83, 85ff, und zur Differenzierung zwischen Begriffen wie „Allgemein anerkannte Regeln der Technik", „Stand der Technik" und „Stand von Wissenschaft und Forschung".

hier verstanden als das Bedürfnis, Daten geheim zu halten und einen Zugriff nur an einen bestimmten Personenkreis zu ermöglichen.[16] Ein Beispiel sind Firmengeheimnisse oder Forschungsergebnisse wie etwa die Formel für ein Vakzin gegen das Corona-Virus.[17] Das Recht des Datenschutzes hebt den Schutz von personenbezogenen Daten heraus.[18]

2. *Verfügbarkeit*

Die Verfügbarkeit (availability) eines IT-Systems ist ebenfalls ein Schutzziel. IT-Systeme müssen jederzeit einen Zugriff erlauben, um die Nutzung eines Dienstes zu ermöglichen.[19] So wurde etwa die Ruhr-Universität Bochum im Mai 2020 Ziel einer Attacke, die es für Studierende und Mitarbeitende für Wochen unmöglich machte, auf E-Mails, Online-Lernplattformen und auch Notendatenbaken zuzugreifen.[20] Der Hackerangriff auf ein Universitätsklinikum in Düsseldorf im September 2020 stand zunächst in Verdacht, Ursache für den Tod einer Patientin gewesen zu sein. Medienberichten zufolge konnte die Staatsanwaltschaft diesen Verdacht zwar nicht erhärten.[21] Ein Angriff auf ein Krankenhaus, der tatsächlich Menschenleben gefährdet ist durchaus denkbar. Ein Angriff auf die Funke Mediengruppe im Dezember 2020 erschwerte das Erscheinen vieler Blätter

16 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23, 26.

17 Siehe dazu die Informationen der European Medicines Agency, die im Dezember angeriffen wurde: Cyberattack on EMA – update 5, https://www.ema.europa.eu/en/news/cyberattack-ema-update-5, mit weiteren Nachweisen auf die Historie des Angriffs. (abgerufen am 10.1.2020), die Debatte, ob die Formeln für die Vakzine der Öffentlichkeit gleichsam als öffentliches Gut zur Verfügung stehen sollten wird hier außen vorgelassen.

18 *Jandt*, IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 391.

19 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23.

20 Ruhr-Uni fährt IT nach Cyberangriff wieder hoch, https://www.forschung-und-lehre.de/politik/ruhr-uni-faehrt-it-nach-cyberangriff-wieder-hoch-2797/. (abgerufen am 10.1.2020).

21 Hackerangriff auf Düsseldorfer Uniklinik: Ermittlungen wegen fahrlässiger Tötung eingestellt, https://www1.wdr.de/nachrichten/rheinland/duesseldorf-uniklinik-hackerangriff-ermittlungen-fahrlaessige-toetung-100.html. (abgerufen am 10.1.2020).

in Deutschland.[22] Die wirtschaftlichen Folgen des Angriffs dürften erheblich sein.[23]

3. *Integrität und Authentizität*

Schließlich sind die Integrität und die Authentizität von Daten zu nennen. Der Autor oder Urheber einer Nachricht oder eines Datensatzes müssen eindeutig sein. Für den Bereich der *Smart Contracts* wird hier auch oft von der Nicht-Abstreitbarkeit eines Datensatzes (etwa einer Willenserklärung) gesprochen.

4. *IT-Sicherheit und der Gedanke der Vorsorge*

Der IT-Sicherheit wohnt die Idee und die Notwendigkeit der Vorsorge inne.[24] Der Gedanke der Vorsorge scheint dahingehend immer dringender geboten, dass das heraufziehende Zeitalter der Quantencomputer viele auf klassischer Kryptografie basierenden IT-Sicherheitsmaßnahmen schon heute in Frage stellt (*record now, decrypt later*).[25] Die Notwendigkeit zur Vorsorge dürfte gleichzeitig Hemmschuh für eine systematische politisch-rechtliche Durchdringung des Themenfelds IT-Sicherheit sein: das in Zeiten von Corona viel zitierte Präventionsparadox – *there is no glory in prevention*.

Der Ansatz, Unternehmen verstärkt Vorsorgepflichten in Bezug auf IT-Sicherheit aufzuerlegen, findet sich bereits vielfach einfachgesetzlich[26], und wird im „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme", auch bekannt als „IT-Sicherheits-

22 *Muth*, Der Ransomware-Schrecken des deutschen Mittelstands, Süddeutsche Zeitung, 31.12.2020 zur Attacke auf die Funke Mediengruppe, https://www.sueddeutsche.de/digital/ransomware-clop-fin11-fire-eye-cybercrime-1.5161726. (abgerufen am 10.1.2020).

23 Konkrete Zahlen zum Vorfall sind nicht verfügbar; siehe generell *Bertschek/Janßen/Ohnemus*, IT-Sicherheit aus ökonomischer Perspektive, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 63f.

24 *Wolff*, You'll See This Message When It Is Too Late, The Legal and Economic Aftermath of Cybersecurity Breaches, 2018, S. 205ff.

25 Zum Entwicklungsstand von Quantencomputern mit Daten aus einer Studie mit dem Stand Juni 2020 siehe etwa https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer_node.html. (abgerufen am 10.1.2020).

26 Z.B. § 8a BSIG.

gesetzes 2.0“, der im Dezember 2020 auf Ebene des Bundeskabinetts beschlossen wurde[27], weiter ausgedehnt. Sicherheit ist indes teuer. Der „Erfüllungsaufwand“ für die Wirtschaft allein in der Folge der Änderungen im „IT-Sicherheitsgesetz 2.0“ wird auf 21,6 Millionen Euro geschätzt. Für die Verwaltung werden die Kosten auf 202,2 Millionen Euro jährlich geschätzt.[28]

C. IT-Sicherheit und Verfassungsrecht

In diesem Abschnitt erfolgen Bestandsaufnahme und Rekonstruktion dessen, was die Verfassung in Bezug auf die „IT-Sicherheit“ aufweist. Der Abschnitt dient dazu, verschiedene verfassungsrechtliche Bausteine sichtbar zu machen. Das uneinheitliche Gesamtbild, zu dem sich die Bausteine fügen, offenbart den Bedarf, Fragen der IT-Sicherheit grundsätzlich zu beleuchten.

I. IT-Sicherheit in privater Hand und die Rolle des Gewährleistungsstaates

Lagen in analogeren Zeiten zentrale „digitale“ Leistungen in den Händen des Staates, etwa die Telekommunikation, ist heute der private Wettbewerb die Regel: Die meisten Dienste, die jeder Zeitgenosse und jede Zeitgenossin in der Informationsgesellschaft über Kommunikationsinfrastrukturen benutzt, werden privatwirtschaftlich ermöglicht. Dabei sind die beteiligten Unternehmen oft mächtig; jedenfalls dem *durchschnittlichen* Nutzer überlegen.[29] In weiten Teilen handelt es sich also bei der Bereitstellung des digitalen Raumes als Grundlage für die Ausübung von Grundrechten einschließlich wirtschaftlicher Wertschöpfung nicht um staatliche Daseinsvorsorge, sondern um privatwirtschaftliche Wertschöpfung. Diese Ausgangslage ist für die heutige Rolle des „Gewährleistungsstaates“ prägend.

---

27 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme; https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=39F809A1188D562C61D08270E7764FA0.2_cid295?__blob=publicationFile&v=2 (abgerufen am 10.1.2020).

28 Siehe E 2 und E 3 in Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Fn. 27).

29 *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009, 1010.

Diejenigen Rechtsbereiche, die die Folgen der Privatisierung betreffen – auch „Privatisierungsfolgenrecht“[30] – regeln für gewisse netzgebundene Sektoren (z.B. Post, Telekommunikation) besondere Gewährleistungspflichten direkt in der Verfassung. So geht Art. 87f Abs. 1 GG in seinem Wortlaut davon aus, dass der Bund im Bereich des Postwesens und der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen *gewährleistet*. Für den Bereich der Energie finden sich keine expliziten verfassungsrechtlichen Vorgaben. Indes wird hier ein verfassungsrechtliches Mindestmaß über das verfassungsrechtliche Gebot der Gewährleistung gleichwertiger Lebensverhältnisse über die Ländergrenzen hinweg (Art. 72 Abs. 2 GG, Art. 104b Abs. 1 Nr. 2 GG) konstruiert, unter Zuhilfenahme des Sozialstaatsprinzips.

Einfachgesetzlich findet sich die Idee der Gewährleistung bzw. des Gewährleistungsstaates in dem Begriff des „Universaldienstes“ wieder.[31] So sieht z.B. das Regelungsmodell des Telekommunikationsgesetz (TKG) vor, dass ein konkret verpflichtetes Unternehmen einen finanziellen Ausgleich erhalten soll, zu dem alle abstrakt verpflichteten Unternehmen eine Abgabe leisten (§§ 82, 83 TKG). Die Verfassungsmäßigkeit dieser Sonderabgabe ist wiederum zweifelhaft.[32] Die Finanzverfassung geht von der Leitidee aus, dass die Finanzierung der staatlichen Aufgaben in erster Linie aus dem Ertrag der in Art. 105 ff. GG geregelten Einnahmequellen erfolgt. Alle Gemeinlasten sind danach aus Steuern zu finanzieren.

Bisher haben Unternehmen durch die freiwillige Übernahme von Pflichten das Universaldienstmodell praktisch kaum relevant werden lassen.[33] Ob sich das hier skizzierte Modell auf den Aspekt der IT-Sicherheit bei der Erbringung von Universaldiensten übertragen lässt, sei hier dahingestellt. Vor dem Hintergrund der verfassungsrechtlichen Fragwürdigkeiten wäre das Modell wohl auch über die sektoralen Grenzen des Privatisierungsfolgenrecht hinaus nicht tauglich, um Verantwortung zwischen Staat und Privaten aufzuteilen.

---

30 *Gärditz*, Die Organisation der Wirtschaftsverwaltung, § 4, Rn. 40; auch *Ludwigs*, Netzregulierungsrecht, § 12 Rn. 2, jeweils in Schmidt/Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 2016, 4. Auflage.

31 *Ludwigs*, § 12, Rn. 3, 33, 82.

32 Statt vieler etwa *Von Danwitz*, Die Universaldienstfinanzierungsabgaben im Telekommunikationsgesetz und im Postgesetz als verfassungswidrige Sonderabgaben, NvwZ 2000, S. 615.

33 *Möstl*, Art. 87f GG, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Rn. 81, 82 (Stand: 92. EL 2020).

II. IT-Sicherheit als Staatsaufgabe und der Gedanke der Vorsorge

Sicherheit ist Grund und Rechtfertigung jedes Staatswesens. In der aktuellen „Datenstrategie der Bundesregierung" heißt es dazu: „Neben entsprechenden Rechten der Einzelnen und Transparenz im Umgang mit Daten ist die Gewährleistung von struktureller Daten- und IT-Sicherheit für alle Beteiligten *existenziell*.[34] Die Fassbarkeit von IT-Sicherheit in der Kategorie „Staatsaufgabe" wird im Kern zu bejahen sein.[35] IT-Sicherheit als Staatsaufgabe bedeutet nicht, dass der Staat selbst tätig werden muss, vgl. auch Art. 33 Abs. 4 GG. *Hornung/Schallbruch* leiten einen „Auftrag" des angemessenen Schutzes von IT-Sicherheit aus der „Kernaufgabe des modernen Staates zur Gewährleistung von Sicherheit" ab, und führen zur verfassungsrechtlichen Herleitung den Beschluss des Bundesverfassungsgericht zum Kontaktsperregesetz von 1978 an.[36] Das Bundesverfassungsgericht ließ dort wissen, dass

> „[d]ie Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung […] *Verfassungswerte* [sind], die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet."[37]

Betrachtet man die Entwicklungen, die das heute 30-jährige Bundesamt für Sicherheit in der Informationstechnik (BSI) durchlaufen hat, so zeichnet sich hier eine Ausweitung der Aufgaben ab: zunächst stand der Schutz staatlicher Einrichtungen vor IT-Risiken im Vordergrund. Inzwischen werden auch Akteure in der Wirtschaft einbezogen.[38]

---

34 Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt
und nachhaltiges Wachstum, 27.1.2021. https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632. Hervorhebung der Autorin (abgerufen am 30.1.2020).

35 *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, Rn. 48.

36 *Hornung/Schallbruch*, Einführung, Rn. 7, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, unter Rekurs auf BVerfG 49, 24, 56.

37 BVerfG 49, 24, 56, Hervorhebung von der Autorin.

38 *Hornung*, Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, NJW 2015, 334; Selbstdarstellung des BSI: „Entscheidend erweitert wurden die Aufgaben und Befugnisse des BSI durch das im Juli 2015 in Kraft getretene „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz). Mit verbindlichen Mindestanforderungen an die

Staatsaufgabe ist dabei, was der Staat sich selbst zur Aufgabe macht, die Begründung einer Staatsaufgabe unterliegt keinem Verfassungsvorbehalt.[39] Die Einrichtung von Behörden wie etwa dem BSI und der immer weiter aufgefächerten Gesetzgebung im Bereich der IT-Sicherheit können dabei Indiz für eine Staatsaufgabe sein. Ein Schluss auf die Modalitäten und wohl auch Lastentragung der Aufgabenwahrnehmung durch den Staat selbst oder durch Dritte ist jedoch nicht möglich.

Die Rolle des Staates in der sich wandelnden Gesellschaft gepaart mit Herausforderungen neuer Technologien ist indes keine neue Fragestellung.[40] Der Begriff der Risikogesellschaft[41] drängt sich dabei im Zusammenhang mit der Frage nach Staatsaufgaben auf und stammt aus dem Kontext eines vorwiegend anlagenbezogenen staatlichen Risikomanagements. In der Staatsrechtslehre, insbesondere von *Grimm*, wird dazu beobachtet, dass im Zusammenhang mit immer weiter gehenden Staatsaufgaben das (Verfassungs-)recht an Steuerungskraft verliert. Damit einher gehen größere Handlungsspielräume der Administration.[42] *Köck* kommt (nicht im konkreten Kontext der IT-Sicherheit) zu dem Ergebnis, dass die Rolle des Staates sich dahingehend gewandelt hat, „die Organisation von Kommunikations- und Koordinationsprozessen durch Institutionalisierung von Wissen und Interessen, die Organisation von Wissensaggregierung (Monitoring) und die Ermöglichung von Risikotransparenz“[43] zu übernehmen.

