DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Handelsrecht

zu § 38 BSIG-RefE des Entwurfs eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Stellungnahme Nr.: 35/2024 Berlin, im Mai 2024

Mitglieder des Ausschusses Handelsrecht

- RA Dr. Marc Löbbe, Frankfurt/Main (Vorsitzender und Berichterstatter)
- RAin Dr. Gabriele Apfelbacher, LL.M., Frankfurt/Main
- RA Prof. Dr. Michael Arnold, Stuttgart (Berichterstatter)
- RA Prof. Dr. Christian Decher, Frankfurt/Main (Berichterstatter)
- RA Dr. Hans Friedrich Gelhausen, Frankfurt/Main
- RAin Dr. Julia Sophia Habbe, Frankfurt/Main
- RAin Dr. Hilke Herchen, Hamburg (Berichterstatter)
- RA Prof. Dr. Hans-Christoph Ihrig, Mannheim (Berichterstatter)
- RA Dr. Thomas Kremer, Düsseldorf
- RA Prof. Dr. Gerd Krieger, Düsseldorf (Berichterstatter)
- RA Prof. Dr. Andreas Pentz, Mannheim
- RAin Dr. Gabriele Roßkopf, LL.M., Stuttgart (Berichterstatter)
- RA Prof. Dr. Frank A. Schäfer, LL.M., Düsseldorf
- RAin Dr. Alexandra Schluck-Amend, Stuttgart
- RA Dr. Bernd Singhof, LL.M., Frankfurt/Main
- RA Prof. Dr. Jochen Vetter, München (Berichterstatter)
- RA Dr. Jost Wiechmann, Hamburg
- RA Prof. Dr. Hans-Ulrich Wilsing, Düsseldorf (Berichterstatter)
- RA Arne Wittig, Frankfurt/Main

Zuständig in der DAV-Geschäftsführung

- RA Max Gröning, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Als Reaktion auf die zunehmende Zahl von Angriffen auf kritische Infrastruktur und Unternehmen im Cyberbereich hat die Europäische Union verschiedene Rechtssetzungsakte erlassen, die die Cybersicherheit in Europa erhöhen sollen. Kernstück ist die NIS-2-Richtlinie ("RL"), die bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden muss. Am 7. Mai 2024 hat das Bundesministerium des Inneren und für Heimat den Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung ("RefE") veröffentlicht. Der RefE erweitert den Anwendungsbereich des Informationssicherheitssicherheitsrechts deutlich über den klassischen Bereich kritischer Infrastruktur hinaus. Mehrere zehntausend Unternehmen in Deutschland werden von der gesetzlichen Neuregelung betroffen sein.

Diese enthält in § 38 BSIG-RefE eine Regelung zu den Pflichten der Geschäftsleiter, die u.a. die Privatautonomie von Unternehmen beim Abschluss von Organhaftungsvergleichen mit Geschäftsleitern erheblich einschränkt. Diese weder durch die RL gebotene noch durch den Schutz kritischer Infrastruktur zu rechtfertigende Einschränkung der Vergleichsmöglichkeiten führt für die betroffenen Unternehmen, die Opfer eines Cyberangriffs geworden sind, zu einer erheblichen Rechtsunsicherheit und konterkariert die mit einem Vergleichsschluss intendierte Rechtssicherheit. Zu dieser Regelung, die im Widerspruch zu allgemein anerkannten Grundsätzen des Gesellschaftsrechts steht, nimmt der DAV vorliegend durch seinen Ausschuss Handelsrecht Stellung: Der DAV hält die Vorschrift, die Art. 20 RL umsetzen soll, insgesamt für entbehrlich, jedenfalls aber für grundlegend überarbeitungsbedürftig:

1. Nach Art. 20 Abs. 1 RL haben die Mitgliedstaaten sicherzustellen, dass die Leitungsorgane besonders wichtiger und wichtiger Einrichtungen die von diesen ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit "billigen und ihre Umsetzung überwachen". § 38 Abs. 1 RefE will diesen RL-Text wiederholen.

