IT-Organisationspflichten des Geschäftsleiters

Die Haftung von Geschäftsleitern (Geschäftsführern, Vorstands- und Aufsichtsratsmitgliedern) ist ein Wesenselement des Kapitalgesellschaftsrechts und Ausgleich für das Privileg der beschränkten Haftung der Gesellschafter.[1] Die jüngere Entwicklung in Lehre und Rsp rückt die Organisationspflichten des Geschäftsleiters in den Vordergrund. Zunehmende Bedeutung erlangt hierbei die Verantwortung für die Einrichtung und Sicherung leistungsfähiger IT-Systeme in Unternehmen (IT-Organisationspflichten).

JOHANNES REICH-ROHRWIG / ARNO ZIMMERMANN

A. Problemaufriss

In regelmäßigen Abständen ist von großangelegten IT-Angriffen auf Unternehmen oder staatliche Einrichtungen zu lesen. In Österreich wurden jüngst der größte Telekommunikationsanbieter,[2] ein großer Baukonzern,[3] das Außenministerium[4] sowie eine Regierungspartei[5] Opfer professioneller Angriffe. Eine Studie unter mehr als 500 österr Unternehmen hat ergeben, dass in den letzten zwölf Monaten 57% der Unternehmen Opfer zumindest einer Cyber-Attacke waren.[6] Die Datenlage dazu ist allerdings, insb was die erlittenen Schäden anbelangt, schwach. Nicht zuletzt dürften viele Unternehmen bestrebt sein, erfolgreiche Cyber-Attacken nicht publik werden zu lassen, weil die Veröffentlichung das Vertrauen in das Unternehmen untergraben könnte.

Die Komplexität der Aufgabe wird verdeutlicht, wenn bspw ein Banken-Konglomerat jüngst vom Abfluss von drei Millionen Kundendaten berichten musste, trotz Investitionen von rund 2,5 Milliarden in den letzten Jahren in die IT-Sicherheit.[7]

Die Herausforderung für Unternehmen ist damit klar. Unklar sind die Pflichten des Geschäftsleiters in Bezug auf IT-Security. Das AktG und das GmbHG, deren Verfasser sich die aktuellen Gefahren nicht erträumen konnten, schweigen hierzu. Dies ist allerdings nichts Ungewöhnliches für die Anforderungen an eine moderne Unternehmensführung: Kennen doch die Gesetze schließlich auch keine Marketing- oder Public-Relations-Pflichten, Personalführungs-Pflichten oder Forschungs- und Entwicklungspflichten. Es stellt sich damit die Frage, nach welchen Grundsätzen ein Geschäftsleiter verpflichtet ist, sich einer neuralgischen Unternehmensressource wie der IT-System, anzunehmen.

B. Grundlagen der Organisationspflicht

Dem Gesetz ist eine allgemeine Organisationspflicht des Geschäftsleiters nicht ausdrücklich zu entnehmen, doch besteht sie unstrittig.[8] Moderne Unternehmen, als komplexe hochgradig arbeitsteilige Einheiten, erfordern eine weitgehende Delegation von Aufgaben an untergeordnete Ebenen. In den Fokus der „Leitungsverantwortung" des Geschäftsführers rückt damit die Anleitung und Überwachung der Mitarbeiter nachgeordneter Ebenen sowie deren hinreichende Ausstattung mit Ressourcen, um die Wahrnehmung der Aufgaben des Unternehmens sicherzustellen.

1. Internes Kontrollsystem

Eine ausdrücklich im Gesetz genannte Ausprägung der Organisationspflicht des Geschäftsleiters ist die Einrichtung eines internen Kontrollsystems (§ 82 AktG; § 22 GmbHG). Darunter versteht man die Aufgabe, Methoden und Maßnahmen in einem Unternehmen zu etablieren, die das Vermögen der Gesellschaft durch Gewährleistung der Genauigkeit und Zuverlässigkeit der Abrechnungsdaten sichern. Diese bilden die Datengrundlage für die Unterstützung der Geschäftspolitik.[9] Das IKS ist damit in erster Linie rechnungslegungsbezogen zu verstehen und soll eine genaue, aussagekräftige und manipulationssichere Erfassung und Auswertung der Geschäftsfälle sicherstellen.

Der Vorstand hat damit nicht – wie es auch physisch unmöglich wäre – sämtliche Geschäftsprozesse selbst zu überwachen und aufzuzeichnen, sondern organisatorische Maßnahmen zu setzen wie die Etab-

Univ.-Prof. Dr. *Johannes Reich-Rohrwig* ist RA und lehrt am Institut für Unternehmens- und Wirtschaftsrecht der Universität Wien. *Arno Zimmermann,* LL. M., ist RA bei CMS Reich-Rohrwig Hainz Rechtsanwälte in Wien.

Dieser Beitrag ist dem langjährigen Schriftleiter der ecolex, Univ.-Prof. Dr. *Georg Wilhelm,* anlässlich seines Ausscheidens aus der Redaktion gewidmet.

1) *J. Reich-Rohrwig,* Grundsatzfragen der Kapitalerhaltung bei AG, GmbH sowie GmbH & Co KG (2004) 23 ff.
2) https://wien.orf.at/v2/news/stories/2760928/ (abgerufen am 31. 7. 2020).
3) https://industriemagazin.at/a/cyberangriff-auf-den-baukonzern-porr (abgerufen am 31. 7. 2020).
4) https://orf.at/stories/3149769/ (abgerufen am 31. 7. 2020).
5) https://orf.at/stories/3144182/ (abgerufen am 31. 7. 2020).
6) KPMG-Studie Cyber Security in Österreich 2020, Mai 2020, kpmg.at/cyber
7) https://orf.at/stories/3142384/ (abgerufen am 31. 7. 2020).
8) Eingehend *Goette,* Organisationspflichten in Kapitalgesellschaften zwischen Rechtspflicht und Opportunität, ZHR 175 (2011) 388 ff; *J. Reich-Rohrwig* in *Artmann/Karollus,* AktG II⁶ § 70 Rz 57.
9) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II⁶ § 82 Rz 28 mwN; *Wegenstein,* persaldo 1998 H 3, 12; *Manfreda,* RWZ 1999, 271; *Heiss,* RFG 2013/3, 11 (12); *NN,* RWP 2012, 97; *Löffler/Ahammer/Kerschbaumer/Nayer* (Hrsg), Handbuch zum Internen Kontrollsystem² (2011) 17.