IT-Sicherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen (KRITIS) und erhöht die Netzsicherheit in den Bereichen, deren Ausfall oder Beeinträchtigung *dramatische Folgen für Wirtschaft*, Staat und Gesellschaft in Deutschland hätte. Außerdem besteht eine Verpflichtung von KRITIS-Betreibern zur Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI.“, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html (abgerufen am 10.1.2020).

39 Statt vieler: *Korioth* in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Art. 30 GG, Rn. 9 (Stand: 92. EL 2020).

40 Überblick etwa bei *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, 2003, S. 8ff; *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, Verfassungsrechtliche Grundlagen und immissionsschutzrechtliche Ausformung, 1985.

41 Zum Begriff *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986.

42 *Grimm*, Der Wandel der Staatsaufgaben und die Krise des Rechtsstaates, in Grimm (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990, S. 291, 300.

43 *Köck*, Risikovorsorge als Staatsaufgabe, Archiv des öffentlichen Rechts, 1996, S. 1, 22.

Als Zwischenergebnis ist festzuhalten, dass IT-Sicherheit zu einer Staatsaufgabe geworden ist. Jedoch lassen sich daraus keine konkreten verfassungsrechtlichen Maßstäbe für die angemessene Verteilung von Verantwortung zwischen Staat und Privaten entwickeln, vor allem nicht zu Detailfragen und zur Finanzierung.

Auch der Rechtsgedanke der Vorsorge kann, mangels einer ausdrücklichen Staatszielbestimmung zur IT-Sicherheit, allein keine verfassungsrechtliche Steuerungskraft entfalten.

Positiv-rechtlich ist das Vorsorgeprinzip im Grundgesetz etwa in Form der Staatszielbestimmung des Umweltschutzes in Art. 20a GG verankert. Grundsätzlich kann Art. 20a GG auch dazu dienen, den gesetzgeberischen Spielraum bei der Frage, ob dieser tätig werden muss, einzuschränken, wenn auch Spielräume größer sind als die Beschränkungen.[44] Jedoch sind Staatszielbestimmungen keine aus sich selbst heraus operationalisierbaren Normen. Sie wirken grundsätzlich erst durch und über die konkretisierende wie aktualisierende Gesetzgebung.[45]

Wenn man den Staat in der Rolle des Vorsorge-Staates sieht, kommt der Staat seinen verfassungsrechtlichen Pflichten bereits dann nach, wenn er seine Verantwortung prozesshaft wahrnimmt, ohne jedoch ein konkretes Ergebnis zu schulden.

III. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Schutzpflichtendogmatik der Grundrechte könnte für ein Tätigwerden des Staates im Bereich der IT-Sicherheit in den Dienst genommen werden.[46] Grundrechte haben mehrere Dimensionen, in denen sie wirken. Sind in erster Linie Abwehrrechte gegen staatliches Eingriffshandeln. Sie gelten gemäß Artikel 1 Abs. 3 GG primär im Verhältnis zwischen Bürger und Staat. Grundrechte können auch schützendes Verhalten angesichts von Verletzungen und Gefährdungen grundrechtlich geschützter Güter erfordern. *Isensee* griff bereits 1982 das Spannungsverhältnis zwischen Sicherheit und Freiheit auf und versuchte, es über die Grundrechte zu lösen.[47]

---

44 *Voßkuhle*, Umweltschutz und Grundgesetz, NVwZ 2013, S. 1, 5.

45 *Scholz*, Art. 20 a GG, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar (Stand: 92. EL, 2020) Rn. 47.

46 Generell zurückhaltend: *Di Fabio*, Art. 2 GG in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar (Stand: 92. EL, 2020) Rn. 61f.

47 Grundlegend: *Isensee*, Das Grundrecht auf Sicherheit, 1983.

Angesprochen sein kann dabei die Legislative, die Exekutive oder die Judikative. Zudem können Grundrechte Drittwirkung entfalten, also in das Verhältnis von Privaten untereinander einwirken.[48]

Die meisten Grundrechte der deutschen Verfassungsordnung, ob positiv-rechtlich in der Verfassung verankert oder als Ausfluss der Rechtsfortbildung durch das Bundesverfassungsgericht, haben Anwendungsbereiche im digitalen Raum. Bei der Ausübung von einem Großteil der Grundrechte ist ein sicherer digitaler Raum Voraussetzung. Selbstverständlich können Grundrechte auch nach wie vor analog genossen werden, jedoch steigt die verfassungsrechtliche Relevanz der Vorbedingung der IT-Sicherheit für die Ausübung von einer großen Zahl von Grundrechten.

1. Positiv-rechtliche Aussagen des Grundgesetzes zur IT-Sicherheit

Der textliche Befund des Grundgesetzes zeigt, dass einige Grundrechte, etwa Art. 5 GG (Meinungs- und Pressefreiheit), Art. 10 GG (Fernmeldegeheimnis)[49] und Art. 13 GG (Unverletzlichkeit der Wohnung), gewisse Aspekte der Grundrechtsausübung im digitalen Raum schützen.[50] Eine eindeutige Zuweisung im Hinblick auf die Wahrnehmung und Ausgestaltung von IT-Sicherheit durch den Staat oder private Unternehmen lässt sich indes daraus nicht entnehmen. Vielmehr steht diesen Grundrechten die ebenfalls grundrechtlich abgesicherte unternehmerische Freiheit gegenüber, Art. 12 und 14 GG.

2. Rechtsfortbildungen durch das Bundesverfassungsgericht hin zur IT-Sicherheit

Das Bundesverfassungsgericht entwickelt seit den 1970er Jahren das allgemeine Persönlichkeitsrecht aus Art. 1 und 2 Abs. 1 GG.[51] Vorausgegangen war dabei schon seit den 1950er Jahren die Rechtsprechung des BGH zum

48 Einführend siehe *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, S. 1633.

49 BVerfG 100, 313; 106, 28, 110, 33; siehe auch *Hindelang*, Freiheit und Kommunikation. Zur verfassungsrechtlichen Sicherung kommunikativer Selbstbestimmung in einer vernetzten Gesellschaft, 2019.

50 Vgl. *Schliesky*, Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat, Ein Beitrag zur Zukunftsfähigkeit des Grundgesetzes am Vorabend des 70. Geburtstags, NvWZ 2019, S. 693, 698.

51 BVerfG 35, 202.

allgemeinen Persönlichkeitsrecht.[52] In Fortschreibung dieser Rechtsprechung markiert die Errungenschaft des Grundrechts auf informationelle Selbstbestimmung im Volkszählungsurteil von 1983 einen wichtigen Meilenstein.[53]

Seit dem Jahr 2008 spricht das Bundesverfassungsgericht vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[54] Diese grundrechtlichen Entwicklungen betreffen vor allem den *status negativus*, also die Abwehr staatlicher Eingriffe. Das Bundesverfassungsgericht charakterisierte das neu „gefundene" Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine „lückenschließende Gewährleistung… um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann."[55] Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme findet nach der Rechtsprechung des BVerfG im Verhältnis zur Telekommunikationsfreiheit des Art. 10 Abs. 1, zur Unverletzlichkeit der Wohnung des Art. 13 und zum Grundrecht auf informationelle Selbstbestimmung nur subsidiäre Anwendung.[56] In der Literatur wurde diese Neuentwicklung teilweise auch mangels einer Schutzlücke für überflüssig erachtet, die Rezeption war insgesamt eher kritisch.[57] Hier soll keine grundsätzliche Debatte darüber befeuert werden, ob es nicht wünschenswert wäre, die „digitalen" Individualrechte auch zu positiveren. Ihre Sichtbarkeit und Steuerungskraft würden jedoch davon profitieren. Dass eine Kodifikation möglich ist, zeigt etwa die europäische Grundrechtecharta, die entscheidende digitale Grundrechte enthält (z.B. Art. 8 GrC).

---

52 *Kipker*, Informationelle Freiheit und staatliche Sicherheit, 2016, S. 9, mit weiteren Nachweisen.

53 BVerfG 65, 1.

54 BVerfG 120, 274; *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009; *Bäcker*, Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in *Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009, S. 1; kritisch *Manssen*, Das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" – Ein gelungener Beitrag zur Findung unbenannter Freiheitsrechte? In *Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009, S. 61.

55 BVerfGE 120, 274, Rn. 169.

56 BVerfGE 120, 274, 302.

57 Siehe zum Meinungsstand: *Gersdorf*, Art. 2 GG, in Gersdorf/Paal (Hrsg.), BeckOK Informations- und Medienrecht (30. Ed, 2019), Rn. 23 mit weiteren Nachweisen.

3. Die Rolle des Staates über die Abwehrdimension hinaus?

Weniger klar ist, was die vom Bundesverfassungsgericht ausgegebene Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme über den *status negativus* des Grundrechts hinaus bedeutet. In der Literatur wurde eine über die abwehrrechtliche Dimension hinaus gehende Wirkmacht im unmittelbaren Nachgang zum Urteil bejaht.[58] In den etwa 12 Jahren, die seither vergangen sind, ist jedoch ein verfassungsrechtlicher Diskurs zur Rolle des Staates in diesem Themenfeld weitgehend ausgeblieben. *Poscher/Lassahan* stellen dies eher versteckt in einer Fußnote fest: „Im Zuge der immer weiteren Vernetzung wird sich in der Zukunft ein effektiver Schutz vor IT-bezogenen Beeinträchtigungen von Grundrechten womöglich nicht mehr allein durch sektorale oder auf den Schutzbereich nur einzelner Grundrechte beschränkter Maßnahmen verwirklichen lassen. Es erscheint denkbar, dass sich angesichts drohender Gefährdungen einer Vielzahl von Grundrechten durch Manipulation umfassend vernetzter, multifunktionaler Systeme im Ergebnis auch aus der Gesamtheit der potentiell betroffenen Grundrechte eine Schutzpflicht des Staates zu einem umfassenden IT-Sicherheits-Basisschutz ergibt."[59]

Freilich ist das Minimum an Schutz, den der Staat schuldet, vor dem Hintergrund des Untermaßverbotes[60] kaum zu konkretisieren. So erscheint es umso gewinnbringender, intra- und interdisziplinäre Argumente zu bündeln, um Handlungsspielräume und -pflichten des Staates genauer einzugrenzen.

---

58 *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009, 1019; *Roßnagel/Schnabel*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534, 3535. A.A. in zeitlichem Abstand: *Gersdorf*, Art. 2 GG, in Gersdorf/Paal (Hrsg.), BeckOK Informations- und Medienrecht (30. Ed, 2019), Rn. 29.

59 *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 133, 147, dort in der Fußnote 69.

60 BVerfGE 88, 203, 254 f.

D. Der Mehrwert eines intra- und interdisziplinären Blicks auf verfassungsrechtliche Fragen der IT-Sicherheit

Die Datenethikkommission widmete sich dem Thema IT-Sicherheit nur kursorisch in dem Abschlussgutachten vom 23. Oktober 2019. Dort werden die Begriffe der „risikoadäquaten Informationssicherheit" sowie der „risikoadaptierten Regulierung" verwendet.[61] Diese offenen Begriffe spiegeln die multidisziplinäre Fragestellung wider, die die IT-Sicherheit mit sich bringt. Auf die Notwendigkeit eines gelingenden *inter*disziplinären Austausches mit IT-Sicherheitsingenieuren für die angemessene Bewertung von Risiken der IT-Sicherheit und der entsprechenden Verantwortlichkeiten sei hier nur in der gebotenen Kürze hingewiesen.[62] Technische Fragen determinieren auch, welche Rolle der Staat in Rechtsverhältnissen einnehmen kann, die zwischen Privaten bestehen – etwa zwischen einer privaten Bank und einem Kunden.

I. Interdisziplinäre Möglichkeiten: IT-Sicherheit als Public Good

Ökonomisch geleitete *inter*disziplinäre Betrachtungen sind für die Fragestellung der IT-Sicherheit sehr relevant. IT-Sicherheit wird bisweilen als öffentliches Gut (*public good*) charakterisiert.[63] Bei öffentlichen Gütern kann es dazu kommen, dass die Verteilung von Kosten nicht ausschließlich auf diejenigen erfolgen kann, die ein Gut nutzen. Die vielfältigen ökonomischen Erwägungen, von Investitionskosten über Anreizstrukturen bis hin zu den Risiken staatlicher Sanktionierung, sind eine Dimension, die in diesem Beitrag nicht weiterverfolgt werden kann. Die ökonomischen Hintergründe sind jedoch tauglicher Ansatzpunkt für eine kostenoptimale Verteilung von Verantwortung zwischen Staat und Unternehmen.[64] Für

61 Gutachten der Datenethikkommission, 23.10.2019, www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2 (abgerufen am 10.1.2020).

62 Generell dazu bereits *Forsthoff*, Der Jurist in der industriellen Gesellschaft, NJW 1960, S. 1273, 1275.

63 *Bertschek/Janßen/Ohnemus*, IT-Sicherheit aus ökonomischer Perspektive, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020 S. 63, 67; *Schliesky*, Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat, Ein Beitrag zur Zukunftsfähigkeit des Grundgesetzes am Vorabend des 70. Geburtstags, NvWZ 2019, S. 693, 700.

64 Weiterführend *Taddeo*, Is Cybersecurity a Public Good?, Minds and Machines 2019, S. 349.

den vorliegenden Beitrag dient die Hypothese der IT-Sicherheit als öffentliches Gut jedenfalls als Rechtfertigungsmöglichkeit für staatliches Handeln und staatliche Verantwortung für den Bereich der IT-Sicherheit.[65] Für die Risikobewertung im Bereich der IT-Sicherheit ist das Verständnis von (neuen) Geschäftsmodellen von Unternehmen, aber auch von Kriminellen wichtig, um Kosten und Nutzen von IT-Sicherheit besser zu verstehen.[66] So werden nicht nur Kosten für die IT-Sicherheit in den Blick genommen, sondern auch die Kosten sichtbar, die entstehen, wenn ein Angriff auf ein IT-System Erfolg hat.