   Als besonders wichtige und wichtige Einrichtungen gelten nach der Begriffsdefinition des § 28 Abs. 1 und 2 RefE Unternehmen, die kritische Anlagen betreiben, Anbieter öffentlich zugänglicher Telekommunikationsdienste, öffentlicher Telekommunikationsnetze oder qualifizierte Vertrauensdienstanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter sind. Daneben werden Unternehmen erfasst, die u.a. in den Sektoren bzw. Branchen Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheit, Trinkwasserversorgung und Abwasserbeseitigung, Informationstechnik und Telekommunikation, Weltraum, Abfallbewirtschaftung, Chemie, Lebensmittel, Forschung, Anbieter digitaler Dienste, Medizinprodukte, elektrische Ausrüstungen, elektronische und optische Erzeugnisse, Maschinenbau, Kraftwagen und Kraftwagenteile tätig sind, wobei besondere Schwellenwerte für Mitarbeiter- und Umsatzzahlen sowie Bilanzsumme gelten. Einzelheiten sind in § 28 Abs. 1 und 2 RefE, den Anlagen zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und in dem künftigen KRITIS-Dachgesetz geregelt. Nach der Begründung des RefE geht das BMWK davon aus, dass in Deutschland künftig rund 8.250 Unternehmen als besonders wichtige und rund 21.600 Unternehmen als wichtige Einrichtungen zu klassifizieren sind. Dies verdeutlicht, dass die Regelung neben einer Vielzahl börsennotierter Großunternehmen auch zahlreiche mittelständische Unternehmen erfasst.

   Dass bei Unternehmen sorgfältige Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind und dass es sich dabei um eine so wichtige Aufgabe handelt, dass deren Implementierung und Überwachung zu den Pflichten der Geschäftsleiter selbst gehören, unterliegt keinem Zweifel. Gleichwohl empfiehlt der DAV, § 38 Abs. 1 RefE zu streichen. Die Regelung ist einerseits entbehrlich, weil sich die dort genannten Verpflichtungen bereits aus den Sorgfaltspflichten ergeben, die den Geschäftsleitungsorganen nach allgemeinem Gesellschaftsrecht obliegen (vgl. beispielhaft § 93 Abs. 1 Satz 1 AktG). Sie ist andererseits missweisend, weil

nach allgemeinem Gesellschaftsrecht nicht nur die Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen die genannten Sorgfaltspflichten im Bereich der Cybersicherheit treffen, sondern auch die Geschäftsleiter anderer Unternehmen im Rahmen ihrer allgemeinen Sorgfaltspflichten gehalten sind, für ein angemessenes Risikomanagement im Bereich der Cybersicherheit zu sorgen.

§ 38 Abs. 1 RefE ist deshalb entbehrlich. Wenn der Gesetzgeber die Regelung gleichwohl treffen will, sollte er zumindest im Gesetzestext oder der Begründung klarstellen, dass es sich um eine deklaratorische Regelung handelt, die die allgemeinen gesellschaftsrechtlichen Sorgfaltspflichten der Geschäftsleiter unberührt lässt.

2. In einer Vorgängerfassung des RefE war noch vorgesehen, die "Beauftragung eines Dritten zur Erfüllung der Verpflichtungen" nach Abs. 1 für nicht zulässig zu erklären. Diese durch die RL nicht vorgegebene Regelung ist im RefE entfallen. Dies ist zu begrüßen. In der Begründung des RefE heißt es lediglich, dass auch "bei der Einschaltung von Hilfspersonen…das Leitungsorgan letztverantwortlich" bleibt. Wenn damit gemeint ist, dass Geschäftsleiter ihre Sorgfaltspflichten nicht delegieren, also nicht einen Dritten mit der Erfüllung der Sorgfaltspflichten an ihrer Stelle beauftragen können, wird damit nur eine gesellschaftsrechtliche Selbstverständlichkeit wiedergegeben. Die ursprüngliche Regelung hätte auch so verstanden werden können, dass im Zusammenhang mit der Erfüllung der Pflicht nach Abs. 1 überhaupt keine Dritten beauftragt werden dürften. Das wäre nicht nur sachwidrig. Vielmehr wird für die meisten Geschäftsleiter die Zuziehung sachverständiger Unterstützung bei diesen Aufgaben unumgänglich und durch die allgemeine Sorgfaltspflicht geradezu geboten sein.

