By PwC Deutschland | 18. August 2025

Cyberrisiken –Organhaftung und praktische Implikationen für die Geschäftsleitung

Content

Verfasst vonDavid Santa,Dr. Robert Schiller und Dr. Thorsten Ehrhard

A. Digitalisierung als Haftungsfaktor

Die fortschreitende Digitalisierung eröffnet Unternehmen vielfältige Chancen, birgt jedoch zugleich erhebliche Risiken. Insbesondere Cyberangriffe wie Phishing, Ransomware oder gezielte Attacken auf die IT-Infrastruktur stellen eine ernstzunehmende Bedrohung für die wirtschaftliche Integrität von Unternehmen dar. Vor diesem Hintergrund rückt die persönliche Haftung der Geschäftsführung einer GmbH sowie Vorständen einer AG zunehmend in den Fokus. Die Frage, unter welchen Voraussetzungen Organmitglieder für Schäden durch Cyberrisiken persönlich in Anspruch genommen werden können, ist von hoher praktischer Relevanz und wurde jüngst durch die Rechtsprechung weiter konturiert.

Die Haftung von Geschäftsführung und Vorständen ist im Wesentlichen durch die Sorgfaltspflichten nach § 43 GmbHG und § 93 AktG geprägt. Beide Normen verlangen von den Organmitgliedern die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Diese Sorgfaltspflicht erstreckt sich im digitalen Zeitalter nicht mehr nur auf klassische Geschäftsführungsaufgaben, sondern umfasst ausdrücklich auch den Schutz der IT-Infrastruktur, der Unternehmensdaten und der Kommunikationssysteme. Die Geschäftsleitung ist daher verpflichtet, angemessene technische und organisatorische Maßnahmen zur Prävention und Abwehr von Cyberbedrohungen zu implementieren.

B. Sorgfaltspflichten im Bereich der Cybersicherheit

Die Geschäftsleitung ist verpflichtet, ein angemessenes Schutzniveau gegen Cyberrisiken sicherzustellen. Dies umfasst insbesondere:

- Technische Maßnahmen: Implementierung und regelmäßige Aktualisierung von Sicherheitssoftware (z.B. Firewalls, Antivirenprogramme, Verschlüsselungstechnologien), Durchführung von Schwachstellenanalysen und Sicherheitsprüfungen.
- Organisatorische Maßnahmen: Einführung klarer Verantwortlichkeitsstrukturen, Etablierung des Vier-Augen-Prinzips bei Zahlungsanweisungen, regelmäßige Überprüfung und Anpassung interner Prozesse.
- Mitarbeitendenschulungen: Sensibilisierung der Belegschaft für Cyberrisiken, insbesondere im Hinblick auf Phishing und Social Engineering, sowie Schulungen zum sicheren Umgang mit IT-Systemen.
- Notfallmanagement: Entwicklung und Implementierung von Notfallplänen für den Fall eines Cyberangriffs, einschließlich klarer Handlungsanweisungen zur Schadensbegrenzung.

Die Einhaltung dieser Sorgfaltspflichten ist nicht nur aus haftungsrechtlicher Sicht geboten, sondern stellt auch einen wesentlichen Bestandteil eines effektiven Risikomanagements dar.

C. Rechtsprechung

Ein Urteil des OLG Zweibrücken vom 18. August 2022 (Az. 4 U 198/21) hat die Anforderungen an die persönliche Haftung der Geschäftsführung im Zusammenhang mit Cyberangriffen konkretisiert. Im zugrundeliegenden Fall wurde eine Geschäftsführerin einer GmbH nach einem erfolgreichen Phishing-Angriff auf Schadensersatz in Anspruch genommen, nachdem sie auf gefälschte E-Mails hereingefallen war und Überweisungen an Betrüger veranlasst hatte. Das Gericht verneinte jedoch eine persönliche Haftung der Geschäftsführerin. Entscheidend war, dass die streitgegenständlichen Überweisungen als administrative Tätigkeit und nicht als originär organschaftliche Aufgabe eingestuft wurden. Zudem lag lediglich leichte Fahrlässigkeit vor, da die Geschäftsführerin bei der Ausführung der Überweisungen keine weitreichende Entscheidungsfreiheit besaß und der Alleingesellschafter und Mitgeschäftsführer in die Vorgänge eingebunden war.