II. Ein intradisziplinärer Blick auf den verfassungsrechtlicher Konkretisierungsbedarf zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Für die Verantwortung des Staates im Rahmen der Gewährleistung von IT-Sicherheit lassen sich keine konkreten Schlüsse ziehen, welches Ergebnis, wenn überhaupt, der Staat schuldet.

Für den Teilbereich der Ausnutzung von IT-Schwachstellen für straf- und nachrichtendienstliche Maßnahmen haben u.a. *Derin/Golla* angemahnt, dass vor dem Hintergrund des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die Beeinträchtigungen der IT-Sicherheit grundsätzlich nicht hinnehmbar seien, die entstehen, wenn der Staat Sicherheitslücken weitläufig offenhält und es unterlässt, diese zu melden und zu ihrer Schließung beizutragen.[67]

Auch für das Handeln der gefahrenabwehrenden Verwaltung vermag das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht Recht wahrgenommen zu werden. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, das beschrieben wird als „Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen aller

65 Grundlegend, wenn auch nicht bezogen auf IT-Sicherheit: *Ostrom*, Governing the Commons: The Evolution of Institutions for Collective Action, 1990.

66 Z.B. *Acquisti/ Taylor/ Wagman*, The Economics of Privacy, Journal of Economic Literature 2016, S. 442; *Lusthaus*, Industry of Anonymity: Inside the Business of Cybercrime, 2018.

67 *Derin/Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit? Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung“ und Quellen-TKÜ, NJW 2019, S. 1111, 1115; siehe auch generell *Snowden*, Permanent Record, 2019.

Größen"[68] ist ein Instrument des soft law. In dem 810-seitigen Werk, das jährlich aktualisiert wird, wird das Grundgesetz nur ein einziges Mal erwähnt, dies geschieht im Zusammenhang mit dem Datenschutz.[69] Ein Rekurs auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgt nicht.

Der unbestimmte Rechtsbegriff der Angemessenheit, der etwa in § 8a des BSI-Gesetzes verwendet wird, und in dem gewissen Unternehmen ein Mindestniveau an IT-Sicherheit vorgeschrieben wird, bleibt grobkörnig.[70] Im Kontrast hierzu meint *Bull* für den verwandten Bereich des Datenschutzes Fehlentwicklungen zu beobachten, die mit der zu engmaschigen Durchnormierung aller Formen des Umgangs mit personenbezogenen Daten einher gingen. Er verallgemeinert seine Kritik dahingehend, dass die Wertordnung, die in unserer Verfassung angelegt sei, die Abwehr von unerwünschtem Verhalten grundsätzlich nicht als alleinige Aufgabe des Staates anlege.[71]

Verfassungsrechtliche Wertungen wirken auf vielfache Weise in das Privatrecht und auf das Handeln Privater auch untereinander ein.[72] Der erste Zugriff auf die konkrete Ausgestaltung von IT-Sicherheit liegt in privater Hand. Vor diesem Hintergrund scheint eine *intra*disziplinäre Sichtweise, wie in diesem Tagungsband, auf die Frage der Verantwortungsverteilung besonders lohnend. Für das Zivilrecht, in dem verfassungsrechtliche Wertungen über Generalklauseln wie §§ 133, 134, 157, 242 BGB, das Recht der AGB und anderen generalklauselartigen Auffangnormen (z.B. § 280, § 823 BGB) Wirkung entfalten, bietet der Gehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Syste-

68 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz- Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6 (abgerufen am 10.1.2020).

69 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz- Kompendium, Abschnitt CON 2 (Fn 68).

70 *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, Rn. 3.

71 *Bull*, Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, JZ 2017, S. 797, 802.

72 Ausführlich bei *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, Eine verfassungsrechtliche Untersuchung zur Privatrechtswirkung des Grundgesetzes, 2001.

me noch wenig konkrete Orientierung.[73] Der Ausgleich zwischen verschiedenen nicht nur privaten Interessen und Verantwortungsbereichen scheint somit weitgehend in Richterhand zu liegen. In der Literatur wird versucht, zur Bestimmung von IT-Sicherheitsanforderungen auf spezialgesetzliche Regelungen und technische Normen zurückzugreifen.[74]

E. Fazit: von der Nützlichkeit eines verfassungsrechtlichen Kompasses für Fragen der IT-Sicherheit

Das Grundgesetz ist zukunftsgerichtet. Dies findet unter anderem in der Ewigkeitsklausel Ausdruck. Das Verfassungsrecht hat eine wichtige Orientierungsfunktion inne: technologische Entwicklungen sollen grundrechts- und gemeinwohlverträglich gestaltet werden.

Wolfgang Hoffmann-Riem fasste die Ausgangsposition für den verwandten Bereich der Regulierung von „Big Data" folgendermaßen zusammen:

> *„Ob und wie Chancen der Digitalisierung genutzt und Risiken minimiert werden, ist gestaltbar. Gestaltende Akteure sind wirtschaftliche Unternehmen, die vielen Nutzer, individuelle Innovatoren, interessenwahrnehmende Verbände, aber auch Hacker. Für die Schaffung eines Rahmens zur Sicherung von Individual- und Gemeinwohl aber ist der Staat zuständig. Dabei kann er neben anderem das Steuerungsmedium Recht einsetzen."*[75]

Der Ausgleich von staatlichen und privaten Interessen einerseits, und der Ausgleich zwischen Privaten andererseits, sollte auf die Verfassung rückführbar sein. Dabei muss auch sichergestellt werden, dass die Errungenschaften aus der analogen Zeit angemessen in neue Kontexte übersetzt werden. Verfassungsrechtlich klare Maßstäbe und dogmatische Durchdringung von Fragen der IT-Sicherheit sind dabei kein Selbstzweck. Sie sind auch für Unternehmen ein Gewinn an Rechtssicherheit[76]; sie können auch

---

73 *Wehage*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht, 2013, S. 155ff.

74 *Pour Rafsendjani/Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020 S. 181, 190ff.

75 *Hoffmann-Riem*, Big Data – Regulative Herausforderungen, 2018, Vorwort, S. 5.

76 *Roßnagel/Hornung*, Handlungsbedarf für einen Grundrechteausgleich, in: *Roßnagel/ Hornung*, (Hrsg.) Grundrechtsschutz im Smart Car, Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, 2019, S. 470, 472.

ein Standortvorteil sein. Ein hoher Abstraktionsgrad, den das Verfassungsrecht erlaubt, ist dabei auch nicht in Verdacht, Hemmschuh für Innovationen durch Überregulierung zu sein.

Grundsätzlich fraglich ist, ob die IT-Sicherheit ähnlich kleinteilig zu fassen ist wie bisherige Herausforderungen, wie etwa ausgehend von Atomkraft oder gefährlichen Industrieanlagen. Der Facettenreichtum der Querschnittsmaterie der IT-Sicherheit stellt gegenüber dem klassischen Recht „Recht des Risikomanagements", wie etwa dem des Rechts des Immissionsschutzes, womöglich nicht nur einen graduellen, sondern einen grundsätzlichen Unterschied dar. Dieser Unterschied drückt sich darin aus, dass die Gefahren für die Sicherheit von IT-Systemen bisweilen nicht abgrenzbar und damit für einen allein Pflichtigen beherrschbar sind. Er erfordert aus regulatorischer Sicht einen umfassenden Ansatz. Fragen der IT-Sicherheit betreffen die Hardware, Software und die Personen, die die Technik bedienen und benutzen. Umso mehr scheint eine abstrakte verfassungsrechtliche und zusammenführende Festlegung sinnvoll.

Sollte das deutsche Verfassungsrecht weiter nur zögerlich entwickelt und wissenschaftlich begleitet werden, wird eine noch weitergehende „Hochzonung" auf das (sekundäre) Recht der Europäischen Union erfolgen, wie es beim Recht des Datenschutzes der Fall war. Diese Verlagerung in ein Mehrebenensystem ist durchaus auch vorteilhaft, und im Integrationsprogramm des Grundgesetzes selbst so angelegt. Die Verlagerung in eine Verordnung, wie etwa der Datenschutzgrundverordnung, erschwert jedoch auch die Nachjustierung und die Veränderung von darin enthaltenen Grundentscheidungen. Die Mühe, sich im deutschen Verfassungsrecht vertieft mit der Materie auseinanderzusetzen, lohnt indes. Auch in anderen Teilbereichen haben sich Argumente und Problemlösungen, die im Rahmen einer nationalen Grundrechtsordnung erarbeitet wurden und sich dort als praktikabel erweisen haben, Einfluss auf unionsrechtliche Entwicklungen gezeitigt.[77]

77 *Bäcker* spricht von „grundrechtlichen Exportartikeln" und einem möglichen „Beitrag zum europäischen Rechtsgespräch", Grundrechtlicher Informationsschutz gegen Private, Der Staat 2012, S. 91, 115.

Cybersecurity in der unternehmerischen Praxis des Mittelstandes

Andreas Beyer

A. Cyberangriffe und -risiken in mittelständischen Unternehmen

„There is no glory in prevention.", sagte der Virologe Christian Drosten im März 2020 im Zusammenhang mit der Verbreitung des Coronavirus. Der Grundsatz, dass man durch die Vermeidung von Risiken keinen Ruhm erlangt, trifft – wie dieser Beitrag zeigen wird – auch auf den bisherigen Umgang von kleinen und mittelständischen Unternehmen mit dem Thema Cybersecurity zu. Doch ist eine langfristige Strategie zur Risikominimierung sowohl in der Coronapandemie als auch für eine sichere IT-Infrastruktur erfahrungsgemäß der Schlüssel zum Erfolg.

Die fortschreitende Digitalisierung birgt Gefahren und potenzielle Risiken für Unternehmen. So drohen Unternehmen weltweit innerhalb eines Zeitraums von fünf Jahren gigantische Mehrkosten und Umsatzverluste durch Cyber-Angriffe in Höhe von rund 5,2 Billionen Dollar.[1] Dementgegen erscheint das Bewusstsein insbesondere von kleinen und mittelständischen Unternehmen[2] für Cybersecurity und die damit verbundene Vermeidung von Risiken für die IT-Infrastruktur und den fortlaufenden Betrieb eines Unternehmens oftmals noch nicht ausgeprägt genug. Zwar erkennen bereits ca. zwei Drittel der mittelständischen Unternehmen die Gefahr und das Risiko von Cyberkriminalität grundsätzlich an, jedoch sehen lediglich ca. ein Drittel ein solches Risiko für ihren eigenen Betrieb.[3]

---

1 *Abbosh/Bissel*, Accenture Studie "Securing the digital economy", S. 16, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50 (abgerufen am 29.12.2020).

2 Im Folgenden: KMU.

3 Gesamtverband der deutschen Versicherungswirtschaft (GDV): Cyberrisiken im Mittelstand, 2020, S. 6, https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf (abgerufen am 12.04.2021).

Dieses mangelnde Bewusstsein ist problematisch, weil gerade KMU zunehmend von Cyberangriffen betroffen sind.[4]

Um auf dem Markt wettbewerbsfähig zu bleiben, können sich KMU der fortschreitenden Digitalisierung nicht entziehen. Dabei nimmt die Abhängigkeit der KMU von IT-Systemen und -strukturen stetig zu.[5] Gleichzeitig werden Angriffe auf die Informationsstrukturen im Cyberraum zunehmend komplexer und umfangreicher.[6] Eine sichere IT-Infrastruktur und wirksame Maßnahmen zur Prävention von Cyberangriffen werden somit auch für diese Unternehmen immer wichtiger. Jedes vierte mittelständische Unternehmen war bereits von erfolgreichen Cyberangriffen betroffen.[7] Bei einer Forsa-Umfrage im Auftrag des Gesamtverbands der deutschen Versicherungswirtschaft e.V. (GDV) gaben mehr als die Hälfte (59 %) der betroffenen Unternehmen an, sie hätten in Folge der Cyberangriffe unter Betriebsausfällen gelitten.[8] Solche Unterbrechungen der Betriebsabläufe stellen gemeinsam mit den damit verbundenen Kosten für die Wiederherstellung der Daten und IT-Systeme die regelmäßige Folge von Cyberangriffen dar.[9]

Der Begriff der Cybersecurity umfasst vor allem die Einhaltung von technischen und organisatorischen Maßnahmen, die für den Schutz des Unternehmens, der Arbeitnehmer, der Kunden sowie der Lieferanten vor Angriffen von außen erforderlich sind.[10] Art. 32 DSGVO stellt dabei die zentrale gesetzliche Grundlage dar. Hiernach sind Unternehmen, die selbst oder im Auftrag eines Anderen personenbezogene Daten verarbeiten insbesondere dazu verpflichtet, die zum Schutz der Daten angemessenen

---

4 Bitkom-Studie Wirtschaftsschutz 2020, S. 8, https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf (abgerufen am 13.01.2021); *Meyer*, *Seitz*, Deloitte Studie: Cybersecurity im Mittelstand, Download unter: https://www2.deloitte.com/de/de/pages/mittelstand/contents/cyber-security-im-mittelstand-studie.html (abgerufen am 13.01.2021).

5 GDV: Cyberrisiken im Mittelstand 2020 (Fn. 3), S. 7.

6 *Schuster*, Cyberangriffe werden immer komplexer, https://www.it-business.de/cyberangriffe-werden-immer-komplexer-a-798881/ (abgerufen am 13.01.2021).

7 Gesamtverband der deutschen Versicherungswirtschaft (GDV): Cyberrisiken im Mittelstand, 2019, S. 5, https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf (abgerufen am 20.04.2021).

8 GDV: Cyberrisiken im Mittelstand 2019 (Fn. 7), S. 5.

9 *Dreißigacker u.a.*, PWC Studie: Cyberangriffe gegen Unternehmen in Deutschland, S. 36 ff., https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf (abgerufen am 13.01.2021).

10 *Wybitul*, Vermeidung von DS-GVO-Risiken nach Datenpannen und Cyberangriffen, NJW 2020, 2577.

technischen und organisatorischen Maßnahmen zu treffen. Eine wirksame Minimierung von Risiken im Zusammenhang mit Cyberattacken ist daher das wesentliche Element für eine sichere und unterbrechungsfreie IT-Infrastruktur. Hierbei stellen die Identifikation, die Beurteilung und der korrekte Umgang mit den jeweiligen Risiken die zentrale Herausforderung für kleine und mittelständische Unternehmen dar.