lierung eines Vier-Augen-Prinzips, die Trennung und wechselseitige Kontrolle von Funktionen (Beschaffung/Buchhaltung), die Einräumung von Pouvoir-Grenzen, die Erteilung von Dienstanweisungen und die Festlegung von Berichtslinien. Unterlässt er es, derartige organisatorische Vorkehrungen größen-, branchen- und situationsadäquat in vertretbarem Umfang angemessen einzurichten, so handelt er pflichtwidrig. Er handelt allerdings nicht schon deshalb pflichtwidrig und ist der Gesellschaft daher nicht schon deshalb zu Schadenersatz verpflichtet, weil innerhalb dieser Organisation Fehler passieren,[10] diese sind Teil des unternehmerischen Risikos, das der Rechtsträger – in unserer Ausgangssituation die AG oder GmbH – trägt.

Ein Teilbereich eines Internen Kontrollsystems kann hierbei ein „Steuerkontrollsystem" sein. Die BAO enthält eine Legaldefinition eines solchen Systems als *„die Summe aller Maßnahmen (Prozesse und Prozessschritte), die gewährleisten, dass die Besteuerungsgrundlagen für die jeweilige Abgabenart in der richtigen Höhe ausgewiesen und die darauf entfallenden Steuern termingerecht und in der richtigen Höhe abgeführt werden"*. Die Einrichtung eines Steuerkontrollsystems zur begleitenden Kontrolle durch die Finanzbehörden ist nach der BAO fakultativ. Unseres Erachtens lässt sich ein solches Steuerkontrollsystem in – was zu betonen ist – größen-, branchen- und situationsadäquater Ausgestaltung aber bereits unter § 82 AktG bzw § 22 GmbHG subsumieren und stellt damit eine allgemeine Pflicht jedes Geschäftsleiters dar.[11]

2. Compliance Organisation

a) Grundlagen

Seit geraumer Zeit in aller Munde sind zudem Compliance-Systeme. Diese sollen dazu dienen, gesetzeswidrige Handlungen durch Mitarbeiter – oder die Geschäftsleitung selbst – zu verhindern.

Dem Gesetz ist keine ausdrückliche Pflicht zur Einrichtung einer Compliance-Organisation zu entnehmen.[12], [13] Vereinzelte Vorschriften

- wie das Verwaltungsstrafrecht (§ 9 VStG),[14] wonach den Geschäftsleiter im Rahmen seiner verwaltungsstrafrechtlichen Verantwortlichkeit nur der Nachweis der Einrichtung eines durchgreifenden Kontrollsystems vom Verschuldensvorwurf entlastet, oder
- die Datenschutzgrundverordnung, wonach organisatorische Vorkehrungen zum Schutz von Daten und deren unberechtigten Gebrauch zu treffen sind,[15]

legen die Notwendigkeit oder zumindest Zweckhaftigkeit einer Compliance-Organisation nahe. Letztlich folgt aber die Verantwortung für eine Compliance-Organisation – zumindest bei großen und komplexen Unternehmen – in erster Linie aus der Schadensabwendungspflicht des Geschäftsleiters. Dieser hat die Gesellschaft vor Nachteilen zu schützen und entsprechende Vorkehrungen zu treffen. Führt man sich die Auswirkungen von Compliance-Skandalen – bspw in der deutschen Großindustrie – vor Augen, aber auch die drohenden Geldbußen im Kartell- oder Datenschutzrecht von 10% des Konzernumsatzes, wird schnell deutlich, dass „Compliance" keine bloße Aufgabe für Weltverbesserer ist, sondern im ureigenen finanziellen Interesse von Unternehmen liegt.

Den Geschäftsleiter größerer bzw komplexer Unternehmen trifft damit in aller Regel auch eine – ungeschriebene – Organisationsverantwortung im Compliance-Bereich.[16] Maßnahmen, die ein Geschäftsleiter zu setzen hat, sind bspw die Einführung von Compliance-Richtlinien, Schulungen für Mitarbeiter, Maßnahmen zur Überprüfung von Geschäftspartnern, die Einrichtung von Kontrollinstanzen im Unternehmen (Compliance-Officer), die entsprechende Gestaltung von Anreizsystemen für die Mitarbeiter und die regelmäßige Überprüfung der Wirksamkeit des Compliance Systems.[17] Der Geschäftsleiter darf sich hierbei selbstverständlich auch externer Berater zur Evaluierung bedienen, deren Kosten die Gesellschaft trägt.

Gleichzeitig zu betonen ist, dass die Einrichtung einer Compliance-Organisation dennoch keine allgemeine (kapital-)gesellschaftsrechtliche Pflicht ist. Im Bereich der KMU wäre es uE überschießend, eine Compliance-Organisation im engeren Sinne zu fordern. Dies betrifft nach ihrer Anzahl die große Mehrheit der Kapitalgesellschaften in Österreich.[18] Hier

10) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 84 Rz 184; *Schopper/Walch in Kalss/Frotz/Schörghofer*, HB Vorstand Rz 42/70; *Hopt/Roth* in Großkomm AktG[5] § 93 Rz 76 f, 84; *Bachmann*, ZIP 2014, 579.

11) Zutreffend *P. Schörghofer*, § 22 Abs 1 GmbHG – Pflicht zur Führung eines internen Kontrollsystems, ZSS 2020, 81 f; anders *Stieglitz*, Der GmbH-Geschäftsführer im Finanzstrafrecht, Tax Compliance Management Systeme als mögliches Instrument der finanzstrafrechtlichen Risikominimierung, taxlex 2016, 346.

