Zeitschrift:	BOARD
Autoren:	Michael Beyer/Hélène Hesselmann
Beitragstyp:	Beitrag
Ausgabe:	6/2021

Auswirkungen der VUCA-Welt auf die Aufsichtsratsarbeit

Eine Illustration am Beispiel von Cyberrisiken

Michael Beyer

Dr. Michael Beyer, Director Board Advisory Services, FAS, Berlin;

Hélène Hesselmann

Hélène Hesselmann, Chief Financial Officer, Air Liquide Management Services GmbH, Frankfurt

Aufgrund der Brisanz und des zunehmenden Umfangs der Cyberkriminalität mit monatlich neuen Vorfällen, zuletzt die REvil Ransomware im Juli 2021 und das Hacking auf Colonial Pipeline im Mai 2021, liegt der Fokus des Beitrags im Folgenden darauf, wie der Aufsichtsrat in dem aktuellen VUCA-Kontext seinen Verpflichtungen zur Überwachung und Beratung des Vorstands nachkommen kann.

Inhalt

Keywords

Aufsichtsrat; Business Continuity Plan; Cyberkriminalität; Global Risks Report; Kompetenz; Organisation

I. Was bedeutet VUCA?

VUCA ist ein Akronym und steht für die Begriffe volatility (Unbeständigkeit), uncertainty (Unsicherheit), complexity (Komplexität) und ambiguity (Mehrdeutigkeit). Diese aus dem Militärischen stammende Beschreibung für das (Re-)Agieren unter schwierigen Rahmenbedingungen wird seit geraumer Zeit auch in der Management-Beratung verwendet und steht sinngemäß für die Unternehmensführung unter besonderen Herausforderungen.

Fraglich ist, ob sich die aktuelle VUCA-Situation auf Aufsichtsräte in Bezug auf deren Mandatsarbeit, Zusammensetzung etc. sowie auf das Zusammenspiel mit dem Vorstand auswirkt.

Einerseits lässt sich argumentieren, dass unternehmerische Entscheidungen grundsätzlich unter unsicheren Rahmenbedingungen getroffen wurden und werden und daher der Aufsichtsrat im Rahmen seiner Überwachung und Beratung schon immer unter VUCA-Bedingungen agieren musste. Andererseits kann angeführt werden, dass die aktuellen und zu erwartenden Herausforderungen, wie Pandemie, Digitalisierung, Disruption von Geschäftsmodellen und Klimawandel inkl. der ESG-Anforderungen, über die bisherigen Anforderungen hinausgehen, und somit auch Auswirkungen auf die Kompetenzen und die Organisation der Mandatsarbeit zu spüren sein müssten.

II. Aktuelle Beispiele

Die Vielfalt der heutigen Herausforderungen lässt sich gut anhand der letzten Monate aufzeigen. Die Covid-19-Pandemie hat nicht nur im hohen Ausmaß einige Wirtschaftsbranchen existentiell betroffen (z.B. Gastronomie und Tourismus). Alle Arbeitgeber mussten besondere Maßnahmen zum Schutz der Gesundheit ihrer Mitarbeiter treffen und ihre Arbeitsorganisation umstellen. Teilweise wurden die Lieferketten in Frage gestellt und die Kundensolvabilität wurde kritisch beobachtet. Auf Landesebene sind darüber hinaus die Organisation des Gesundheitssystems und die politische Stabilität bezüglich der Akzeptanz von Einschränkungen gefordert gewesen.

Der 2021 Global Risks Report des World Economic Forums zählt bei den Risiken mit höchster Wahrscheinlichkeit in den nächsten 10 Jahren an oberster Stelle:

- Umweltschäden durch extremes Wetter,
- unzureichende Umweltschutzmaßnahmen und
- menschlich verursachte Katastrophen.

Darauf folgen ohne nennenswerten Abstand:

- IT-relevante Risiken wie digitale Machtkonzentration,
- digitale Ungleichheit und
- Versagen von Datensicherheit.[1]

III. Anforderungen an den Aufsichtsrat

In Anlehnung an den Artikel „Der zukunftsorientierte Aufsichtsrat“[2] werden folgende Perspektiven unterschieden:

Rolle: Inzwischen ist in vielen Gremien das Selbstverständnis etabliert, dass der Aufsichtsrat über seine Überwachungsfunktion hinaus der Geschäftsleitung auch beratend und impulsgebend zur Seite stehen soll. Entsprechende regulatorische Anforderungen untermauern diesen Wechsel im Rollenverständnis.[3] Dies setzt jedoch voraus, dass im Gremium einschlägige Kompetenzen zu Themen wie IT, Digitalisierung, Cybercrime etc. überhaupt vorhanden sind.