Der Verfasser leitet als Syndikusrechtsanwalt die Rechtsabteilung der Vimcar GmbH[11], einem mittelständisches Berliner Tech-Unternehmen, welches zu den 20 wachstumsstärksten Tech-Unternehmen Deutschlands zählt und auf dem Markt für digitale Flottenmanagementlösungen für Unternehmen tätig ist.[12] Zuvor leitete er die Rechtsabteilung der VAI Trade GmbH, einem Fintech-Startup und Tochterunternehmen der Berliner Volksbank eG. Die Erkenntnisse aus diesen Tätigkeiten und der damit einhergehenden juristischen Betreuung des Themas Cybersecurity sowie kontinuierlichem Austausch mit der Geschäftsführung und dem CTO von Vimcar, geben diesem Beitrag fachliche und praktische Relevanz.

Im Folgenden werden zunächst einige ausgewählte und häufig vorkommende Cyberangriffe und -risiken von außen und innen näher beleuchtet (I.). Anschließend werden Lösungsansätze und Präventionsstrategien dargelegt, die kleine und mittelständische Unternehmen dabei unterstützen können, mit dem wichtigen Thema der Cybersecurity umzugehen und die Risiken weit wie möglich zu minimieren (II.). Schließlich wird dieser Beitrag aufzeigen, dass der Umgang mit dem Thema Cybersecurity nicht nur Aufgabe der Rechts- oder IT-Abteilungen ist (III.). Vielmehr stehen insbesondere die Geschäftsleitungen der Unternehmen in der Pflicht, entsprechende Strukturen zu schaffen und Budgets freizugeben.

I. Cyberangriffe und -risiken von außen

Die Häufigkeit und Qualität der Cyberangriffe von außen hat in den letzten fünf Jahren enorm zugenommen. In den Jahren 2015 und 2017 waren circa 50 % der im Rahmen einer Bitkom-Studie zum Wirtschaftsschutz befragten Unternehmen von Angriffen wie Datendiebstahl, Industriespiona-

11 Im Folgenden: Vimcar.

12 Deloitte, Winners of the 2020 Technology Fast 50 Award, https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/fast-50-2020-germany-winners.html (abgerufen am 17.04.2021).

ge oder Sabotage betroffen; im Jahre 2020 waren es bereits 75 % der befragten Unternehmen.[13]

1. *Cyberangriffe durch Dritte*

Angriffe mittels einer Schadsoftware stellten im Jahre 2018 mit 53 % die häufigste Form von Cyberangriffen durch Dritte auf deutsche Unternehmen und Institutionen dar.[14] Unter den Begriff Schadsoftware oder Schadprogramme fallen alle Arten von Software, die schädliche Funktionen auf einem Computersystem verursachen können.[15] In 90 % der Fälle von Cyberangriffen durch Dritte mittels Schadsoftware dienten dabei schädliche Anhänge oder Links in E-Mails als Zugangsmöglichkeit.[16] Im Lagebericht des Bundesamts für Sicherheit in der Informationstechnik aus dem Jahre 2019 wurde das „Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware" sowie die „Infektion mit Schadsoftware über Internet und Intranet" als massive Risiken mit weiterhin zunehmender Tendenz identifiziert.[17]

a. Ransomware

Das Bundeskriminalamt bezeichnet *Ransomware* in einem aktuellen Report als „die primäre, existenzielle Bedrohung von Unternehmen".[18] Unter dem Begriff der *Ransomware* sind Schadprogramme zu verstehen, die den Zugriff auf das eigene Computersystem oder die eigenen Dateien durch Datenverschlüsselung einschränken oder verhindern.[19] Die Freigabe der Daten oder des Systems erfolgt in der Regel erst dann, wenn ein vom

13 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 7.
14 BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 49, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7 (abgerufen am 27.12.2020).
15 BSI, Die Lage der IT-Sicherheit in Deutschland 2019 (Fn. 14), S. 11.
16 BSI, Cyber-Sicherheitsumfrage der Allianz für Cybersicherheit 2018, S. 12, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9 (abgerufen am 20.04.2021).
17 BSI, Die Lage der IT-Sicherheit in Deutschland 2019, (Fn. 14), S. 11.
18 Bundeskriminalamt, Cybercrime, Bundeslagebild 2019, S. 56, zum Download unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (abgerufen am 03.01.2021).
19 *Beukelmann*, NJW Spezial 2017, 376, 376.

Täter geforderter, als „Lösegeld" bezeichneter Geldbetrag, meist in Form von Kryptowährungen, bezahlt wurde.[20] Bei diesen Schadprogrammen handelt es sich in der Regel um Verschlüsselungstrojaner, die zufällig oder gezielt durch infizierte Anhänge in E-Mails oder durch das Besuchen von vorgetäuschten Websites Zugriff auf Systeme erhalten.[21] Mittlerweile übersteigt die Anzahl der existierenden Varianten von Schadsoftware die Milliardengrenze und täglich kommen durchschnittlich 320.000 neue Schadprogramme hinzu.[22] Der Modus Operandi der Cyberkriminellen besteht häufig aus gefälschten Bewerbungsmails auf tatsächlich vom betroffenen Unternehmen geschaltete Stellenanzeigen. Diese E-Mails enthalten als Bewerbungsunterlagen getarnte Anhänge, die beim Herunterladen und Öffnen der Dateien Verschlüsselungstrojaner aktivieren.[23] Der Umstand, dass das Unternehmen infolge eines erfolgreichen Angriffs bis zur möglichen Lösegeldzahlung keinen Zugriff auf gespeicherte Daten hat, kann im schlimmsten Falle enorme Auswirkungen auf die gesamte unternehmerische Existenz haben.[24] Potenzielle Folgen sind dabei Eigenschäden wie Betriebsunterbrechungen und Reputationsschäden sowie Fremdschäden, die infolge der Nichterfüllung vertraglicher Verpflichtungen gegenüber Dritten entstehen.[25] Seit dem Jahr 2016 ist ein eindeutiger Trend zu einem kontinuierlichen Anstieg der Risiken durch *Ransomware* zu beobachten.[26]

WannaCry ist wohl die weltweit bekannteste *Ransomware*, welche seit Jahren erhebliche Schäden anrichtet. Sie infizierte im Mai 2017 innerhalb weniger Stunden hunderttausende Computer und erreichte in den folgenden Monaten nach Einschätzung der europäischen Ermittlungsbehörde Europol weltweit ein „beispielloses Ausmaß".[27] Neben Verbrauchern sowie kleinen und mittleren Unternehmen waren auch Großkonzerne, wie

---

20 *Salomon*, MMR 2016, 575, 575; *Wabnitz/Janovsky*, WirtschaftsStrafR-HdB, 6. Kapitel. Geldwäsche, 5. Aufl. 2020 Rn. 29c.

21 *Siller*, Definition Trojaner, in: Gablers Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/trojaner-53413 (abgerufen am 20.04.2021).

22 BSI, Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (abgerufen am 04.01.2020).

23 *Ceffinato*, NZWiSt 2016, 464, 467.

24 *Salomon* (Fn. 20), 575.

25 BSI, Ransomware Bedrohungslage, Prävention und Reaktion 2019, S. 8, zum Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html (abgerufen am 19.04.2021).

26 BSI, Die Lage der IT-Sicherheit in Deutschland 2019 (Fn. 14), S. 17.

27 *Dörner*, Was steckt hinter dem Wanny-Cry-Angriff?, https://t3n.de/news/wannacry-podcast-823684/ (abgerufen am 12.01.2021).

Renault oder FedEx, Regierungsbehörden, wie z.B. das russische Innenministerium oder der britische National Health Service mit seinen Krankenhäusern betroffen. Bei der Deutschen Bahn sorgte die Schadsoftware für einen Ausfall der Anzeigetafeln.[28] Auch 2019 noch soll *WannaCry* weltweit für 23,56 % aller *Ransomware*-Attacken verantwortlich gewesen sein und verursachte dabei Schäden in Höhe von ca. 4 Milliarden US-Dollar.[29] Rund zwei Drittel der betroffenen Nutzer fingen sich dabei die *Ransomware* über Spam- oder *Phishing*-E-Mails ein.[30] Die *WannaCry Ransomware* ist so programmiert, dass sie sich nach einer initialen Infektion ohne Zutun eines Nutzers in einem Netzwerk von einem Computer zum anderen ausbreitet und Systeme gezielt verschlüsselt. Dies kann insbesondere in Netzwerken von Unternehmen und Organisationen zu großflächigen Systemausfällen führen.[31]

Ein aktuelles Beispiel für Angriffe auf Unternehmen mittels *Ransomware* stellt der Cyberangriff auf die Funke-Mediengruppe im Dezember 2020 dar. Dabei verschlüsselte die Schadsoftware sämtliche IT-Systeme. Infolgedessen litt die Funke-Mediengruppe mehrere Wochen unter den Folgen der Attacke. Es konnten weder E-Mails empfangen werden, noch funktionierte die Telefonanlage. Daher mussten zunächst alle genutzten IT-Systeme bundesweit heruntergefahren werden.[32] Von den Angriffen waren alle großen Standorte der Funke-Mediengruppe betroffen. Zur Funke-Mediengruppe gehören insgesamt zwölf Regionalzeitungen, darunter die „Berliner Morgenpost" und das „Hamburger Abendblatt". Alle Ausgaben dieser Zeitungen konnten nur sehr eingeschränkt erscheinen.[33] Der Weg zu einer wieder störungsfreien IT stellte sich beinahe als Sisyphus-

28 *Briegleb*, WannaCry: Was wir bisher über die Ransomware-Attacke wissen, https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html (abgerufen am 12.01.2021).

29 *Dörner*, Was steckt hinter dem Wanny-Cry-Angriff? (Fn. 27).

30 *Brien*, Ransomware reloaded: Wanna Cry verursacht immer noch Schäden in Milliardenhöhe, https://t3n.de/news/ransomware-reloaded-wannacry-1240246/ (abgerufen am 12.01.2021).

31 BSI, Weltweite Cyber-Sicherheitsvorfälle durch Ransomware, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/PM_WannaCry_13052017.html (abgerufen am 12.01.2021).

32 Wilkens, Trojaner-Angriff auf Funke-Mediengruppe dauert an – Notausgaben am Kiosk, https://www.heise.de/news/Trojaner-Angriff-auf-Funke-Mediengruppe-dauert-an-Notausgaben-am-Kiosk-4999342.html (abgerufen am 12.01.2021).

33 Thier, Hacker greifen Funke-Mediengruppe an – Erpressungsversuch vermutet, https://www.nzz.ch/technologie/hacker-greifen-funke-mediengruppe-an-ld.1593670 (abgerufen am 04.01.2021).

Arbeit heraus, da 6000 potenziell infizierte Rechner infrage kamen, die jeweils einzeln sehr aufwändig überprüft werden mussten. Die kolportierten Meldungen zu einer Lösegeldforderung in Form von Bitcoin ließ sowohl die Funke-Mediengruppe als auch die Staatsanwaltschaft unkommentiert.[34]

Die Zahlung von Lösegeld im Rahmen eines Cyberangriffs mittels *Ransomware* stellt sich als nicht unproblematisch dar. Zum einen können Unternehmen nicht mit absoluter Sicherheit davon ausgehen, dass die Täter die Unternehmensdaten und -systeme nach Zahlung des Lösegelds tatsächlich entschlüsseln.[35] Zum anderen birgt die Zahlung des Lösegelds zumindest die Möglichkeit, sich gemäß § 129 Absatz 1 Satz 2 StGB wegen Unterstützung einer kriminellen Vereinigung strafbar zu machen. Nach der wohl herrschenden Meinung in Rechtsprechung und Schrifttum liegt eine Verwirklichung des Straftatbestandes durch die Lösegeldzahlung vor. Diese ist weder durch den rechtfertigenden Notstand gemäß § 34 StGB gerechtfertigt, noch ist sie gemäß § 35 StGB entschuldigt, weil durch die Cyberangriffe in aller Regel keine Gefahr für Leib, Leben oder Freiheit eines Menschen besteht. Die herrschende Meinung wendet bisher die sogenannte Mitläufer-Klausel gemäß § 129 Abs. 6 StGB an. Diese gibt vor, dass „bei Beteiligten, deren Schuld gering und deren Mitwirkung von untergeordneter Bedeutung ist, von einer Bestrafung [...] abgesehen werden kann." Die Voraussetzungen dieser Klausel sind in den Fällen verschlüsselter IT-Systeme von Unternehmen regelmäßig gegeben, da die finanzielle Unterstützung ebenso wie die Schuld durch die Drucksituation als vergleichsweise gering anzusehen ist.[36] Die Klausel verhindert allerdings nur die Bestrafung, nicht aber den Schuldspruch und die Kostenfolge des § 465 StPO. Parallel dazu eröffnet die Mitläufer-Klausel die Möglichkeit eines Absehens von der Verfolgung gem. § 153b StPO.[37] Allerdings ist dies für die o.g. Fallkonstellation nicht höchstrichterlich entschieden, sodass Unsicherheiten in Bezug auf die strafrechtliche Bewertung bestehen bleiben. Zudem laufen Unternehmen durch die Bereitschaft zur Lösegeldzahlung Ge-

34 *Linde/Renner*, Hackerangriff auf Funke-Mediengruppe "hält unvermindert an" – Lösegeldforderung soll eingegangen sein, https://www.handelsblatt.com/technik/it-internet/cyberkriminalitaet-hackerangriff-auf-funke-mediengruppe-haelt-unvermindert-an-loesegeldforderung-soll-eingegangen-sein/26753992.html?ticket=ST-2610008-2L4DLvqXCdDycWJOyICv-ap1 (abgerufen am 12.01.2021).

35 Wie z.B. bei der Ransomware *GermanWiper* vgl. Bundeskriminalamt (Fn. 18), S. 5.

36 *Salomon* (Fn. 20), 577.