12) Siehe dazu näher *J. Reich-Rohrwig/A. Zimmermann* in *Artmann/Karollus*, AktG[6] § 82 Rz 34 ff.

13) Sondergesetzlich existieren solche Pflichten, etwa iZm den Geldwäschevorschriften sowie ganz allgemein für Kreditinstitute (§§ 39, 39 b und 99 BWG), Versicherungen (§§ 108 und 117 VAG 2016), Börseunternehmen (§ 21 BörseG 2018), Wertpapierunternehmen (§ 26 WAG 2018), Investmentfonds (§ 15 InvFG 2011) und Zahlungsdienstleister (§ 20 ZaDiG).

14) VwGH 16. 5. 2011, 2009/17/0186; 30. 6. 2006, 2003/03/0033; 21. 1. 2004, 2001/09/0215; 20. 2. 2014, 2011/07/0225 ecolex 2014/231, 572 *(Primosch)*; zu den Anforderungen an eine wirksames Kontrollsystem zB VwGH 27. 1. 2012, 2011/02/0347, und 18. 11. 2011, 2011/02/0322.

15) Vgl hierzu, *Löschhorn/Furhmann*, *„Neubürger"* und die Datenschutz-Grundverordnung: Welche Organisations- und Handlungspflichten treffen die Geschäftsleitung in Bezug auf Datenschutz und Datensicherheit? NZG 2019, 161.

16) So die herrschende Meinung in Deutschland und Österreich *Kort* in Großkomm AktG[5] § 91 Rz 121; *Mertens/Cahn* in KölnKomm AktG[3] § 91 Rz 35; *Spindler* in MüKo AktG[4] § 91 Rz 52 je mwN; *G. Schima*, DRdA 2014, 197; *Frotz/Schörghofer* in *Kalss/Kunz*, HB AR[2] § 8 Rz 21; *Feltl*, wbl 2010, 265 (270); *U. Torggler* in *Kalss/U. Torggler*, Compliance 111, allerdings aufgrund einer breiten Auslegung des Begriffs „Compliance", der insb auch das IKS umfasst; *Strauss/Hiermann*, ARaktuell 2014 H 6, 8; eine strenge Pflicht zur Einrichtung einer Compliance-Organisation ablehnend *Napokoj* in *Kalss/Frotz/Schörghofer*, HB Vorstand, Rz 13/19, 22 f.

17) Vgl hierzu insb die Normen ONR 192050; ISO 19600:2014.

18) Vgl *J. Reich-Rohrwig*, Struktur der Aktiengesellschaften in Österreich (Teil I), ecolex 2018, 526, und (Teil II) ecolex 2018, 912. Zur Statistik: Nur rd 7.700 Betriebe (= 1,5% aller Arbeitgeberbetriebe, die Mitglieder der Wirtschaftskammer in Österreich sind), haben 50 bis

wird idR das wachsame Auge der Geschäftsleitung in Bezug auf mögliche Gesetzesverletzungen als hinreichend zu erachten sein.[19]

C. IT-Organisation

Ein bislang in der juristischen Debatte wenig beachteter Aspekt sind die Sorgfaltspflichten von Geschäftsleitern in Bezug auf die Einrichtung einer IT-Organisation (teilweise auch „Digitale Unternehmensverantwortung" genannt), wenngleich in der Wirtschaft die Abhängigkeit der Unternehmen von leistungsfähigen IT-Systemen rasant steigt. Dies kann auch kleine und Kleinstunternehmen betreffen.[20]

1. Gesetzliche Rahmenbedingungen

a) AktG und GmbHG

Das AktG und das GmbHG enthalten keine ausdrücklichen Vorstandspflichten in Bezug auf die IT-Organisation. Auf sondergesetzliche Vorschriften wird noch zurückzukommen sein (etwa § 39 Abs 2b BWG; § 110 Abs 2 VAG 2016; § 85 ZaDiG 2018).

Der Gesetzgeber hebt zwar iZm den „Kardinal-Pflichten" von Vorstand und Geschäftsführern im Bereich der Rechnungslegung die Einrichtung eines internen Kontrollsystems hevor (s hierzu bereits oben). Mittlerweile ist allerdings die Frage zu stellen, ob diese Hervorhebung durch den Gesetzgeber unvollständig geworden ist.

Unseres Erachtens sind im 21. Jahrhundert die Pflicht zur Ausstattung der Gesellschaft mit branchen- und größenadäquaten IT-Systemen und der angemessene Schutz dieser vor unberechtigten Zugriffen als neue wesentliche Aufgabe des Geschäftsleiters zu betrachten. Die eingangs genannten Beispiele belegen dies.

Zutreffend sprechen Autoren deshalb von der digitalen Unternehmensverantwortung als Leitungsaufgabe oder „Chefsache".[21]

Ausdrückliche IT-Organisationspflichten bestehen bisher nur in Sondergesetzen:

b) Finanzmarktrechtliche Sondervorschriften

Im Finanzmarktrecht bestehen zahlreiche Sondervorschriften für die IT-Sicherheit: Kreditinstitute haben ihr operationelles Risiko gem § 39 Abs 2b BWG zu begrenzen.[22] Dafür hat die FMA einen Leitfaden für IKT-Sicherheit (Informations- und Kommunikationstechnologie) erlassen. Sehr instruktiv ist auch das Pendant der deutschen BaFin „Bankaufsichtliche Anforderungen an die IT (BAIT)".

Beispielhaft sind Maßnahmen wie die Festlegung einer IT-Strategie einschließlich einer IKT-Aufbauorganisation und von Prozessen zur Identifikation, Bewertung und Steuerung von Risken, die Dotierung ausreichender Ressourcen oder die Aus- und Weiterbildung von Mitarbeitern zu nennen. Auf technischer Ebene umfasst dies Maßnahmen wie Protokollierungsvorschriften, Verschlüsselungen, Zugangskontrollen oder Penetrationstests.

c) Netz- und Informationssicherheitsgesetz[23] basierend auf EU-NIS Richtlinie (EU 2016/1148)[24]

Für Betreiber kritischer Infrastruktur in verschiedenen Sektoren (Energie, Banken, Verkehr, Gesundheitswesen, Trinkwasser, digitale Infrastruktur) bestehen Sondervorschriften nach dem Netz- und Informationssicherheitsgesetz (NISG).