Kompetenzen: Im DCGK 2020 wird als Empfehlung angeführt: „Der Aufsichtsrat soll für seine Zusammensetzung konkrete Ziele benennen und ein Kompetenzprofil für das Gesamtgremium erarbeiten. Dabei soll der Aufsichtsrat auf Diversität achten. Vorschläge des Aufsichtsrats an die Hauptversammlung sollen diese Ziele berücksichtigen und gleichzeitig die Ausfüllung des Kompetenzprofils für das Gesamtgremium anstreben.“[4]

Weiterhin gilt gem. Grundsatz 11: „Der Aufsichtsrat ist so zusammenzusetzen, dass seine Mitglieder insgesamt über die zur ordnungsgemäßen Wahrnehmung der Aufgaben erforderlichen Kenntnisse, Fähigkeiten und fachlichen Erfahrungen verfügen und die gesetzliche Geschlechterquote eingehalten wird.“

Häufig sind Aufsichtsräte in Bezug auf deren Kompetenzen geprägt von juristischem Sachverstand, betriebswirtschaftlichem Wissen und Branchenexpertise. Da gerade Themen wie IT und Digitalisierung neuralgische Punkte für Geschäftsmodelle und Unternehmenserfolge sind, ist eine profunde Kompetenz und Besetzung im Aufsichtsrat nicht nur wünschenswert, sondern in den meisten Fällen sicher unerlässlich. Hierbei geht es nämlich nicht nur um die Einschätzung von Strategien „mit der entsprechenden Flughöhe“, sondern im Rahmen der konkreten Überwachung und Beratung auch um Risikoeinschätzungen, Gefährdungsanalysen, Verständnis für technische und gesellschaftliche Entwicklungen etc.

Organisation: Hierbei geht es primär um die Frage, wie die Kompetenzen gebündelt und möglichst effektiv genutzt werden können. Neben der Behandlung im Plenum wäre es denkbar, einen temporären oder sogar dauerhaften Ausschuss einzurichten („Digitalisierungsausschuss“ o.Ä.) und genau in diesem die Wissensträger zusammenzuführen.

In diesem Zusammenhang heißt es in der Empfehlung D2 des DCGK 2020: „Der Aufsichtsrat soll abhängig von den spezifischen Gegebenheiten des Unternehmens und der Anzahl seiner Mitglieder fachlich qualifizierte Ausschüsse bilden.“

Unstrittig ist, dass der Aufsichtsrat seinerseits die nötigen Kompetenzen vorhalten beziehungsweise aufbauen muss (so noch nicht geschehen) sowie in seiner Selbstorganisation auch unter VUCA-Bedingungen sicherzustellen hat, dass er den Vorstand angemessen überwacht und berät.

1 Vgl. WEF, The Global Risks Report 2021, S. 11 ff.

2 Siehe Klarner/Kircher 2019, Aufsichtsrat aktuell, S. 19 ff. Auf den Punkt der Evaluation wird hier verzichtet.

3 Vgl. z.B. Grundsatz 6 DCGK 2020.

4 Vgl. DCGK 2020, C1.

IV. Anforderungen an die Zusammenarbeit mit dem Vorstand

Neben einem aktiven Eindringen in das Netzwerk versuchen Cyberkriminelle häufig, mit gefälschten Mails an gezielte Mitarbeiter (sog. Phishing) das Unternehmen anzugreifen. Mitarbeiter können durch scheinbar harmlose und verlockende Botschaften zur unbewussten Mithilfe bewegt werden. Zum Beispiel werden sie aufgefordert, einen Link anzuklicken oder einen Dateianhang zu öffnen, und führen so mögliche Viren ins Netzwerk ein.

Typische Beispiele sind Mails aus einer angeblich vertrauenswürdigen Quelle wie vom Top Management oder von Vorgesetzten oder aus einer gefälschten Lieferanten-Adresse. Im schlimmsten Fall werden mit solchen Tricks Anweisungen für Zahlungen auf unberechtigte Konten übermittelt.