37 *Salomon* (Fn. 20), 577.

fahr, sich für Cyberkriminelle attraktiv zu machen und in der Folge erneut Opfer eines solchen Angriffs durch *Ransomware* zu werden. Aus diesem Grund lässt sich bei von Cyberattacken betroffenen Unternehmen beobachten, dass Fragen der Medien zu etwaigen Lösegeldzahlungen für die Entschlüsselung von Daten regelmäßig unbeantwortet bleiben.[38]

b. Phishing

Unter *Phishing* versteht man Versuche, über gefälschte Websites, E-Mails oder Kurznachrichten an persönliche Daten eines Nutzers zu gelangen, um damit einen Identitätsdiebstahl zu begehen. Ziel dieses Vorgehens ist es, mit den persönlichen Daten beispielsweise Zugang zu unternehmensinternen Systemen zu erhalten, um die dort enthaltenen Daten auszuspähen, zu verschlüsseln oder zu löschen.[39] *Phishing*-Nachrichten werden meist unter dem Deckmantel vertrauenswürdiger Geschäftspartner oder Dienstleister per E-Mail oder Instant-Messaging versandt und fordern den Empfänger auf, auf einer nachgeahmten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Typisch ist dabei die Nachahmung des Internetauftritts einer vertrauenswürdigen Stelle, etwa der Website eines E-Mail-Dienstleisters, durch die Verwendung des bekannten Corporate Designs. Der Nutzer wird auf einer solchen gefälschten Website etwa dazu aufgefordert, in ein Formular die Passwörter, PINs oder ID-Kennungen für den E-Mail-Dienst oder andere Produkte externer Dienstleister einzugeben. Diese Daten erhalten anschließend die Ersteller der gefälschten Websites. Der jeweilige Nutzer ist sich oftmals auch nach Eingabe der Daten nicht darüber im Klaren, dass die Daten an unautorisierte Personen gelangt sind. Währenddessen können die Phisher die erhaltenen unternehmensinternen Zugänge für ihre Zwecke missbrauchen.[40]

c. Spear-Phishing

Emotet galt bisher als eine der schädlichsten *Ransomwares* weltweit und infizierte auch in Deutschland IT-Systeme zahlreicher Unternehmen und In-

38 *Linde/Renner* (Fn. 34).
39 Auer-Reinsdorff/Conrad IT-R-HdB, § 3 Technische Grundlagen des Internets, 3. Aufl. 2019, Rn. 274.
40 Grützner/Jakob, Compliance von A-Z, 2. Aufl. 2015, P – Phishing.

stitutionen.[41] Im Jahr 2019 waren zahlreiche Behörden und Unternehmen, darunter die Bundesanstalt für Immobilienaufgaben, eine Niederlassung des Industriekonzerns Norsk Hydro, das Kammergericht in Berlin sowie verschiedene Krankenhäuser und lokale Stadtverwaltungen von Angriffen mittels *Emotet* betroffen. BSI-Präsident Arne Schönbohm bezeichnete *Emotet* vor diesem Hintergrund als „König der Schadsoftware".[42]

Emotet war in der Lage, besonders authentisch aussehende *Phishing*-Mails zu verschicken. Dazu las die Schadsoftware Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Diese Informationen nutzte sie automatisiert zur Weiterverbreitung, sodass die Empfänger fingierte E-Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen.[43] Aufgrund der korrekten Angabe der Namen und E-Mail-Adressen des jeweiligen Absenders und Empfängers in Betreff, Anrede und Signatur wirkten diese Nachrichten auf viele Empfänger authentisch. In der Folge konnten die Angreifer nahezu perfekte *Phishing*-Mails versenden, die an das gängige Kommunikationsschema des Absenders angepasst waren.[44]

Dieses maßgeschneiderte Erstellen von *Phishing*-Mails wird als *Spear-Phishing* bezeichnet. Mittels *Emotet* und anderer *Spear-Phishing* Software sind Kriminelle bereits in hochgesicherte Netzwerke von Regierungen und Rüstungskonzernen eingedrungen.[45] Wenn diese maßgeschneiderten E-Mails mittels einer Software automatisiert erstellt und in sehr großer

41 BSI, Aktuelle Information zur Schadsoftware Emotet, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html (abgerufen am 05.01.2020); Bundeskriminalamt, Infrastruktur der Emotet-Schadsoftware zerschlagen, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html (abgerufen am 12.04.2021).

42 *Beuth*, Wer ist Mummy Spider, https://www.spiegel.de/netzwelt/web/trojaner-emotet-wer-ist-ivan-a-a8bf3c85-cac9-4cb4-8755-d350ff5850f7 (abgerufen am 05.01.2020).

43 BSI, Informationen zur Schadsoftware Emotet, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Sonderfall-Emotet/sonderfall-emotet_node.html (abgerufen am 12.04.2021).

44 BSI, Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/Emotet/emotet_node.html (abgerufen am 12.04.2021).

45 *Wellbrock*, Spear Phishing mit Emotet, https://www.psw-group.de/blog/spear-phishing-mit-emotet/6665 (abgerufen am 05.01.2021).

Zahl versendet werden, wird auch von *Dynamit-Phishing* gesprochen.[46] Durch die maßgeschneiderten Inhalte werden Empfänger zum unbedachten Öffnen von schädlichen Dateianhängen oder der in den Nachrichten enthaltenen URLs verleitet. Ist der Computer erst infiziert, laden *Spear-Phishing* Softwares in der Regel weitere Schadsoftware nach, wie z.B. den Banking-Trojaner *Trickbot*. Diese Schadprogramme führen zu Datenabfluss oder ermöglichen den Cyberkriminellen die vollständige Kontrolle über IT-Systeme zu erlangen. In mehreren bekannten Fällen hatte dies große Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden mussten.[47] Im Januar 2021 gelang es einem internationalen Team von Strafverfolgungsbehörden schließlich die Infrastruktur, über die die *Emotet* lief, zu übernehmen und zu zerschlagen, wie das Bundeskriminalamt, welches maßgeblich an der Aktion beteiligt war, bekanntgab.[48] Andere *Spear-Phishing*-Softwares sind nach wie vor aktiv und richten nicht unerhebliche Schäden an.[49]

d. Whaling

Whaling ist eine Methode Cyberkrimineller, bei der sie sich als hochrangige Mitarbeiter in einem Unternehmen ausgeben und unternehmenseigene Führungskräfte oder andere wichtige Personen direkt angreifen, um Geld oder vertrauliche Informationen zu stehlen oder sich für kriminelle Zwecke Zugriff auf ihre Computersysteme zu verschaffen.[50]

Wie beim *Spear-Phishing* wird eine individuell angepasste E-Mail verfasst und zumeist an leitende Mitarbeiter eines Unternehmens gesendet. Die E-Mail soll den Eindruck vermitteln, es handele sich bei dem Absender um einen noch höherrangigen Mitarbeiter. Meist wird hierfür die Identität des jeweiligen CEO, CTO oder CFO vorgetäuscht. Die versendeten E-Mails enthalten oftmals Unternehmenslogos oder Links zu betrügerischen Web-

46 *Schmidt*, Achtung Dynamit Phishing: Gefährliche Trojaner-Welle Emotet legt ganze Unternehmen lahm, https://www.heise.de/security/meldung/Achtung-Dynamit-Phishing-Gefaehrliche-Trojaner-Welle-legt-ganze-Firmen-lahm-4241424.html?view=print (abgerufen am 05.01.2021).

47 BSI, Aktuelle Information zur Schadsoftware Emotet (Fn. 41).

48 BKA, Infrastruktur der Emotet-Schadsoftware zerschlagen (Fn. 41).

49 *Auer*, So erkennen Sie E-Mail-Betrüger, https://www.computerwoche.de/a/so-erkennen-sie-e-mail-betrueger,3549545 (abgerufen am 17.04.2021).

50 https://www.kaspersky.de/resource-center/definitions/what-is-a-whaling-attack (abgerufen am 18.12.2020).

sites, die authentisch erscheinen. Cyber-Kriminelle werten soziale Medien und öffentliche Unternehmensinformationen gezielt aus, um ein Profil und einen Angriffsplan zu erstellen. Außerdem nutzen sie in einigen Fällen *Ransomware* und *Rootkits*[51], um Netzwerke zu infiltrieren. Dadurch können sogar E-Mails vom echten E-Mail-Konto des jeweiligen CEO gesendet werden. Da Führungskräfte bzw. „Wale", auf die derartige Angriffe abzielen, innerhalb des Unternehmens hohes Vertrauen genießen und umfassende Zugriffsrechte haben, lohnt sich der Aufwand für Cyberkriminelle, den Angriff möglichst glaubwürdig zu gestalten. Dadurch kommt ein weiteres Element des Social Engineerings[52] ins Spiel: Mitarbeiter werden in aller Regel nur ungern eine Anfrage von jemandem ablehnen, den sie für wichtig halten. Dies kann erhebliche Folgen haben. So überwies ein Mitarbeiter einer Rohstofffirma aufgrund eines *Whaling*-Angriffs 17,2 Mio. US-Dollar in mehreren Tranchen auf ein Bankkonto in China. Er wurde zuvor in E-Mails, die den Anschein machten, als hätte sie sein CEO geschrieben, zu den Überweisungen aufgefordert. Das Unternehmen plante zu diesem Zeitpunkt, nach China zu expandieren, weshalb die Anfrage ausreichend plausibel wirkte.[53]

2. Cybersecurity in Zeiten der Coronapandemie

Noch kann keine exakte Prognose darüber getroffen werden, inwieweit eine Pandemie, wie wir sie seit Verbreitung von COVID-19 erleben, auch die Sicherheitskonzepte in Unternehmen in Bezug auf Cybersecurity nachhaltig beeinflussen wird. Eine Befragung von Bitdefender aus dem Jahr 2020 liefert dahingehend erste Erkenntnisse. Im Rahmen der Studie wurden über 6700 Information Security Professionals – Fachleute aus dem Be-

---

51 Der Begriff Rootkit beschreibt Schadprogramme, die Computer infizieren und dadurch Cyberkriminellen erlauben, verschiedene Programme darauf zu installieren, die ihnen dauerhaften Zugriff auf die jeweiligen Computer ermöglichen. Vgl. *Malenkowich,* Was ist ein Rootkit?, https://www.kaspersky.de/blog/was-ist-ein-rootkit/853/ (abgerufen am 17.01.2021).

52 Bei dieser Vorgehensweise wird das Opfer dazu gebracht, Daten von sich aus einer ihm unbekannten Person mitzuteilen. Mit den dadurch erlangten Daten werden in der Regel missbräuchliche Zahlungen veranlasst. Eine Manipulation des Rechners des Opfers findet dabei nicht statt.
Vgl. Auer-Reinsdorff/Conrad IT-R-HdB, 3. Aufl. 2019, § 27 E-Payment und E-Invoicing Rn. 14.

53 *Rahmati-Georges*, Was ist ein Whaling-Angriff, https://blog.varonis.de/was-ist-ein-whaling-angriff/ (abgerufen am 06.01.2021).

reich der Informationssicherheit – hinsichtlich ihres Umgangs mit der Coronakrise befragt. Dabei gaben 26 % der befragten „InfoSec Professionals" an, dass *Phishing*- und *Whaling*-Attacken aus ihrer Sicht am stärksten zugenommen hätten. Eine Zunahme von *Ransomware*-Angriffen wurde von 22 % der Befragten wahrgenommen. 67 % der im Rahmen der Studie befragten Führungskräfte gaben an, dass ihre Mitarbeiter kein spezielles Cybersecurity-Training für die Heimarbeit erhalten hätten. Dabei glaubt fast die Hälfte von ihnen (43 %), dass die Häufigkeit und Intensität der Cyber-Attacken weiter zunehmen wird.[54] Dennoch: mehr als die Hälfte der Führungskräfte (55 Prozent) in deutschen Unternehmen nutzt ihre privaten Endgeräte auch im beruflichen Umfeld.[55]

Bereits jetzt kann festgestellt werden, dass Cyberkriminelle durchaus kreativ auf die Pandemiesituation reagieren. So hat das BKA im Laufe des Jahres 2020 Informationen zu mehreren *Phishing*-Kampagnen mit Bezug auf die Pandemie gesammelt. Es existierte beispielsweise über mehrere Wochen eine Website, die sowohl im Design als auch der URL der Website der Investitionsbank Berlin stark ähnelte. Über eine darüber verlinkte *Phishing*-Website konnten die Nutzer ein Online-Formular für die Beantragung von finanziellen Soforthilfen des Landes Berlin für betroffene Unternehmen aufrufen. Ziel dieses Konstrukts dürfte die Erlangung von personen- und unternehmensbezogenen Daten gewesen sein, um damit Folgestraftaten zu begehen.[56] Ähnliche gelagerte Fälle, die mithilfe täuschend echt wirkender E-Mails und Websites verschiedener staatlicher Institutionen in Zusammenhang mit den Soforthilfen des Bundes und der Länder arbeiteten, wurden aus beinahe allen Bundesländern gemeldet.[57]

Laut einer Studie von Unit42, einem Kooperationspartner des European Cybercrime Centers von Europol, sind im Zeitraum Januar bis April 2020 insgesamt 116.357 neu registrierte Domains mit Bezug auf die Pandemie identifiziert worden. Seit dem 12.3.2020 werden täglich ca. 3.000 neue Do-

---

54 vgl. Bitdefender Study "The indelible impact of Covid-19 on Cybersecurity", https://www.bitdefender.com/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf (abgerufen am 24.09.2020).

55 vgl. https://www.crowdstrike.com/blog/securing-a-remote-workforce-in-the-time-of-covid-19/ (abgerufen am 24.09.2020).

56 Bundeskriminalamt, Sonderauswertung, Cybercrime in Zeiten der Coronapandemie, S. 6, Download unter folgendem Link: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html (abgerufen am 04.01.2020).

57 BKA, Sonderauswertung, Cybercrime in Zeiten der Coronapandemie (Fn. 57), S. 7.

mains pro Tag registriert. Unit42 stufte dabei 1,74 % der Domains als eindeutig maliziös und über ein Drittel als hochriskant ein. Die Anzahl der maliziösen bzw. der „Hochrisikodomains" sei im Februar und März 2020 um ca. 569 % bzw. 788 % gestiegen. 16 % dieser Domains würden für *Phishing*-Attacken und 84 % für das Hosten verschiedener *Ransomware* genutzt.[58]

II. Cyberangriffe und -risiken von innen

Den größten Risikofaktor im Bereich von Cyberangriffen auf Unternehmen stellt der einzelne Mitarbeiter selbst dar. Cyberangriffe können in der Regel nur Erfolg haben und Schäden für das Unternehmen nach sich ziehen, wenn ein Mitarbeiter durch eigenes Fehlverhalten ermöglicht, dass der jeweilige Angriff zum Erfolg führt.