Nach dem NISG werden bspw für die öffentliche Verwaltung, aber auch für die einzelnen Sektoren Notfallteams eingerichtet, die bei Sicherheitsvorfällen in kritischer Infrastruktur (sog „wesentliche Dienste") zum Einsatz kommen.

Betreiber wesentlicher Dienste haben geeignete Sicherheitsvorkehrungen zu ergreifen und sich von speziell nach dem NISG zertifizierten Anbietern auditieren zu lassen.

2. Pflichten für nicht regulierte Unternehmen

Welche Pflichten treffen Geschäftsleiter nicht besonders regulierter Unternehmen in Bezug auf die IT-Organisation?

a) Strategische Pflichten

Unzweifelhaft treffen den Vorstand im Lichte der Digitalisierung strategische Pflichten in Bezug auf die IT-Organisation.[25] Hierbei hat sich ein Geschäftsleiter bspw zu fragen, inwieweit bestehende Unternehmensprozesse digitalisiert werden können oder müssen, um die Wettbewerbsfähigkeit des Unternehmens zu erhalten oder ob die wesentlichen Daten des Unternehmens digital und so strukturiert erfasst werden, sodass Digitalisierungsprozesse überhaupt erfolgversprechend in Angriff genommen werden können. Entscheidende Themen in Konzernen können hier bspw die Vereinheitlichung von Systemen sein bzw die Umstellung von veralteten oder parallell aufenden Systemen.

Zumeist werden diese strategischen Pflichten, die für den künftigen Erfolg oder Misserfolg des Unter-

249 Beschäftigte, nur rd 1.600 Betriebe (= 0,3% aller Arbeitgeberbetriebe) haben 250 oder mehr Beschäftigte (Stand 07/2019). Quelle: http://wko.at/statistik/bundesland/arbeitgeber.pdf

19) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II⁶ § 82 Rz 37; *Kalss* in *Kalss/U. Torggler,* Compliance, 9; *Kort* in Großkomm AktG⁵ § 91 Rz 139 f; *Mertens/Cahn* in KölnKomm AktG³ § 91 Rz 37; *Spindler* in MüKo AktG⁴ § 91 Rz 67.

20) Hierzu in jüngerer Zeit *Spindler,* Gesellschaftsrecht und Digitalisierung, ZGR 2018, 17; *Noack,* Organisationspflichten und -strukturen kraft Digitalisierung, ZHR 2019, 105 ff; *Schmidt-Versteyl,* Cyber Risks – neuer Brennpunkt Managerhaftung? NJW 2019, 1637; *Heese/Fröhlich,* Bedeutung von IT und Organisation in Unternehmen, WPg 2013, 547.

21) *Spindler,* Gesellschaftsrecht und Digitalisierung, ZGR 2018, 40; *Schmidt-Versteyl,* NJW 2019, 1640.

22) *Kammel* in *Laurer/M. Schütz/Kammel/Ratka,* BWG⁴ § 39 Rz 28.

23) NISG BGBl I 2018/111.

24) *Kristoferitsch/Lachmayer,* Die NIS-Richtlinie und ihre österreichische Umsetzung im NIS-Gesetz, ecolex 2020, 74.

25) *Noack,* Organisationspflichten und -strukturen kraft Digitalisierung, ZHR 2019, 125 ff; vgl zu den Pflichten hinsichtlich strategischem Management *J. Reich-Rohrwig* in *Artmann/Karollus,* AktG II⁶ § 70 Rz 35.

nehmens entscheidend sein können, abstrakt nicht klar erfassbar und letztlich auch unjustiziabel sein.

Im höheren Maße definierbar und damit auch potenziell haftungsbegründend können die Pflichten des Vorstands hinsichtlich der Sicherung der IT-Systeme sein. Darauf wollen wir im Folgenden eingehen:

b) Pflichten in Hinblick auf die Sicherung der IT-Systeme

■ **Schadenabwendungspflicht**

Ausgangspunkt für die Pflichten des Geschäftsleiters zur Sicherung der IT-Systeme ist seine Schadenabwendungspflicht, nach der er die Gesellschaft betreffende Gefahren und Risken zu berücksichtigen und – sofern erforderlich – einzudämmen hat.[26)]

Der Geschäftsleiter ist nicht gehalten, jede erdenkliche Schadenquelle zu minimieren. Vielmehr ist der Geschäftsleiter stets zu einer Kosten-Nutzen-Rechnung berechtigt, die allerdings nach hA bestandsgefährdende Risken besonders zu berücksichtigen hat.[27)] Für IT-Systeme bestehen hierbei folgende Besonderheiten

- Unternehmen sind heutzutage für ihren tagtäglichen Betrieb von IT-Systemen in hohem Maße abhängig;
- Störungen können nicht nur lokal auftreten, sondern können binnen kürzester Zeit das gesamte Unternehmen/Konzern weltweit erfassen. Sie sind damit Bündelrisken;
- die Wiederherstellung der Funktionsfähigkeit kann unmöglich sein, bspw bei permanentem Datenverlust;
- IT-Systeme stellen unmittelbare Kontaktpunkte zu Kunden dar, Fehlverhalten von Kunden kann Unternehmen mittelbar wie unmittelbar schädigen (bspw Fishing-Attacken);
- über IT-Systeme ist sowohl der Zugang zu sensiblen Informationen des Unternehmens als auch Dritter möglich. IT-Systeme sind darüber hinaus auch in der Lage, physische Beschädigungen zuzufügen (bspw an den oder durch von ihnen gesteuerte Anlagen).