3. Zu begrüßen ist auch, dass der RefE anders als seine Vorgängerfassung keine eigenständige Haftungsnorm mehr für Geschäftsleiter vorsieht, welche ihre Pflichten nach Abs. 1 verletzen. Eine solche gesonderte Haftungsregelung hätte zu erheblicher Rechtsunsicherheit geführt, weil das Verhältnis zur gesellschaftsrechtlichen Innenhaftung der Geschäftsleiter unklar gewesen wäre: Es ist ein allgemeiner Grundsatz des Gesellschaftsrechts, dass Geschäftsleiter, die ihre Pflichten verletzen, der Gesellschaft zum Ersatz des daraus entstehenden Schadens

verpflichtet sind. Eine nochmalige spezielle Haftungsregelung ist deshalb entbehrlich und entspricht dem Ansatz, den der Gesetzgeber auch für den Bereich der öffentlichen Verwaltung gewählt hat, wo er ebenfalls auf eigene Haftungsregelungen verzichten und es bei den allgemeinen Vorschriften über die Amtshaftung belassen will.

4. § 38 Abs. 2 Satz 1 RefE will einen Verzicht der Einrichtung auf Schadensersatzansprüche oder einen Vergleich über Ansprüche gegen die Geschäftsleiter wegen der Verletzung ihrer Pflichten nach Abs. 1 für unwirksam erklären, wenn der Vergleich "in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis" steht. Eine Ausnahme soll nach Satz 2 nur dann gelten, wenn der ersatzpflichtige Geschäftsleiter "zahlungsunfähig ist und sich zur Abwendung des Insolvenzplanverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird". Die Vorgängerfassung des RefE hatte sogar noch weitergehend ein generelles Vergleichsverbot vorgesehen.

   Eine solche Regelung ist weder durch die RL geboten noch erscheint sie sachgerecht. Sie würde vielmehr in der Praxis zu erheblichen Rechtsunsicherheiten führen. Schon nach allgemeinem Gesellschaftsrecht sind Verzicht und Vergleich über Schadensersatzansprüche der Gesellschaft gegen ihre Geschäftsleiter eingeschränkt. Insbesondere bedürfen sie der Zustimmung der Gesellschafterversammlung. Im Aktienrecht schränkt § 93 Abs. 4 Satz 3 AktG die Zulässigkeit weiter ein und lässt einen Zustimmungsbeschluss der Hauptversammlung erst nach drei Jahren und nicht gegen den Widerspruch einer 10%-igen Aktienminderheit zu. Das sind ausgewogene Regelungen. Für Schadensersatzansprüche wegen der Verletzung von Sorgfaltspflichten im Bereich der Cybersicherheit gibt es keinen Grund, schärfere Regelungen zu treffen und einen Vergleich oder Verzicht über diese Ansprüche grundsätzlich auszuschließen bzw. einen solchen massiv zu erschweren. Die Regelungen des RefE blenden vielmehr aus, dass es im Einzelfall auch ein hohes Interesse der Gesellschaft geben kann, sich über Ersatzansprüche zu vergleichen oder auf sie zu verzichten.

Die mit Vergleichen bezweckte Rechtssicherheit würde konterkariert, wenn ein Gericht zur Beurteilung der Wirksamkeit eines Vergleichs zunächst die Prozessaussichten eines Schadensersatzanspruchs gegen die Geschäftsleiter umfassend prüfen müsste, um auf dieser Grundlage zu beurteilen, ob die Vergleichssumme aus der Perspektive der Gesellschaft noch in einem angemessenen Verhältnis zu etwaigen Prozessrisiken steht. Dies zu beurteilen ist vielmehr Aufgabe der zuständigen Gesellschaftsorgane und der Gesellschafter. Ein rechtssicherer Abschluss außergerichtlicher Vergleiche wäre auf Grundlage der in § 38 Abs. 2 Satz 1 RefE vorgesehenen Regelung in der Praxis kaum noch möglich. Zudem wäre ungewiss, ob und inwieweit D&O-Versicherer zu substantiellen Zahlungen im Rahmen eines Vergleichs überhaupt noch bereit wären, wenn dieser noch mehrere Jahre nachträglich unter Hinweis auf seine (angebliche) Unangemessenheit in Frage gestellt werden könnte.