1. Disgruntled employees

Ist von Cyberangriffen die Rede, vermutet man zunächst unternehmensfremde Menschen oder Hacker im Staatsauftrag dahinter. Dabei geht laut BSI von Innentätern eine größere Gefahr aus, da ihre Angriffe größere Aussicht auf Erfolg hätten. Angreifer hätten „bereits Zugang zu internen Ressourcen einer Organisation und könnten so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren".[59] Daher können sich Mitarbeiter als ein großes Risiko für Unternehmen erweisen. Ein Drittel der im Rahmen einer Bitkom-Studie zum Wirtschaftsschutz im Jahr 2020 befragten Unternehmen gab an, bei Cyberattacken von früheren Mitarbeitern vorsätzlich geschädigt worden zu sein.[60] Doch nicht nur (Ex-)Mitarbeiter können ihren Unternehmen Probleme bereiten. Auch externe Dienstleister stellen ein Risiko dar, weil diese durch ihre Tätigkeit

58 *Szurdi, Chen u.a.*, Studying how Cybercriminals Prey on the Covid-19 Pandemic, https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/ (abgerufen am 04.01.2020).

59 BSI, Glossar der Cybersicherheit, Innentäter, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 (abgerufen am 28.12.2020).

60 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 26.

teilweise Einfluss oder direkten Zugang zu internen IT-Systemen des Unternehmens haben.[61]

2. *Cyberrisiken durch geteilte Zugriffsrechte und Remote Devices*

a. Zugriffsrechte

Ein weiteres Risiko liegt im Bereich der Zugriffsrechte für Dateien, Ordner und Festplatten. Häufig haben Mitarbeiter, insbesondere in kleinen Unternehmen, zwischen mehreren Arbeitskollegen geteilte Zugriffsrechte auf Daten und Informationen. Gründe hierfür können Kostenvorteile durch geteilte Zugänge bei externen Diensten, Steigerung der Effizienz von Arbeitsprozessen oder schlicht mangelndes Risikobewusstsein sein.[62] In der Praxis hat sich gezeigt, dass Mitarbeiter durch geteilte Zugriffsrechte auf eine Fülle an Daten zugreifen können, die sie für ihre Arbeit oftmals gar nicht benötigen. Dies erhöht das Risiko eines Missbrauchs dieser Daten erheblich.

b. Mobile Endgeräte

Auch mobile Endgeräte und die immer weiter fortschreitende Möglichkeit, von zuhause oder von verschiedenen Orten weltweit arbeiten zu können, spielen im Rahmen von Cyberangriffen von innen eine große Rolle.[63] Auch vor Beginn der Corona-Krise war ein leichter Trend zum Arbeiten im Homeoffice und zu *remote work* erkennbar; durch die Pandemie hat sich dieser Trend erheblich verstärkt.[64] Aufgrund des Infektionsgeschehens am Arbeitsplatz, haben viele Unternehmen die Notwen-

---

61 BSI, Glossar der Cybersicherheit, Innentäter (Fn. 59).

62 Voitiz, The Comodo Breach and the Dangers of Shared Accounts, https://dzone.com/articles/the-comodo-breach-and-the-dangers-of-shared-accoun (abgerufen am 18.04.2021).

63 BSI, Mindeststandard des BSI für Mobile Device Management, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mobile_Device_Management/Mobile_Device_Management_node.html (abgerufen am 19.04.2021).

64 *Rosenbach/Börsch*, Covid-19-Briefing: HomeOffice-Trends vor, während und nach Corona, https://www2.deloitte.com/de/de/blog/covid-19-briefings/2020/covid-19-briefing-homeoffice-trends-corona.html (abgerufen am 07.01.2021).

digkeit erkannt und zunehmend Maßnahmen ergriffen, um Homeoffice oder *remote work* zu ermöglichen. Um die kurzfristige Arbeitsfähigkeit des Unternehmens aufrechtzuerhalten, wurden dabei Sofortmaßnahmen vieler Unternehmen größtenteils ohne konzeptionelle Vorbereitungsmaßnahmen umgesetzt. Dass dies Sicherheitsrisiken mit sich bringt, ist dabei wenig überraschend. Je flexibler die Mitarbeiter hinsichtlich des Arbeitsortes sind, desto mehr Möglichkeiten für Missbrauch und Sicherheitslücken entstehen. Denn im Homeoffice sind Daten und IT-Technik der unmittelbaren Kontrolle des Arbeitgebers entzogen. Gleichzeitig steigt die Gefahr unberechtigter Zugriffe durch Dritte, etwa durch die Nutzung öffentlicher W-Lan-Netzwerke im Café um die Ecke oder im Co-Working-Space.[65]

B. Lösungsansätze und Präventionsstrategien

Um die zuvor genannten Risiken so gut es geht einzudämmen und als Unternehmen vorbereitet zu sein, empfehlen sich verschiedene Vorgehensweisen und Präventionsstrategien. Für die Geschäftsführung von Unternehmen ist es dabei unabdingbar, Maßnahmen zur Gewährleistung sicherer IT-Systeme zu ergreifen. Bei einer allzu stiefmütterlichen Behandlung der Cybersecurity begibt sich die Geschäftsführung in ein immanentes Haftungsrisiko, da sie von Dritten für die wirtschaftlichen Folgen eines Cyberangriffs in Anspruch genommen werden kann.[66] Gemäß § 93 AktG und § 43 I GmbHG haben die Vorstandsmitglieder und Geschäftsführer eines Unternehmens in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsleiters bzw. -mannes anzuwenden. Zu diesem Pflichtenmaßstab zählt dabei auch die Einhaltung der in der DSGVO festgelegten Pflichten, so auch die in Art. 32 DSGVO verankerte Pflicht, zum Schutz der Daten angemessene technische und organisatorische Maßnahmen zu treffen. In diesem Zusammenhang wird die Gewährleistung eines einheitlichen Sicherheitskonzepts die zentrale Herausforderung der Geschäftsleitungen sein.

In der Praxis hat sich gezeigt, dass für eine erfolgreiche Einführung eines Sicherheitskonzepts an erster Stelle eine klare Definition der Verantwortlichkeiten für das Thema Cybersecurity im jeweiligen Unternehmen

---

65 *Schonschek*, Home Office fordert die Cybersecurity, https://www.computerwoche.de/a/home-office-fordert-die-cybersecurity,3549013 (abgerufen am 19.04.2021).

66 *Schmidt-Versteyl*, Cyber Risk – neuer Brennpunkt Managerhaftung?, NJW 2019, 1637, 1642.

entscheidend ist. Diese Zuständigkeit dürfte in den meisten kleinen und mittelständischen Unternehmen aufgrund der – wie oben beschrieben – oftmals unzureichenden Auseinandersetzung mit dem Thema Cybersecurity noch nicht abschließend geregelt sein. Es ist durchaus häufig zu beobachten, dass bereits mehrere Mitarbeiter für wichtige Einzelthemen aus dem Bereich Cybersecurity zuständig sind. An einer gebündelten ausschließlichen Verantwortlichkeit eines Mitarbeiters oder einer Abteilung für sämtliche IT-Sicherheitsfragen fehlt es jedoch zumeist. In mittelständischen Unternehmen könnte dabei einerseits die Rechtsabteilung und andererseits die IT-Abteilung ein Interesse daran haben, dass Maßnahmen im Bereich Cybersecurity getroffen und vor allem umgesetzt und eingehalten werden. Hier zeigt sich regelmäßig, dass Schwierigkeiten hinsichtlich der Abstimmung und der Arbeitsteilung entstehen können. Es empfiehlt sich, in Unternehmen eine Schnittstelle zwischen den Bereichen IT, Recht und Entwicklung zu bilden, die für die Entscheidungsprozesse bezogen auf die Datensicherheit zuständig ist. Denkbar ist auch die Gründung eines kleinen Teams, welches diese Aufgaben übernimmt. Entscheidend ist, dass die Kompetenzen gebündelt werden und, dass es mindestens einen Ansprechpartner gibt, der ausschließlich für den Bereich der Cybersecurity verantwortlich ist und die Entwicklungen des Unternehmens sowie die aktuelle Rechtslage im Blick behält.

Unternehmen sollten sich zudem die Frage stellen, welche Daten sensibel und somit besonders schützenswert sind und vor welchen Angriffen sie geschützt werden sollen.

Sind diese ersten Schritte vollzogen, sollte der Fokus daraufgelegt werden, einen soliden Schutz gegen die jeweiligen unternehmensspezifischen Risiken zu entwickeln.

I. Lösungsansätze für Risiken von außen

Insbesondere Tech-Unternehmen wie Vimcar sehen sich mit vielen Risiken von außen konfrontiert. Je mehr ein Unternehmen mit Software und digitalen Daten arbeitet, desto höher sind die Anforderungen an die technischen und organisatorischen Maßnahmen, die im gesamten Unternehmen implementiert und im Anschluss fortlaufend und konsequent umgesetzt werden sollten.

1. Prävention gegen Ransomware

Software wie Betriebssysteme, Antivirenprogramme und Browser, sowie darin enthaltene Plug-ins, sollten stets auf dem aktuellen Stand sein, um Sicherheitslücken vorzubeugen.[67] Dazu können Mitarbeiter regelmäßig erinnert werden, Updates zu installieren. In der Praxis hat sich die Nutzung einer Patch-Management-Software, die auf den Unternehmensrechnern installierte Software beständig auf Aktualität überprüft und an Updates erinnert, bewährt. Diese kann auch so konfiguriert werden, dass wichtige Updates automatisch installiert werden.

Es empfiehlt sich außerdem ein vom System abgetrenntes Backup einzurichten und regelmäßig zu aktualisieren.[68] Dies dient als Vorbereitung für den Schadensfall. Durch das Backup können betrieblichen Daten gesichert werden. Dadurch kann die oben beschriebene Bredouille in Hinblick auf etwaige Lösegeldzahlungen im besten Falle vermieden und möglichst bald zum Tagesgeschäft zurückgekehrt werden. Im Fall von Tech-Unternehmen, deren Fokus auf der Verarbeitung von Daten liegt, empfiehlt es sich, eine komplette Spiegelung des Hauptservers vorzunehmen.

Vimcar spiegelt beispielsweise sämtliche Daten in Echtzeit. Die Spiegelung erfolgt auf mindestens zwei völlig voneinander unabhängigen Servern in geografisch getrennten Rechenzentren in Frankfurt am Main. Für den Fall, dass bei einem Server Probleme auftreten, schaltet das System sofort auf einen der anderen Server um. Die Funktionalität dieser Spiegelung wird kontinuierlich überwacht und einmal im Quartal manuell überprüft. Von allen Servern werden täglich Backups erstellt. Die manuelle Wiederherstellung dieser Backups wird einmal im Quartal von Vimcar geprüft. Im Rahmen der Prüfung wird mit jeweils einem Backup ein Test durchgeführt, der den unwahrscheinlichen und zeitgleichen Ausfall aller redundant betriebenen Server nachstellt.

Da *Ransomware* in den meisten Fällen durch Anhänge von E-Mails auf Unternehmensrechner und -systeme eingeschleust wird[69], gelten die folgenden Ausführungen zum *Phishing* auch zur Prävention gegen *Ransomware*.

---

67 BSI, Ransomware: Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25), S. 15.
68 BSI, Ransomware: Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25), S. 11.
69 BSI, Ransomware, erpresserische Schadprogramme, https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Ransomware.html (abgerufen am 09.01.2021).

2. Prävention gegen Phishing

Phishing-Attacken sind in aller Regel aufgrund von Unachtsamkeit oder mangelnder Vorbereitung der Mitarbeiter auf derartige Angriffe erfolgreich.[70] Daher ist es beinahe unerlässlich, Mitarbeiter für den Umgang mit *Phishing*-Attacken zu sensibilisieren. Hierzu können externe Experten für unternehmensweite Workshops engagiert werden. Alternativ können Mitarbeiter durch digitale *Phishing*-Trainings geschult werden. Einige digitale Anbieter auf dem Markt haben sich darauf spezialisiert, die notwendige Sensibilität der Mitarbeiter im Umgang mit *Phishing*-E-Mails zu trainieren. Teilweise bieten diese Anbieter darüber hinaus Tools zur *Phishing*-Simulation an. Zur Durchführung der *Phishing*-Simulation wird den Anbietern durch das jeweilige Unternehmen in der Regel zunächst eine Liste von Mitarbeitern und deren E-Mail-Adressen zur Verfügung gestellt. Der Anbieter simuliert im Anschluss mögliche *Phishing*-Attacken im Unternehmen, indem er den Mitarbeitern in unregelmäßigen Abständen Test-E-Mails zukommen lässt, ohne dass die Mitarbeiter darauf vorbereitet werden. Diese Test-E-Mails orientieren sich in Design und Inhalt an tatsächlich existenten *Phishing*-Mails. Sie können jedoch keinen Schaden anrichten, sondern dienen lediglich dazu, Sicherheitslücken ausfindig zu machen und unvorsichtige Mitarbeiter zu sensibilisieren. Sollten Mitarbeiter die Test-E-Mails und deren Anhänge öffnen, wird der jeweilige Administrator des Tools entweder vom Anbieter darüber informiert, oder er kann dies jeweils anhand eines Dashboards verfolgen. Ziel ist es, einen Überblick über den Umgang der Mitarbeiter mit solchen E-Mails zu erhalten.

Vimcar arbeitet beispielsweise zur *Phishing*-Prävention mit einem Anbieter, der im Rahmen seines cloudbasierten Services eine Mischung aus digitalen Mitarbeitertrainings und Phishing-Simulationen bietet. Sobald ein Mitarbeiter eine der simulierten *Phishing*-Mails oder deren Anhänge öffnet oder vertrauliche Daten auf einer gefälschten Login-Website angibt, gelangt er zu einer Lernseite. Diese bietet dann individuelle Hinweise und Tipps, die bei der Vermeidung solcher Fehler helfen. Dieses System funktioniert anonym und über das Jahr verteilt, sodass alle Mitarbeiter eine kontinuierliche Schulung erhalten. Der Anbieter stellt außerdem ein Dashboard mit allen wichtigen Kennzahlen und Statistiken zur Verfügung.