IT-Systeme in Unternehmen werden daher regelmäßig als „kritische Infrastruktur" zu bewerten sein.[28)] Hierbei kommt dem Geschäftsleiter wohl auch ein Ermessen bei der Intensität des Schutzes kritischer Infrastruktur zu, jedoch dürfte eine sorgfältig betriebene Kosten-Nutzen-Analyse rasch zugunsten des Schutzes derartiger Infrastruktur ausschlagen: So dürften bspw die Kosten für eine Mitarbeiterschulung, für die Einrichtung hinreichend sicherer Passwörter oder für den Schutz von IT-Infrastruktur vor einem physischen Zugriff durch Unberechtigte regelmäßig relativ gering sein, sie sind aber wirksame Mittel, um potentiell existenzbedrohende Schäden zu vermeiden.

Gleichzeitig darf nicht verlangt werden, dass jeder Geschäftsleiter den höchstmöglichen oder idealen Schutz der IT-Systeme einrichtet. Die technischen Möglichkeiten zur Sicherung von Systemen sind hierbei nach oben hin beinahe unbegrenzt, aber mit erheblichen Kosten und auch Behinderungen im Geschäftsbetrieb verbunden. Nicht zuletzt zeigen aktuelle Angriffe sowie empirische Daten,[29)] dass das Auftreten staatlicher oder staatsnaher Akteure iZm IT-Angriffen zunimmt. Auch von großen Unternehmen kann hierbei nicht verlangt werden, Angriffe auf geheimdienstlichem Niveau jederzeit abwehren zu können, ebenso wenig wie man fordern würde, das Betriebsgelände vor gut organisierten terroristischen Anschlägen oder vor dem Zugriff militärisch operierender Akteure schützen zu können.

Aufsetzend auf einem vertretbaren Grundniveau einer Sicherung der IT-Systeme kommt dem Geschäftsleiter daher bei der Optimierung des Schutzes durchaus weites Ermessen zu.[30)]

Nachfolgend sollen ohne Anspruch auf Vollständigkeit denkbare Schritte in der Festlegung einer auf den Schutz der IT-Systeme ausgerichteten Organisation skizziert werden.[31)]

■ **Bestandsaufnahme und Risikoanalyse**

Das Handeln auf angemessener Informationsgrundlage iS der Business Judgment Rule wird es in der Regel erfordern, dass das Unternehmen eine Bestandsaufnahme der bestehenden IT-Systeme und der Risken und Schwächen durchführt.[32)]

Ein wesentlicher Punkt ist hierbei die Definition kritischer Systeme, sohin solcher Systeme, deren Ausfall für das Unternehmen besonders schadenträchtig wäre. Ein Handels- oder Produktionsunternehmen wird sich bspw fragen müssen, inwieweit Kassensysteme oder Produktionsmaschinen offline und autonom von den sonstigen Systemen betrieben werden können oder ob ein Ausfall der IT die völlige Betriebsunterbrechung mit sich bringt. Klassische Fragestellungen sind ferner, welche Daten oder Anwendungen zum Geschäftsbetrieb notwendig oder welche verwundbaren Schnittstellen nach außen, bspw Internet-Seiten oder vernetzte Geräte, vorhanden sind.

■ **Festlegung einer IT-Strategie, Aufbau- und Ablauforganisation**

Die Bestandsaufnahme mündet in die Festlegung einer IT-Strategie bzw Aufbau- und Ablauforganisation, die bspw folgende Inhalte hat:

- Festlegung der Verantwortungsbereiche und Zuständigkeiten. Auf Ebene der Geschäftsleitung ist hier auch festzulegen, welcher Geschäftsführer/welches Vorstandsmitglied res-

26) Hierzu *Holle,* Legalitätskontrolle im Kapitalgesellschafts- und Konzernrecht (2014) 47 f; *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 47; *U. Torggler,* Wider die Verselbständigung der Begriffe: Compliance, Legalitätspflicht und Business Judgment Rule, in *Kalss/U. Torggler* (Hrsg), Compliance (2016) 99.

27) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 42.

28) Die beschriebenen Pflichten besonders regulierter Unternehmen können hierfür als gewichtiges Indiz betrachtet werden, *Noack,* ZHR 2019, 127.

29) KPMG-Studie Cyber Security in Österreich 2020, Mai 2020, kpmg.at/cyber

30) *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 42; *Kort* in Großkomm AktG[5] § 91 Rz 141.

31) Vgl hierzu insb ISO 27001; das Österreichische Informationssicherheitshandbuch; den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik; zu all dem auch *Michl/Reautschnig,* „Better safe than sorry!", GRCaktuell 2018, 66.

32) *Schmidt-Versteyl,* NJW 2019, 1637.

sortzuständig ist, ob ein Chief Technology Officer in den Vorstand aufgenommen wird und ob das Unternehmen eine eigene IT-Sicherheitsabteilung unter Leitung eines CISO (Chief Information Security Officer) erhält;
- Festlegung der IT-Architektur, Festlegung von Grundsätzen des Lebenszyklusmanagements (Updates von Hard- und Software);
- Dokumentationspflichten für IT-Systeme;
- Festlegung von ausgelagerten Systemen und Anwendungen;
- Festlegung von Notfallsplanungen.

■ **Schutzmaßnahmen/Risikomanagement**

Im Kernbereich der hier behandelten Organisationspflichten steht das IT-Risikomanagement einschließlich der Etablierung entsprechender Schutzmaßnahmen. Hierbei wird der Geschäftsleiter idR für die Erstellung einer entsprechenden Sicherheitsrichtlinie zu sorgen haben, die ua folgende Aspekte berücksichtigt bzw Maßnahmen anordnet:
- IT-Sicherheitsarchitektur (Firewalls, Intrusion Detection Systeme, Spam-Filter, Antiviren Software, ggf Trennung von Systemen „demilitarisierte Zone");
- Passwort- und Verschlüsselungsrichtlinien;
- Berechtigungsmanagement (wer hat unter welchen Voraussetzungen auf welche Systeme Zugriff, einschließlich ggf Background-Checks von Mitarbeitern, Need-to-know-Prinzipien);
- Protokollierung und Erkennung von Datenschutzverletzungen und unberechtigten Zugriffen;
- physische Sicherheit der IT-Systeme, Zugangskontrollen;
- Backup-Systeme (bspw online, auf physischen Datenträgern etc);
- Richtlinien zur Mitarbeiterschulung und Fortbildung.