Insgesamt sind die Geschäftsleitung und die Finanzleitung angehalten, alle Mitarbeiter über diese Risiken aufzuklären und an die gängigen Kommunikationswege zu erinnern, u.a. die Unternehmens-Mailadresse genau zu prüfen oder keine eiligen Zahlungsaufforderungen auf verkürzten Wegen zu veranlassen.

Gefälschte Mails enthalten in der Regel entweder in der Absenderadresse oder im Text mehr oder weniger grobe Abweichungen von einer unbedenklichen Mail: das können auffällig eingefügte Buchstaben sein oder unsorgfältige Übersetzungen einer Fremdsprache. In allen Fällen ist beim Empfänger äußerste Sorgfalt geboten. Die nächste Reaktion ist die Kontaktaufnahme mit einer internen Prüfstelle oder dem Vorgesetzten, um das weitere Vorgehen zu besprechen. Besonders in Zeiten geänderter Organisation (Home-Office beim Lockdown, Ferienvertretung etc.) hoffen Cyberkriminelle auf eine Lücke im üblichen Kontrollprozess. Anhand der genannten Beispiele können Geschäftsleitung und Aufsichtsrat den Stand des internen Kontrollsystems (IKS) erörtern und über Auffälligkeiten sollte berichtet werden.

Es ist wichtig, im IKS einen klaren Validierungsprozess unter Wahrung des Vieraugenprinzips für Zahlungsanweisungen und bei Änderungen von kritischen Daten, wie Bankkontennummern für Lieferanten oder Mitarbeiter, zu verankern. Ebenfalls sind die Nachverfolgbarkeit von IT-Änderungen in programmierten Kontrollen sowie ein angemessener Schutz der Zugriffsrechte sicherzustellen. Zusätzlich zu den eingebauten Kontrollen ist es hilfreich, regelmäßige eigene Testversuche durchzuführen, das heißt bewusst die Mitarbeiter auf ihre erhöhte Aufmerksamkeit und Sorgfalt zu prüfen. Daraus ergeben sich Verbesserungsmaßnahmen und weitere Inhalte für Kommunikationskampagnen.