Auch stellt sich die Frage, welches Gericht für die Prüfung der Wirksamkeit des Vergleichs zuständig wäre. Da die Gesellschaft, wenn sie mit Zustimmung der Gesellschafter- bzw. Hauptversammlung mit den Geschäftsleitern einen Vergleich geschlossen hat, in der Regel nicht gegen diese vorgehen wird, könnte dies lediglich in der Insolvenz der Gesellschaft im Rahmen des von einem Insolvenzverwalter eingeleiteten Schadensersatzprozesses gegen den Geschäftsleiter oder inzident im Rahmen einer Anfechtungsklage gegen den dem Vergleich zustimmenden Gesellschafter- bzw. Hauptversammlungsbeschluss, eines Klagezulassungsverfahrens nach § 148 AktG oder eines Regressprozesses gegen Aufsichtsratsmitglieder erfolgen, wenn der Aufsichtsrat der Hauptversammlung einen solchen Vergleich vorgeschlagen hat. Gerade bei börsennotierten Gesellschaften würde dies regelmäßig eine erhebliche Rechtsunsicherheit noch für viele Jahre nach dem Vergleichsschluss bedeuten, die der mit dem Vergleich angestrebten Befriedungsfunktion und Rechtssicherheit zuwiderliefe. Letztlich könnten Gesellschaften rechtssicher Vergleiche über Organhaftungsansprüche wegen Verletzung von Sorgfaltspflichten im Bereich der Cybersicherheit wohl nur auf Basis eines gerichtlichen Vergleichsvorschlags und kaum noch außergerichtlich abschließen. Da ein wesentliches Motiv für den Abschluss von Organhaftungsvergleichen neben der Befriedungsfunktion häufig gerade auch in der Verhinderung negativer Folgen für das Unternehmen durch einen öffentlichen

Haftpflichtprozess (beispielsweise bei Drittklagen) liegt, widerspricht die in § 38 Abs. 2 Satz 1 RefE vorgesehen Beschränkung der Vergleichsmöglichkeiten den Interessen des betroffenen Unternehmens. Dies gilt auch und gerade für Unternehmen, die Opfer eines Cyberangriffs geworden sind.

Ein solch massiver Eingriff in die Privatautonomie von Unternehmen ist weder durch die RL geboten noch durch das öffentliche Interesse am Schutz kritischer Infrastruktur vor Cyberangriffen zu rechtfertigen. Auch Art. 20 RL fordert einen solche Beschränkung der Vergleichsmöglichkeiten von Unternehmen nicht. Das räumt auch die Entwurfsbegründung zu § 38 Abs. 2 RefE ausdrücklich ein, meint aber, es würde den Zielen der RL widersprechen, wenn es sich nur um eine disponible Haftung handeln würde. Das ist jedoch nicht zutreffend. Die Regelungen über die Geschäftsleiterhaftung haben einen doppelten Zweck: Sie sollen das Gesellschaftsvermögen schützen und zugleich eine Abschreckungswirkung entfalten, um die Geschäftsleiter zu sorgfältigem Handeln zu veranlassen. Beide Ziele können eine so weitgehende Einschränkung der Vergleichsmöglichkeiten der Unternehmen nicht rechtfertigen. Der Vermögensschutz der Gesellschaft ist nicht Sache des Gesetzgebers, sondern Sache der letztlich betroffenen Gesellschafter. Um die Abschreckungswirkung zu gewährleisten, enthält das AktG die Dreijahresfrist (§ 93 Abs. 4 Satz 3 AktG) und zusätzlich noch einen zwingenden Selbstbehalt bei Abschluss einer D&O-Versicherung (§ 93 Abs. 2 Satz 3 AktG). Angesichts der hohen Bedeutung der Cybersicherheit bei besonders wichtigen und wichtigen Einrichtungen mag man erwägen, dieses Konzept auf Schadensersatzansprüche wegen unzureichender Risikomanagementmaßnahmen im Bereich der Cybersicherheit auch auf andere Rechtsformen zu übertragen. Jedenfalls mit diesen Einschränkungen erzeugt die Haftungsgefahr aber auch dann hinreichende Abschreckungswirkung, wenn das Gesetz es zulässt, im Nachhinein auf den Anspruch zu verzichten oder sich über ihn zu vergleichen.