■ **Überwachung, Überprüfung, Zertifizierung**

Einmal gesetzte Sicherheitsmaßnahmen können ihre Wirksamkeit verlieren, wenn sie nicht regelmäßig überprüft und aktualisiert werden.

In der Praxis verbreitet sind bspw Penetrationstests, bei denen das Unternehmen externe Anbieter beauftragt, Schwachstellen der IT-Sicherheit im Unternehmen zu entdecken und so Zugriff in das System zu erlangen (vulgo „hacken"). Derartige Tests sind sowohl vor der Inbetriebnahme neuer Systeme als auch laufend im Geschäftsbetrieb sinnvoll. Auch Tests der physischen Sicherheit, bspw durch sog „Tiger-Teams", die versuchen, physisch in die Geschäftsräume zur Hardware vorzudringen, um diese zu entwenden, können Schwachstellen aufzeigen.

Audits bzw eine Zertifizierung nach internationalen Standards bieten eine weitere Möglichkeit zum Erkennen von Schwachstellen, zur externen Validierung und Nachbesserung der getroffenen Maßnahmen. Hierbei können Unternehmen sich auch einem „Rating" für Cyber-Security unterziehen, das je nach Güteklasse (bspw A, B) verschiedene Anforderungen vorsieht und deren Einhaltung überprüft.

Schließlich bedarf es einer regelmäßigen Schulung von Mitarbeitern: Denn die Mitarbeiter stellen häufig das größte Risiko dar. Zu nennen sind Trainingsprogramme oder nachgebildete Angriffe, bspw durch simulierte Fishing-E-Mails (vgl *„CEO Fraud"*).

D. Business Judgment Rule mit Hinblick auf die IT-Organisation

Vor dem Hintergrund der oben skizzierten möglichen Maßnahmen zur Implementierung einer IT-Sicherheitsorganisation ist zu fragen, welche Anforderungen an die Sorgfaltspflicht des Geschäftsleiters nach der Business Judgment Rule zu stellen sind. Auszugehen ist hierbei davon, dass die Maßnahmen zur Erfüllung der Organisationspflichten weitestgehend unternehmerische Entscheidungen iSd § 84 Abs 1 a AktG (§ 25 Abs 1 a GmbHG) sind:[33]

1. Hinreichende Informationsgrundlage

Um auf Basis angemessener Informationsgrundlage entscheiden zu können, wird ein Geschäftsleiter in der Regel zunächst eine fachkundige Analyse der IT-Systeme des Unternehmens und deren mögliche Schwachstellen durchzuführen haben bzw eine solche durch externe Experten durchführen lassen oder sich vergewissern müssen, dass eine solche Analyse bereits besteht.

Ein Geschäftsleiter muss nicht IT-Fachmann sein.[34] Etwaige inhaltliche Mängel der Analyse sind ihm daher uE nicht als mangelnde Informationsgrundlage anzulasten. Wenn, um einige der oben genannten Maßnahmen zu nennen, daher bspw Mängel bei der Notfallsplanung bestehen, die Backup-Systeme unzureichend dimensioniert sind oder, mögen sie für einen Experten auch offenkundig sein, Schwachstellen bestehen, die externe Angreifer ausnützen können, ist dies nicht mit einer mangelnden Informationsgrundlage oder gar einem Verschulden gleichzusetzen.

Sehr wohl wird sich ein Geschäftsleiter aber vergewissern müssen, ob die beigezogenen Mitarbeiter oder Dritte die notwendige Sachkunde aufweisen und ob die Analyse unplausibel ist.[35] Problematisch können hierbei insb eingeschränkte Auftragsstellungen sein: Wird ein externer Anbieter nur zur Analyse von gewissen Schwachstellen (bspw unberechtigter Zugriff von außen) herangezogen, liegt in Bezug auf andere Risken (bspw Datenverlust durch physische Beschädigung, Fehlbedienung durch Mitarbeiter) keine vollständige Risikoanalyse vor, es sei denn das Unternehmen hat eine solche fachgerecht bereits intern durchgeführt. Die Risikoanalyse sollte daher möglichst ganzheitlich erfolgen.

Über die Umsetzung der IT-Strategie bzw des Sicherheitskonzepts wird die Geschäftsleitung, und in höherem Maße der ressortzuständige Geschäftsleiter, regelmäßige Berichte einzufordern haben.

33) Eingehend zu den Tatbestandsmerkmalen der Business Judgment Rule *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 84 Rz 179 ff.

34) *Noack*, Organisationspflichten und -strukturen kraft Digitalisierung, ZHR 2019, 127.

35) Zur Pflicht einer Plausibilitätskontrolle bei komplexen Fragestellungen *J. Reich-Rohrwig/K. Grossmayer* in *Artmann/Karollus*, AktG II[6] § 84 Rz 129.

Zudem ist sicherzustellen, dass geeignete Kontrollen etwaiger Schwachstellen in den IT-Systemen vorgenommen werden. Hierbei kann uE auch die Anweisung an die entsprechenden (fachkundigen) Mitarbeiter, regelmäßige Kontrollen durchzuführen, hinreichend sein. Bei entsprechend großen bzw komplexen Organisationen können – und dies dürfte weitgehend auch Marktstandard sein – aber auch weitergehende Überprüfungen wie Audits oder Penetrationstests als erforderliche Informationsgrundlage betrachtet werden. Anzuraten sind solche externen Kontrollen einem Geschäftsleiter jedenfalls.

Im Rahmen der Entscheidung für oder gegen Investitionen in IT-Systeme sind zumindest grundsätzliche Abwägungen in Bezug auf die Kosten bzw Nutzen anzustellen, also Schadenpotenziale und Wahrscheinlichkeiten grob abzuschätzen.