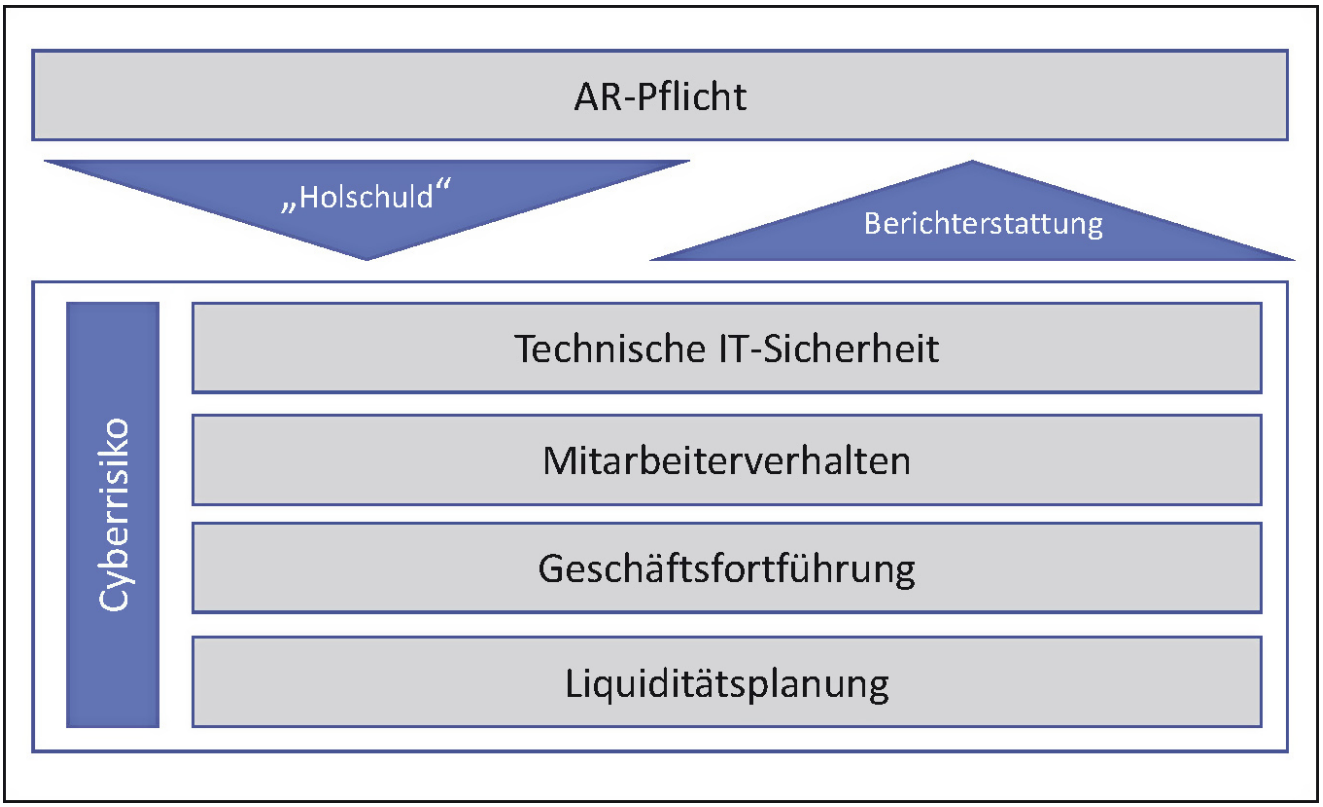

Abb. 1: AR-Pflichten in Bezug auf Cyber-Risiken

Angemessene Schulungsmaßnahmen für alle Mitarbeiter über die Risiken, deren Ausmaß für das Unternehmen und über die vorgegebenen Sicherheitsvorkehrungen sind notwendig, um das Risiko zu minimieren. Für den Aufsichtsrat ist anhand der Anzahl von Schulungen, deren Inhalten und der Teilnehmeranzahl gut nachvollziehbar, wie das Thema in der Organisation lanciert und gelebt wird.

Dementsprechend ist zu empfehlen, bei jeder wirtschaftlichen Nachricht über ein größeres Schadensausmaß bei jeglichem Unternehmen, eine Erklärung der Geschäftsführung zu verlangen, wie ähnliche Risiken konkret in diesem Unternehmen berücksichtigt werden und wie der Stand der Vorbereitung zur Bekämpfung liegt. Im Fall der Cyberkriminalität und der Anstrengungen zu einem sicheren Verhalten der Mitarbeiter ist es sinnvoll, mit der Geschäftsführung jährlich die Anzahl der durchgeführten Schulungen und die Erfolgsquote der Testversuche zu besprechen.

V. Fazit

Zusammenfassend lässt sich daher für das Zusammenspiel zwischen Aufsichtsrat und Geschäftsleitung ableiten:

Bei der Risikoeinschätzung der Cyberkriminalität soll sich der Aufsichtsrat einerseits über die IT-Sicherheit und eine möglichst lückenlose Abwehr von Cyberattacken informieren. Dabei sind sowohl technische Maßnahmen als auch ein sicherheitsbewusstes Verhalten aller Mitarbeiter zu berücksichtigen.

Andererseits geht es um die operative Vorbereitung von Notmaßnahmen bei einem längeren Ausfall der Hardware und Software des Unternehmens (sog. Business Continuity Plan). Im Zusammenhang mit der Sicherstellung des Tagesgeschäfts und der Erstellung der Monats-/Jahresabschlüsse ist die Finanzleitung

weiterhin auf eine richtige und vollständige Darstellung der Umsatzrealisierung und der Kostenerfassung verpflichtet.

Die Mindestanforderungen des Internen Kontrollsystems sind einzuhalten (Nachweis der erbrachten Lieferung und Dienstleistungen, periodengerechte Aufteilung der Kosten,...).

Neben den operativen Geschäftsprozessen deckt der Notfallplan auch die kritischen finanzspezifischen Abläufe ab: Wie werden Auszahlungen gesichert? Wie ist die Liquiditätsplanung durch einen möglichen Verzug der Erstellung von Verkaufsrechnungen und der Kundenzahlungen beeinträchtigt?

Damit ist die Mitwirkung der Finanzleitung bei der Erstellung des Business Continuity Plans unabdingbar. Die Finanzleitung ist auch der Hauptansprechpartner des Aufsichtsrats zur Sicherstellung der Finanzprozesse in diesem Risikoszenario.