5. § 38 Abs. 3 RefE schließlich will in Ausführung von Art. 20 Abs. 2 RL den Geschäftsleitern besonders wichtiger und wichtiger Einrichtungen Schulungspflichten auferlegen. Nach der Begründung des RefE sollen solche Schulungen mindestens alle drei Jahre angeboten werden. Auch das scheint dem DAV eine letztlich entbehrliche Regelung, da sich auch angemessene Schulungspflichten bereits aus

den allgemeinen Sorgfaltspflichten der Geschäftsleiter ergeben. Wenn man die Regelung gleichwohl beibehalten will, müsste man jedenfalls auch hier klarstellen, dass die allgemeinen gesellschaftsrechtlichen Sorgfaltspflichten durch sie nicht berührt werden. Andernfalls würde auch diese Regelung die Frage aufwerfen, ob Geschäftsleiter anderer als besonders wichtiger und wichtiger Einrichtungen im Gegenschluss von entsprechenden Schulungspflichten befreit wären.

Unklar erscheint aufgrund von § 38 Abs. 3 RefE auch, ob die Schulungspflicht jeden einzelnen Geschäftsleiter persönlich trifft oder ob diese Pflicht innerhalb des Geschäftsleitungsorgans auf das für Cybersicherheit zuständige Mitglied delegiert werden kann. Sachgerecht wäre allein letzteres, da eine Arbeitsteilung innerhalb der Geschäftsleitungsorgane grundsätzlich zulässig und im Interesse einer effektiven Aufgabenwahrnehmung regelmäßig auch sinnvoll erscheint. Dass dies auch im Rahmen von § 38 Abs. 3 RefE möglich ist, sollte daher zumindest in der Gesetzesbegründung klargestellt werden. Eine gewisse Hürde könnte hier auf den ersten Blick Art. 20 Abs. 2 RL bilden, der davon spricht, dass die Mitgliedstaaten sicherzustellen haben, dass "die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen". Allerdings spricht der Richtlinienwortlaut auch nicht von "allen" Mitgliedern der Leitungsorgane und die RL lässt auch nicht erkennen, dass sie in diesem Zusammenhang anerkannte Grundsätze innerorganschaftlicher Arbeitsteilung in Frage stellen wollte.

Verteiler

- Bundeministerium des Innern und für Heimat
- Bundesministerium der Justiz
- Bundesministerium für Wirtschaft und Klimaschutz
- Bundesministerium für Finanzen

- Fraktionen im Deutschen Bundestag
- Ausschuss für Recht im Deutschen Bundestag
- Ausschuss für Wirtschaft im Deutschen Bundestag
- Ausschuss für Finanzen im Deutschen Bundestag
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Wirtschaft der im Deutschen Bundestag vertretenen Parteien

- Justizministerien und -senatsverwaltungen der Länder
- Wirtschaftsministerien der Länder

- Regierungskommission Deutscher Corporate Governance Kodex
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
- Europäische Kommission - Vertretung in Deutschland

- Vorstand und Geschäftsführung des Deutschen Anwaltvereins
- Landesgruppen und -verbände des DAV
- Vorsitzende der Gesetzgebungsausschüsse des DAV
- Vorsitzende der Arbeitsgemeinschaften des DAV
- Handelsrechtsausschuss des DAV

- Bundesrechtsanwaltskammer
- Bundesnotarkammer
- Deutscher Notarverein
- Institut der Wirtschaftsprüfer (IdW)
- Deutscher Richterbund
- Deutsche Schutzvereinigung für Wertpapierbesitz (DSW)
- Deutscher Steuerberaterverband
- Bundesverband der Deutschen Industrie (BDI)
- Deutscher Industrie- und Handelskammertag (DIHK)
- Gesamtverband der Deutschen Versicherungswirtschaft
- Bundesverband Deutscher Banken
- Schutzgemeinschaft der Kapitalanleger e.V. (SdK)

Presse:

- Die Aktiengesellschaft
- GmbH-Rundschau
- NZG Neue Zeitschrift für Gesellschaftsrecht
- WM Wertpapiermitteilungen
- ZIP Zeitschrift für Wirtschaftsrecht
- Börsenzeitung
- Handelsblatt
- Frankfurter Allgemeine Zeitung
- Juris

- GfK
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Legal tribune online
- NJW