2. Handeln zum Wohle der Gesellschaft

Schließlich ist zu fragen, wann ein Geschäftsleiter seine IT-Organisationspflichten in geradezu unvertretbarer Weise verletzt und damit nicht zum Wohle der Gesellschaft handelt.

Ein Fall einer unvertretbaren Handlung könnte in einer schlicht unvertretbaren Kosten-Nutzen-Analyse liegen. Zahlreiche IT-Sicherheitsmaßnamen sind – wie bereits erwähnt – durch erträglich geringen Aufwand umsetzbar: Passwortrichtlinien, Zwei-Faktor-Authentifizierung, physischer Schutz von Einrichtungen, Mitarbeiterschulungen – tragen aber gleichzeitig massiv zum Sicherheitsstandard bei. Lehnt ein Geschäftsleiter derartige Maßnahmen ab, bspw durch die Versagung eines entsprechenden Budgets, kann dies uE in den Bereich der Unvertretbarkeit reichen.[36] Ähnliches kann für erkannte Personalmängel oder die erkannte Unterqualifikation von Mitarbeitern gelten.

Unvertretbar kann ferner die Unterlassung der Behebung von erkannten Schwachstellen sein: wenn bspw dem Geschäftsleiter Verstöße gegen die etablierten Sicherheitsrichtlinien bekannt sind oder eine Häufung von Vorfällen eintritt, ohne dass der Geschäftsleiter Anweisungen zur Behebung der Schwachstellen erteilt.

Durchaus verbreitet in der Praxis sind hier auch Verstöße durch die Geschäftsleiter selbst, die nicht von der Business Judgment Rule erfasst sind: Dauerhafte Weitergabe von persönlichen Passwörtern mit weitgehenden Berechtigungen oder TAN-Codes an nicht vertrauenswürdige Mitarbeiter, habituelle Umgehung von Sicherheitsvorschriften durch Erteilung von abweichenden Weisungen an Untergebene.[37] Hier gilt, dass die Geschäftsleitung die sorgfältig ausgearbeiteten Sicherheitsvorkehrungen nicht durch faktisches Handeln aussetzen darf. Will die Geschäftsleitung Prozesse im Unternehmen in höherem Ausmaß delegieren, wie zB durch Vergabe weitergehender Bankzeichnungs- oder sonstiger Berechtigungen an Untergebene, ist dies generell zulässig, nur bedarf es einer Anpassung der entsprechenden Sicherheitsvorkehrungen und die Prüfung und Beobachtung der Vertrauenswürdigkeit der eingesetzten Mitarbeiter.

3. Cyber-Versicherung

Ein iZm der IT-Organisationspflicht des Geschäftsleiters vielfach gestellte Frage ist die Versicherbarkeit dieser Risken zwecks Schadens- und Haftungsminimierung.

Der Versicherungsmarkt hat Cyber-Risken als Zukunftsmarkt längst entdeckt und bietet vielfältige Produkte zur Versicherung derartiger Risken an. Das Prämienvolumen auf diesem Gebiet ist indes in Europa derzeit noch eher bescheiden, in den USA boomt hingegen diese Sparte. Das Schadenvolumen, über das soweit ersichtlich nur grobe Schätzungen bestehen, wurde bereits im Jahr 2016 mit bis zu 500 Mrd USD jährlich beziffert.[38]

Zunächst stellt sich die Frage, ob „Cyber-Risken" überhaupt eigens versichert werden müssen, wo doch Unternehmen bereits vielfach Haftpflicht-, Sach- oder Betriebsunterbrechungsversicherungen geschlossen haben. Versicherer verweisen hierbei regelmäßig darauf, dass Cyber-Schäden, bspw an Daten etc, nicht unter den „Sachbegriff" dieser herkömmlichen Versicherungen fallen bzw regelmäßig nur ta-

36) Umfassend hierzu *Kath*, Die Cyberversicherung, ZVers 2019, 102 ff; *Keltner*, Versicherbarkeit von Cyber Risiken und ausgewählte Abgrenzungsfragen der Sparten Cyber, Vertrauensschaden-, D&O- und Betriebshaftpflichtversicherung, in *Berisha/Gisch/Koban (Hrsg)*, Haftpflicht-, Rechtsschutz- und Cyberversicherung (2018) 107.

37) Dies sind idR keine unternehmerischen Entscheidungen; vgl *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II⁶ § 84 Rz 179.

38) So *Kath*, Die Cyberversicherung, ZVers 2019, 102.

xativ aufgezählte Gefahren versichern, zu denen bspw Cyber-Attacken nicht zählen.[39]

Cyber-Versicherungen bieten hier den Vorteil von Rechtssicherheit und der Bündelung verschiedener Versicherungsarten (Eigenschaden, Drittschaden, Haftpflicht) in einem Produkt. Die Musterbedingungen (AVB Cyber in Deutschland bzw ABC 2018 in Österreich) verdeutlichen, dass Cyber-Versicherungen stark auf verschiedenen Bausteinen basieren, für die der Versicherungsnehmer optieren kann. Der bloße Abschluss einer Cyber-Versicherung bietet allerdings noch keinen allumfassenden Schutz. Als Bausteine zu nennen sind

- die Service- und Kostenversicherung für die Schadenfeststellung und -behebung oder
- die Betriebsunterbrechungsversicherung, wobei bspw nach den Musterbedingungen der Ausfall Systeme Dritter (Cloud-Dienste) nicht erfasst ist;
- die Haftpflichtversicherung, bspw auch für Schäden aus rechtswidriger Offenlegung von Daten Dritter, und
- die Versicherung für die Kosten der Wiederherstellung der Daten.

Schließlich sind auch mannigfaltige Deckungsausschlüsse zu beachten: So sind nach den Musterbedingungen der Abfluss von Vermögenswerten infolge einer Informationssicherheitsverletzung (bspw CEO-Fraud), Lösegeld- oder Erpressungszahlungen oder Schäden aufgrund wissentlicher Verletzung von IT-Sicherheitsvorschriften durch Mitarbeiter nicht versichert, sie können aber gesondert eingedeckt werden.