70 *Nollau*, Eigene Mitarbeiter sind größte Security-Schwachstelle, https://www.it-business.de/eigene-mitarbeiter-sind-groesste-security-schwachstelle-a-732202/ (abgerufen am 17.04.2021).

Dadurch können sich die für Cybersecurity zuständigen Mitarbeiter zügig einen Überblick über die bei den Mitarbeitern aktuell vorhandene Sensibilität im Umgang mit *Phishing*-Mails verschaffen.

Außerdem hat sich in der Praxis bewährt, Mitarbeiter dahingehend zu verpflichten, sich auf allen beruflich genutzten Endgeräten Dateierweiterungen, wie z.B. „.doc“ oder „.xls“, vollständig anzeigen zu lassen. Diese Dateierweiterungen werden von den gängigen Betriebssystemen ausgeblendet. Diese Tatsache nutzen Cyberkriminelle gezielt aus. Die Anzeige dieser Dateierweiterungen bewirkt eine weitaus bessere Erkennbarkeit von verdächtigen Dateien. Wenn beispielsweise der Anhang einer Bewerbungsmail anstatt “LebenslaufPDF” als “LebenslaufPDF.exe” angezeigt wird, ist schnell erkennbar, dass es sich nicht um einen echten Lebenslauf im PDF-Format handelt, sondern vermutlich um eine Schadsoftware. Die Anzeige der Dateierweiterung ist ein einfacher und kostenloser Weg, um *Phishing*-Risiken gezielt zu minimieren. Empfehlenswert ist außerdem die Implementierung einer Meldekette für potenzielle *Phishing*-Mails. Sie kann als Warnsystem fungieren, durch das alle Mitarbeiter für den Fall alarmiert werden, dass ein Mitarbeiter eine solche E-Mail erhalten hat.

3. Prävention gegen Whaling

Für eine erfolgreiche Prävention vor *Whaling*-Attacken als spezielle Form des *Phishings* sollten zunächst die oben genannten Grundsätze zur Sensibilisierung von Mitarbeitern vor *Phishing*-Attacken umgesetzt werden.

Außerdem hat es sich in der Praxis bewährt, alle E-Mails, die von Absendern außerhalb des Unternehmens stammen, zu kennzeichnen. So können Whaling-E-Mails, die oberflächlich betrachtet wie die einer unternehmensinternen Führungskraft aussehen, auf den ersten Blick erkannt werden.

4. Passwörter und Passwortmanager

Ein entscheidender Faktor im Rahmen der erfolgreichen Verhinderung von Cyberangriffen stellt die Verwendung sicherer Passwörter dar.[71] Cyberkriminelle haben Tools entwickelt, die vollautomatisch eine Vielzahl

71 *Dirscherl*, BSI gibt Tipps für sichere Passwörter, https://www.pcwelt.de/ratgeber/Datenschutz-BSI-gibt-Tipps-fuer-sichere-Passwoerter-1452884.html (abgerufen am 17.04.2021).

von Zeichenkombinationen ausprobieren können. Dabei werden ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen getestet oder einmal im Internet veröffentlichte Zugangsdaten bei diversen anderen Diensten durchprobiert.[72] Um zu verhindern, dass sich Cyberkriminelle so Zugang zu Unternehmenssystemen verschaffen, sollten Passwörter gängige Qualitätsanforderungen[73] erfüllen und jeweils nur für einen Zugang genutzt werden. Dabei ist regelmäßig die Länge eines Passwortes wichtiger als die Kombination aus Groß- und Kleinbuchstaben sowie Sonderzeichen. Je länger das Passwort, desto länger braucht ein computergestützter Algorithmus im Rahmen eines Cyberangriffs, um dieses zu knacken.

In der Praxis hat sich die Verwendung eines Passwortmanagers als nützlich erwiesen. Dies gilt insbesondere dann, wenn Mitarbeiter eine Vielzahl an Tools und Zugängen nutzen. Passwortmanager sind Programme, die Passwörter und vertrauliche Informationen verwalten.[74] Die Nutzer können verschiedene Passwörter, Softwarelizenzen und weitere sensible Daten in einem virtuellen „Tresor" speichern, der nur durch die Eingabe eines Hauptkennwortes zugänglich ist.[75] Das Hauptkennwort dient dabei als Sicherheitsschlüssel für die im „Tresor" gespeicherten Informationen. Die meisten gängigen Passwortmanager akzeptieren nur Hauptkennwörter, die den Vorgaben an sichere Passwörter entsprechen. Es wird empfohlen, die Hauptkennwörter besonders lang und mit besonders vielen Sonderzeichen zu versehen. In dem Fall kann der jeweilige Nutzer zwar kein simples Passwort wie z.B. „123456" nutzen, welches seit Jahren das beliebteste Passwort in Deutschland ist.[76] Dafür muss er sich lediglich ein Passwort merken.

---

72 BSI, Empfehlungen: Sichere Passwörter erstellen, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (abgerufen am 10.01.2021).

73 Vgl. die jeweils aktuellen Vorgaben im IT-Grundschutzkompendium des BSI; BSI IT-Grundschutzkompendium 2021, Download unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (abgerufen am 19.04.2021).

74 BSI, Passwörter verwalten mit dem Passwort-Manager, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html (abgerufen am 19.04.2021).

75 BSI, Empfehlungen: Sichere Passwörter erstellen (Fn. 74).

76 *Micijewic*, die beliebtesten Passwörter der Deutschen sind auch dieses Jahr die unsichersten, https://www.handelsblatt.com/technik/it-internet/it-sicherheit-di

Selbstverständlich ist auch die Nutzung von Passwortmanagern nicht vollkommen risikolos. Passwortmanager können selbst Opfer von Cyberangriffen werden. Außerdem ist bei der Nutzung eines cloudbasierten externen Dienstleisters zu bedenken, dass dieser theoretisch Zugang zu vertraulichen Informationen des jeweiligen Nutzers erhält. Deshalb sollte der jeweilige Anbieter sorgfältig überprüft werden. Dabei sollte insbesondere auf die AGB, die Datenschutzerklärung, die technischen und organisatorischen Maßnahmen und die Verschlüsselung der Passwörter geachtet werden.

Vimcar verwendet beispielsweise ein Passwortmanager-Tool, welches die Zugangsdaten und Passwörter grundsätzlich anhand einer AES-256-Bit-Verschlüsselung Ende-zu-Ende verschlüsselt. Bei dieser Verschlüsselungsmethode besitzt ausschließlich der jeweilige Nutzer den Schlüssel. Daher kann auch der Anbieter selbst nicht auf die gespeicherten Zugangsdaten und Passwörter zugreifen. Zur Einrichtung des Tools installiert der Nutzer auf seinem Rechner ein Programm bzw. ein Browser Plug-in. Um an die gespeicherten Daten heranzukommen, muss der Nutzer das Hauptkennwort eingeben. Das Tool enthält außerdem einen integrierten Passwortgenerator. Dieser ermöglicht es, spezifische Anforderungen an die verwendeten Passwörter zu stellen, wie z.B. Länge, Anzahl der Sonderzeichen etc. Somit können sichere Passwörter automatisch generiert und über das Tool gespeichert werden.

5. Zwei-Faktor-Authentisierung

Neben dem Verwenden sicherer Passwörter ist der Einsatz eines zweiten Authentisierungsfaktors ein sinnvoller Schutz gegen Cyberangriffe von außen. Bereits in vielen Bereichen elektronischer Geschäftsprozesse ist eine solche sichere Authentisierung erforderlich. Spätestens seit der verpflichtenden Verwendung der Zwei-Faktor-Authentisierung für das Online-Banking aufgrund der PSD2 Richtlinie der EU sollte dieses Verfahren beinahe jedem Bürger bekannt sein. Bei der Zwei-Faktor-Authentisierung kommt zu einem ersten Faktor in Form eines Passworts ein zweiter Faktor hinzu, der einer weiteren Kategorie und einem weiteren Endgerät zuzuordnen ist,

---

e-beliebtesten-deutschen-passwoerter-sind-auch-dieses-jahr-die-unsichersten/25347562.html?ticket=ST-1331496-v5t7mOPREcB6UtbWLiLT-ap6 (abgerufen am 10.01.2021).

wie z.B. das Generieren einer TAN mithilfe eines Mobiltelefons.[77] Dieser Identitätsnachweis eines Nutzers mittels der Kombination zweier unabhängiger Komponenten wird insbesondere vom BSI in seinen IT-Grundschutz-Kompendium empfohlen.[78] Entscheidend für die Implementierung einer Zwei-Faktor-Authentisierung ist, ob das jeweilige System eine solche überhaupt unterstützt und wer der jeweilige Administrator des Systems ist.

6. Firewall und Antivirenprogramme

Zur Absicherung der eigenen Netzwerkinfrastrukturen in Unternehmen ist die Verwendung einer gut konfigurierten Firewall unerlässlich.[79] Ergänzend sollte auf jedem Endgerät eine Antiviren-Software installiert und regelmäßig aktualisiert werden.[80] Diese Vorkehrungen gelten als unbedingte Grundausstattung und wurden von der überwiegenden Anzahl der kleinen und mittleren Unternehmen inzwischen umgesetzt.[81]

7. Haftung und Cyberversicherungen

Cyberangriffe weisen ein enormes Potenzial auf, Schäden in den Unternehmen zu verursachen. Gleichzeitig sind die Fragen der Haftung nicht abschließend geklärt.[82] Zwar haften die Unternehmen bei erfolgreichen Cyberangriffen grundsätzlich sowohl für eigene substanzielle Schäden als

---

77 BSI, Empfehlungen: Sichere Passwörter erstellen (Fn. 74).

78 BSI, IT-Grundschutz-Kompendium 2020, S. 11, Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html (abgerufen am 10.01.2021).

79 BSI, Schutz vor dem Angriff von außen, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Firewall/firewall_node.html (abgerufen am 19.04.2021).

80 BSI, Virenschutz und falsche Antivirensoftware, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html (abgerufen am 20.04.2021).

81 *Hildebrandt/Niederprüm u.a.*, WIK Report, Aktuelle Lage der IT-Sicherheit in KMU, S. 28, https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?__blob=publicationFile&v=3 (abgerufen am 04.01.20219).

82 *Mehrbrey/Schreibauer*, MMR 2016, 75, 75.

auch für Schäden, die ihre Kunden und Dienstleister erleiden, selbst.[83] Jedoch wird das angegriffene Unternehmen in einigen Fällen versuchen, Dritte wie z.B. externe Dienstleister in Anspruch zu nehmen und eigene Ansprüche durchzusetzen. Das Abschließen einer sog. Cyberversicherung wird vor diesem Hintergrund für Unternehmen im Rahmen ihres Risikomanagements immer wichtiger werden. Eine solche Versicherung trägt dem Umstand Rechnung, dass übliche Versicherungen meist einen unzureichenden Schutz gegen Schäden bieten, die durch Cyberangriffe entstehen. Eine Cyberversicherung bietet dem Versicherten dabei die Möglichkeit, Eigen- und Drittschäden im Zusammenhang mit Cyberangriffen und Cyberkriminalität zu versichern. In den letzten Jahren hat sich das Angebot solcher Versicherungen stetig weiterentwickelt. Die Cyberversicherungen erstatten dabei, je nach individuell vereinbartem Versicherungsschutz, Kosten im Rahmen der Wiederherstellung von Daten und IT-Systemen, Kosten infolge eines Betriebsausfalls bzw. einer Betriebsunterbrechung sowie für die Inanspruchnahme spezialisierter Rechtsanwälte. Optional können zusätzlich Fremdschäden – zumeist in Form von Schadensersatzforderungen von Geschäftspartnern und Kunden – versichert werden.[84] Eine mögliche Orientierungshilfe geben die im April 2017 veröffentlichten Musterbedingungen für Cyberversicherungen des Gesamtverbands der Deutschen Versicherungswirtschaft.[85] Diese legen einen Versicherungsschutz für Vermögensschäden fest, die durch eine „Informationssicherheitsverletzung" entstanden sind. Der Umfang des Versicherungsschutzes ist dabei vom Verständnis der Bezeichnung des „informationsverarbeitenden Systems" abhängig.[86] Darunter dürften alle Systeme fallen, die infolge eines Angriffs infiziert werden können, wie z.B. die Unternehmensserver.[87] Allerdings ist vor Abschluss eines Versicherungsvertrages zu beachten, dass in den Versicherungsbedingungen häufig Haftungsausschlüsse für den Fall enthalten sind, dass die Absicherung der Unternehmensnetzwerke und -systeme nicht dem Stand der Technik entspricht.[88] Des Weite-

83 Mehrbrey/Schreibauer (Fn. 82), Rn. 80 ff.

84 *Fortmann*, r+s 2019, 429, 432.

85 Vgl. GDV, Allgemeine Versicherungsbedingungen Cyberversicherung 2017, https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf (abgerufen am 09.09.2020).

86 GDV, Allgemeine Versicherungsbedingungen Cyberversicherung 2017 (Fn. 89), S. 6, Ziff. A1–2.1.

87 *Malek/Schütz*, r + s 2019, 421, 422.