Das OLG stellte klar, dass eine persönliche Haftung nach § 43 Abs. 2 GmbHG nur bei Verletzung spezifisch organschaftlicher Pflichten in Betracht kommt. Eine Haftung für administrative Fehler im Tagesgeschäft ist demnach nicht ohne Weiteres gegeben. Vielmehr ist eine differenzierte Betrachtung erforderlich, die insbesondere die tatsächlichen Entscheidungsbefugnisse und die innerbetrieblichen Abläufe berücksichtigt.

D. Compliance, Haftungsvermeidung und D&O-Versicherungen

Ein zentrales Element zur Vermeidung persönlicher Haftung ist die Implementierung eines wirksamen Compliance-Management-Systems. IT-Compliance bedeutet, dass das Unternehmen nicht nur gesetzliche Vorgaben, sondern auch interne Richtlinien und Sicherheitsstandards aufstellt, kommuniziert und deren Einhaltung überwacht. Die Dokumentation und regelmäßige Kontrolle dieser Maßnahmen ist im Haftungsfall von entscheidender Bedeutung, da sie belegt, dass die Geschäftsleitung ihren Organisationspflichten nachgekommen ist. Es ist darüber hinaus ratsam, externe Berater wie Rechtsanwälte und Steuerberater in die Planung und Implementierung eines geeigneten Compliance-Management-Systems einzubeziehen. Die Umsetzung durch erfahrende Berater:innen kann bei der Beurteilung darüber, ob die Geschäftsleitung die notwendigen Schritte zur Sicherstellung der Compliance des Unternehmens unternommen hat, ebenfalls berücksichtigt werden.

Zur Absicherung des Haftungsrisikos empfiehlt sich der Abschluss einer D&O-Versicherung (Directors and Officers Liability Insurance). Diese schützt das Privatvermögen der Organmitglieder vor Ansprüchen wegen Pflichtverletzungen im Rahmen ihrer Organstellung. Im Bereich der Cyberrisiken gewinnt daneben die Cyber-Versicherung an Bedeutung, die das Unternehmen selbst gegen Schäden aus Cyberangriffen absichert. Beide Versicherungen ergänzen sich und sollten integraler Bestandteil einer umfassenden Risikostrategie sein.

E. Conclusio

Die Haftung von Geschäftsführung und Vorständen für Schäden durch Cyberrisiken ist ein zentrales Thema

moderner Unternehmensführung. Eine persönliche Haftung tritt nicht automatisch bei jedem Fehlverhalten im Tagesgeschäft ein, sondern es wird eine Verletzung organschaftlicher Pflichten vorausgesetzt. Um Haftungsrisiken zu minimieren, sollten Unternehmen auf ein ganzheitliches Sicherheitskonzept setzen, das technische, organisatorische und personelle Maßnahmen miteinander verknüpft. Die Geschäftsleitung ist gut beraten, die Einhaltung der Sorgfaltspflichten umfassend zu dokumentieren und regelmäßig zu überprüfen. Nur so lässt sich das Risiko persönlicher Inanspruchnahme wirksam begrenzen und die Integrität des Unternehmens im digitalen Zeitalter sichern.

Kontaktieren Sie uns

David Santa

Senior Manager Mannheim
Tel.: +49 621 40069-320
E-Mail:**david.a.santa@pwc.com**

Dr. Robert Schiller

Senior Manager Mannheim
Tel.: +49 151 52157484
E-Mail:**robert.schiller@pwc.com**

Dr. Thorsten Ehrhard

Partner Mannheim
Tel.: +49 151 53959752
E-Mail:**thorsten.ehrhard@pwc.com**

Schlagwörter

Gesetzgebung