4. Bewertung von Cyber-Versicherungen aus Sicht einer sorgfältigen Geschäftsführung

Cyber-Versicherungen bieten daher wie gezeigt keinen Rundum-Schutz, wenngleich dies nicht heißt, dass von den Musterbedingungen ausgeschlossene Risken nicht individuell versicherbar sind. Am österr Markt werden idR Deckungssummen bis zu 20 Mio Euro angeboten.

Damit sind Cyber-Versicherungen kein Ersatz für eine IT-Sicherheit auf hohem Niveau: Einerseits weil keineswegs sicher ist, dass der konkrete Schaden gedeckt wird, andererseits weil die Deckungssummen tendenziell nicht derart hoch sind, dass existenzbedrohende Risken abgedeckt werden. Darüber hinaus sind letztlich Schäden aus einem Reputationsverlust bzw Verlust von Kundenvertrauen aufgrund schwerwiegender Sicherheitsvorfälle nicht bewertbar.

Dementsprechend gilt uE, dass ein Geschäftsleiter weder verpflichtet ist, eine Cyber-Versicherung abzuschließen, noch der Abschluss einer Cyber-Versicherung den Geschäftsleiter von seinen IT-Organisationspflichten entlastet.[40] Die Cyber-Versicherung kann aber insb dann sinnvoll und haftungsreduzierend sein, wenn unerkannte IT-Risken schlagend werden oder die Fehleranfälligkeit – insb beim Faktor Mensch = Mitarbeiter – zum Tragen kommt.

Und oft verlangen Versicherungen schon im Stadium der Vertragsanbahnung, dass das Unternehmen, das die Cyber-Deckung sucht, sich einem Cyber-Check durch IT-Experten, die die Versicherung nennt, unterzieht, damit die Versicherung das Risikopotential besser einschätzen, ggf die Abgabe eines Anbots für eine Cyber-Versicherung ablehnen kann. Solche Checks tragen auch massiv zur Selbsterkenntnis des Unternehmens über den Status seiner IT-Sicherheit bei und ist dann oft Anlass für die (dringend) notwendige Verbesserung der innerbetrieblichen IT-Sicherheit. Dies ist aus unserer Sicht ein sehr nützlicher, positiver Nebeneffekt.

5. Erfolgreicher Angriff ≠ Sorgfaltspflichtverletzung

Abschließend ist zu betonen, dass ein erfolgreicher Angriff auf die IT-Systeme eines Unternehmens keinerlei Indiz für eine Sorgfaltswidrigkeit der Geschäftsleitung ist. Das folgt schon aus der konsequenten Anwendung der Business Judgment Rule. Regelmäßig werden solche Vorfälle (i) unvermeidbar oder (ii) aufgrund solcher Lücken oder systemischer Mängel erfolgen, die zulässigerweise weit unterhalb der Wahrnehmungsgrenze einer sorgfältig handelnden Geschäftsleitung liegen. Dies etwa, weil das Erkennen der Schwächen hohes technisches Detailwissen voraussetzen würde – das man von Geschäftsleitern nicht verlangen darf – Geschäftsleiter müssen keine „Allround-Sachverständigen" sein[41] – oder der Vorfall durch individuelles Fehlverhalten von Mitarbeitern ausgelöst wurde. Nicht zuletzt ist zu berücksichtigen, dass bereits in Unternehmen mittlerer Größe zig IT-Mitarbeiter tätig sind, in Großunternehmen hunderte. Es bedarf daher besonderer Umstände, um dem Geschäftsleiter, der nicht IT-Experte sein muss, Mängel in der IT-Organisation vorzuwerfen.

Ein Verstoß gegen Organisationspflichten setzt nach dem oben Gesagten grundsätzlich die unvertretbare Ausgestaltung der IT-Sicherheitssysteme oder unvertretbare Mängel in der Ausgestaltung der Qualitätskontrolle, einschließlich der Reaktion auf erkannte Mängel, voraus.

E. Zusammenfassung

Den Geschäftsleiter einer Kapitalgesellschaft treffen mannigfaltige Organisationspflichten. In deren Rahmen hat der bzw haben die Geschäftsleiter durch Anleitung und Überwachung untergeordneter Ebenen und durch Bereitstellung der erforderlichen Ressourcen die ordnungsgemäße Wahrnehmung der Aufgaben der Gesellschaft sicherzustellen. Längst anerkannt und von Gerichten in Schadenersatzprozessen sanktioniert sind derartige Organisationspflichten für das Rechnungswesen, für die Einrichtung eines internen Kontrollsystems sowie zunehmend auch für ein Mindestmaß einer Compliance-Organisation.

Es bedarf keiner hellseherischen Fähigkeiten, dass aufgrund der Digitalisierung der Wirtschaft

39) *Günther,* Datenträgerklauseln und Sachschaden, VersR 2018, 205; differenzierend für Österreich *Kath,* Die Cyberversicherung, ZVers 2019, 106; zu den Deckungslücken „klassischer" Versicherungen eingehend *Kath,* Die Cyberversicherung, ZVers 2019, 102.

40) Vgl auch *Fortmann,* Cyber-/Datenrisiken: Erhebliche Gefahr für Geschäftsleiter und D&O-Versicherer? r+s 2019, 688 mwN.

41) *J. Reich-Rohrwig/C. Grossmayer* in *Artmann/Karollus,* AktG[6] § 84 Rz 109, 113 f.

auch verstärkt die Pflichten des Geschäftsleiters in Bezug auf die IT-Organisation in den Fokus rücken werden. Nicht erforderlich ist, dass jeder Geschäftsleiter IT-Experte wird. Allerdings haben sich der Vorstand oder die Geschäftsführung zu vergewissern, dass die Gesellschaft die wesentlichen IT-Risken ermittelt, analysiert und mittels branchen-, risiko- und größenadäquater Mittel gering hält. Eine Cyber-Versicherung mag hierbei eine sinnvolle Ergänzung zur Risikosteuerung sein, kann den Geschäftsleiter aber nicht von seinen Organisationspflichten entlasten.