88 BSI, Ransomware Bedrohungslage, Prävention und Reaktion 2019 (Fn. 25).

ren sollten Unternehmen, die eine Cyberversicherungen abschließen wollen, die gängigen Sicherheitsvorschriften, die bspw. in der DSGVO, dem BDSG und weiteren branchenspezifischen Gesetzen, wie dem TKG, enthalten sind, beachten. Die Bedingungen der Cyberversicherungen sind in der Regel so formuliert, dass Verstöße gegen diese Sicherheitsvorschriften ebenfalls zu einem Haftungsausschluss für die jeweilige Versicherungsgesellschaft führen.[89] Allgemein lässt sich unter deutschen Unternehmen ein Trend zum Abschluss von Cyberversicherungen erkennen. Allerdings sind große Unternehmen bisher dabei etwa doppelt so häufig gegen Cyberrisiken versichert, als kleine und mittlere Unternehmen.[90]

II. Lösungsansätze für Risiken von innen

1. Mitarbeiterschulungen und -sensibilisierungen

Laut einer Bitkom-Studie zum Wirtschaftsschutz aus dem Jahr 2020 waren es bisher gerade die aufmerksamen und gut geschulten Mitarbeiter des eigenen Unternehmens, die Cyberangriffe erkannt und damit zu ihrer Aufdeckung beigetragen haben.[91]

Neben Schulungen zum Datenschutz, die bereits häufig in Unternehmen durchgeführt werden, haben sich in der Praxis Schulungen zum Thema Datensicherheit als hilfreich erwiesen. Die Mitarbeiter sollten in diesem Rahmen hinsichtlich des Umgangs mit Hardware und der Ablage und Speicherung von Daten sensibilisiert werden. Dabei spielt neben der Sensibilisierung zur regelmäßigen Durchführung von Updates der Antivirensoftware außerdem die Vorsicht bei Downloads von Dateien von Websites oder als Anhänge von E-Mails eine große Rolle.

Unternehmen müssen für solche Schulungen nicht zwangsweise teure externe Experten beauftragen. Oftmals können die Schulungen in Form von kostengünstigen Online-Trainings erfolgen. Auch diese Online-Trainings können einen erheblichen Beitrag dazu leisten, Risiken aus den Reihen der eigenen Mitarbeiter zu verringern. Die Mitarbeiterschulungen sollten, aufgrund der stetig verbesserten und neu entwickelten Vorgehens-

89 *Fortmann* (Fn. 84), Rn. 437.

90 *Krößmann/Artz*, Industrie setzt zunehmend auf Cyberversicherungen, https://www.bitkom.org/Presse/Presseinformation/Industrie-setzt-zunehmend-auf-Cyberversicherungen.html (abgerufen am 11.01.2021).

91 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 29.

weisen der Cyberkriminellen, mindestens jährlich stattfinden. Idealerweise sollten derartige Schulungen als Teil des „Onboardings" neuer Mitarbeiter implementiert werden, damit diese Mitarbeiter bereits bei Beginn ihrer Tätigkeit für drohende Gefahren im Bereich der Cyberkriminalität sensibilisiert werden. Online-Schulungen bieten zudem den Vorteil, dass sie jederzeit verfügbar sind und von Mitarbeitern daher genutzt werden können, wenn gerade Zeit zur Verfügung steht. So kann die Bindung aller Ressourcen über Stunden oder gar Tage vermieden werden, was in einigen Unternehmen einem Betriebsstillstand nahekommen kann. Des Weiteren enthalten einige Online-Schulungen Abschlusstests, um zu gewährleisten, dass die Inhalte der Schulungen tatsächlich bei den Mitarbeitern angekommen sind.

2. Clean-Desk-Policy

Die Clean-Desk-Policy gibt vor, dass alle Arbeitsplätze bei deren Verlassen aufgeräumt und frei von Arbeitsmitteln hinterlassen werden müssen.[92] Die Einführung einer solchen Policy hat sich in der Praxis als sinnvoll erwiesen. Dies gilt umso mehr, als viele Unternehmen zunehmend Homeoffice-Regelungen einführen und Mitarbeiter häufig wechselnde Arbeitsplätze innerhalb eines Büros besetzen. Die Clean-Desk-Policy kann entweder bereits im Arbeitsvertrag enthalten oder als Büro-Richtlinie ausgestaltet sein.

3. Weitere Policies

Weitere Policies können dazu beitragen, Mitarbeiter zu sensibilisieren, beispielsweise dahingehend, dass betriebliche Systeme, wie z.B. E-Mail-Konten nicht für private Zwecke genutzt werden dürfen. Die Ausgestaltung der Policies hängt dabei maßgeblich von der konkreten Arbeitsumgebung eines Unternehmens ab. In größeren Unternehmen kann es sinnvoll sein, spezifische Policies für die einzelnen Abteilungen zu entwickeln, die ihre jeweiligen Besonderheiten widerspiegeln.

Vimcar hat beispielsweise eine sog. Private-Use-Policy hinsichtlich der verwendeten Systeme implementiert. Dabei werden die Mitarbeiter angehalten, keine private Kommunikation über Unternehmenssysteme zu

92 *Pletke/Schrader* u.a., Rechtshandbuch Flexible Arbeit, 1. Aufl. 2017, B. Dimensionen der Flexibilisierung, Rn. 1040.

führen, keine privaten Daten auf der Hardware des Unternehmens zu speichern sowie keine privaten Informationen im elektronischen Terminkalender einzutragen. Diese Policy ermöglicht es Vimcar, bei Ausscheiden eines Mitarbeiters, die genutzten Accounts zu löschen bzw. an aktive Mitarbeiter zu übergeben. Bei der Übergabe der Accounts muss der neue Nutzer die Zugangsdaten ändern, um einen etwaigen Zugriff ausgeschiedener Mitarbeiter zu verhindern. Bleiben Zugriffsrechte bestehen, steigt die Gefahr, dass ein verärgerter Ex-Mitarbeiter unternehmenskritische Daten stiehlt oder vernichtet. Im Rahmen der Private Use Policy werden die Mitarbeiter auch hinsichtlich des Teilens und Freigebens von Dateien dahingehend sensibilisiert, Verantwortung für die eigenen Dokumente zu übernehmen.

Policies erfüllen allerdings nur ihren Zweck, wenn sich die Mitarbeiter an sie halten. Von Unternehmensseite her gibt es kaum Kontroll- oder Regulierungsmöglichkeiten um zu überprüfen, ob Mitarbeiter den Policies Folge leisten. Die Policies dienen vielmehr als Richtlinien bzw. Empfehlungen, die naturgemäß das Risiko mit sich bringen, nicht beachtet zu werden. Hier ist die Kette nur „so stark wie das schwächste Glied", da bereits im Falle, dass sich ein einzelner Mitarbeiter nicht an die jeweilige Policy hält, potenziell große Schäden eintreten können. Deshalb sollten zumindest stichprobenhafte Kontrollen hinsichtlich der Beachtung der Policies erfolgen, um Mitarbeiter bei Nichtbeachtung der Policies erneut auf deren Geltung aufmerksam machen zu können.

4. Zugriffsrechte

Der Grundsatz der *Least Privileges* ist die wichtigste Regel zur Vergabe von Benutzerrechten. Sie beinhaltet, dass Mitarbeiter genau die Rechte bekommt, die sie für die Erfüllung ihrer Arbeit unbedingt benötigen. Es geht weniger darum, die Rechte einzelner Mitarbeiter zu beschneiden, vielmehr stellt der Grundsatz sicher, dass vertrauliche Daten auch vertraulich bleiben.[93]

Bei Vimcar können Mitarbeiter beispielsweise grundsätzlich nicht auf Kundendaten zugreifen, vielmehr werden für jeden einzelnen Mitarbeiter spezifische bedarfsgerechte Zugriffsrechte festgelegt. Auch für externe Tools benötigt ein Mitarbeiter eigens zugewiesene Zugriffsrechte, um z.B.

93 BSI, Missbrauch von Berechtigungen, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_32_Missbrauch_von_Berechtigungen.html (abgerufen am 13.01.2021).

überhaupt Kundendaten abrufen zu können. Grundsätzlich sind die Zugriffsrechte in Leserechte und Adminrechte zu unterteilen. Leserechte besitzen z.B. Mitarbeiter des First-Level-Kundensupports, um Kunden und deren Daten im System finden zu können und ihnen Unterstützung bei der Nutzung der Vimcar Produkte zu bieten. Adminrechte (Schreiberechte) besitzen beispielsweise ausgewählte Mitarbeiter der Operations-Abteilung, um Kontaktdaten oder Vertragsdetails von Kunden für den Fall einer Änderung dieser Daten im System bearbeiten zu können.

5. Equipment

Ein zunehmend wichtigeres Thema ist zudem die Gewährleistung von Datensicherheit bei der Nutzung mobiler Endgeräte und Hardware. Vimcar führt z.B. eine Liste darüber, welchem Mitarbeiter welches Equipment wann zur Verfügung gestellt wurde. Die Geräte sind mit Identifikationsnummern versehen. Grundsätzlich sollte bei Beendigung eines Arbeitsverhältnisses darauf geachtet werden, dass die erhaltene Hardware bis zum Ende der Tätigkeit zurückzugeben wird, damit Zugriffe auf Daten und Systeme nach Beendigung des Arbeitsverhältnisses unterbunden werden können.

C. Fazit

Die Relevanz des Bereichs der Cybersecurity für die fortlaufende, störungsfreie Unternehmertätigkeit wird auch den kleinen und mittleren Unternehmen zunehmend bewusst. Dieser Prozess beschleunigt sich aufgrund der digitalen Abbildung einzelner Unternehmensprozesse, aber auch wegen der pandemiebedingten Umstellung auf Home-Office-Lösungen. Allerdings verfügen eine nicht zu vernachlässigende Anzahl an Unternehmen nach wie vor nicht über eine hinreichend funktionsfähige IT-Infrastruktur und umfassende Sicherheitskonzepte.

Für alle Unternehmen gilt gleichermaßen, dass Cybersecurity kein Thema ist, das einmal erledigt wird und danach keines Einsatzes mehr bedarf. Vielmehr ist abzusehen, dass auf dem Gebiet der Datensicherheit kontinuierliche Entwicklungen bevorstehen werden. Da Cyberkriminelle unermüdlich neue Methoden entwickeln, um Sicherheitslücken auszunutzen, gleicht es einem Katz-und-Maus-Spiel, den neuen Methoden standzuhalten. Insbesondere die Geschäftsleitungen von Unternehmen sind dazu

angehalten, ein größeres Augenmerk auf das Thema Cybersecurity zu legen. Die Aspekte der Cybersecurity müssen dabei stets mit der Praktikabilität innerhalb des Unternehmens und den notwendigen Innovationen auf dem jeweiligen Markt abgewogen werden. Dies stellt einen schwierigen Balanceakt dar, denn ohne ein innovatives Produkt ist ein Unternehmen am Markt nicht attraktiv. Allerdings kann eine öffentlichkeitswirksame Cyberattacke, die aufgrund von unzureichenden Präventionsmaßnahmen erfolgreich ist, ein ebenso unkontrollierbares unternehmerisches Risiko darstellen. Im Rahmen einer Studie gaben vier von fünf Managern von 108 befragten deutschen Unternehmen mit mindestens einer Milliarde Dollar Jahresumsatz zu, neue Technologien einzusetzen, noch bevor die notwendigen Sicherheitskonzepte angepasst seien.[94] Dies dürfte sich für junge, wachstumsorientierte Unternehmen nicht anders darstellen. Daher sollte frühzeitig eine Risikoanalyse vorgenommen und Schritte eingeleitet werden, die dem jeweiligen Unternehmen nach einer erfolgten Abwägung im Einzelfall finanziell zumutbar sind. Dies gilt nicht nur aufgrund des Umstands, dass sich die Anzahl der Cyberangriffe auf kleine und mittelständische Unternehmen kontinuierlich erhöht.[95] Vielmehr bieten sich Unternehmen bei frühzeitiger Auseinandersetzung mit dem Thema Cybersecurity und der Implementierung von Sicherheitsstandards perspektivisch Kostensparpotenziale. Denn eine Implementierung solcher Standards erweist sich meist als aufwendiger, wenn die Unternehmensstrukturen bereits gefestigt sind. Zudem führt beinahe jeder zweite Cyberangriff, der in der Zwischenzeit erfolgen kann, zu Produktions- bzw. Betriebsausfällen.[96] Ungeachtet aller zu empfehlenden Maßnahmen bleibt der Mensch und somit der Mitarbeiter weiterhin der größte Risikofaktor, welchem nur mit regelmäßig wiederkehrenden Schulungen und Sensibilisierungen begegnet werden kann. Ein erfolgreicher Umgang mit Cybersecurity kann letztlich nur funktionieren, wenn mehrere Akteure innerhalb eines Unternehmens erfolgreich zusammenarbeiten und insbesondere die Geschäftsleitung, die IT- und Rechtsabteilung sowie die Belegschaft am selben Strang ziehen.

94 *Abbosh/Bissel* (Fn. 1), S. 7.

95 Bitkom-Studie Wirtschaftsschutz 2020 (Fn. 4), S. 7.

96 BSI, Cyber-Angriffe haben erhebliche Konsequenzen für die Wirtschaft, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriffe_haben_erhebliche_Konsequenzen_fuer_die_Wirtschaft_31012018.html (abgerufen am 17.01.2021).

Verzeichnis der Autoren und Herausgeber

Andreas Beyer
Syndikusrechtsanwalt, Vimcar GmbH

Marc-Philipp Bittner, LL.B.
Rechtsreferendar am Hanseatischen Oberlandesgericht Hamburg

Dr. Alexander Brüggemeier, LL.B.
Richter am Landgericht Arnsberg

Dr. Anabel Guntermann, LL.B.
Rechtsreferendarin am Hanseatischen Oberlandesgericht Hamburg

Dr. Katrin Haußmann
Rechtsanwältin und Fachanwältin für Arbeitsrecht, Partner, Gleiss Lutz, Stuttgart

Prof. Dr. Dennis-Kenji Kipker
Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Berlin

Christoph Benedikt Müller, LL.B.
Wissenschaftlicher Mitarbeiter bei Prof. Dr. Dr. h.c. mult. Karsten Schmidt, Bucerius Law School, Hamburg

Dr. Isabella Risini, LL.M.
Akademische Rätin auf Zeit an der Juristischen Fakultät der Ruhr-Universität Bochum, assoziiertes Mitglied des NRW-Forschungskollegs SecHuman, Sicherheit für Menschen im Cyberspace

Darius Rostam, LL.B.
Wissenschaftlicher Mitarbeiter an der Juniorprofessur für Bürgerliches Recht, Immaterialgüterrecht sowie Recht und Digitalisierung, Bucerius Law School, Hamburg

Dr. Sarah Schmidt-Versteyl, LL.M.
Rechtsanwältin und Partner, Noerr, Düsseldorf

Prof. Dr. Gerald Spindler
Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Multimedia- und Telekommunikationsrecht, Juristische Fakultät, Georg-August-Universität Göttingen