Deutsches Aktieninstitut
Kapital. Markt. Kompetenz.

Cybersecurity stärken – aber mit Augenmaß

An klaren Verantwortungsbereichen festhalten

Entwurf eines Gesetzes zur Umsetzung der NIS-2 Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 8. September 2025

Einleitung

Am 8. September 2025 hat die Bundesregierung den Regierungsentwurf für ein Gesetz zur Umsetzung der NIS-2 Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vorgelegt. Damit wird der bereits bestehende Rechtsrahmen[1] ergänzt und auf weitere Unternehmen ausgeweitet.

Diese Stellungnahme bezieht sich ausschließlich auf die Pflicht der Geschäftsleitungen zur regelmäßigen Schulung, wie sie in § 38 Abs. 3 BSIG-E[2] vorgegeben wird. Diese Schulungspflicht geht über das notwendige Maß hinaus, wie ein Blick in die Verteilung von Haftung und Verantwortung zeigt.

Das Deutsche Aktieninstitut regt an, die Schulungspflicht für die Geschäftsleitungen bei börsennotierten Unternehmen auf das Vorstandsmitglied zu beschränken, in dessen Verantwortungsbereich die Cybersecurity fällt.

1 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122).

2 Gesetzesentwurf über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz-E – BSIG-E).

1 Haftung des Vorstands

Die Verpflichtung der Geschäftsleitungen zur regelmäßigen Teilnahme an Schulungen betrifft in börsennotierten Unternehmen den Vorstand. Grundsätzlich ist jedes Vorstandsmitglied für die gesamte Geschäftsleitung verantwortlich (§ 76 Abs. 1 AktG). Zum Tragen kommt die Gesamtverantwortung insbesondere in Situationen und bei Entscheidungen, die Auswirkungen auf die gesamte Gesellschaft und ihre zukünftige Entwicklung haben. Dazu zählen unter anderem Entscheidungen über Verkäufe von Unternehmensteilen, Übernahmen von Unternehmen und die Fusion mit einem anderen Unternehmen. Mit Blick auf die erheblichen Folgen einer erfolgreichen Cyberattacke für das gesamte Unternehmen kann davon ausgegangen werden, dass auch grundlegende Entscheidungen zur Resilienz und Wehrhaftigkeit in die Gesamtverantwortung des Vorstands fallen.

2 Verantwortung des Vorstands

Allerdings greift die bloße Betrachtung der formalen Haftung des Vorstands zu kurz. Vielmehr ist die Ressortaufteilung zu berücksichtigen. In der Regel werden durch eine interne Geschäftsverteilung spezifische Aufgabenbereiche des Gesamtvorstands wie Finanzen, Personal oder Cybersecurity einzelnen Vorstandsmitgliedern zugewiesen.

In diesem Fall übernimmt das jeweilige Vorstandsmitglied die volle Verantwortung für sein Ressort. Davon sind im Wesentlichen die Aufsichts-, Organisations- und Berichtspflichten umfasst. Daraus folgt, dass die Vorstandsmitglieder nicht direkt für die Pflichten innerhalb der Ressorts der anderen Vorstandsmitglieder verantwortlich sind. Das Minus an Verantwortung geht einher mit einem Mehr an Kontroll- und Überwachungspflichten hinsichtlich der Vorstandskollegen, bis hin zu einer Haftung für Fehler in fremden Ressorts, wenn die Vorstände diese Kontroll- und Überwachungspflichten verletzen.

Die Kontroll- und Überwachungspflichten finden ihren Ausgleich in einer Berichtspflicht des ressortverantwortlichen Vorstandsmitglieds gegenüber den ressortfremden Vorstandsmitgliedern über die Vorgänge im eigenen Ressort. Die Berichtspflicht hängt maßgeblich von der Art, Größe und Struktur des Unternehmens sowie der Bedeutung des Ressorts für das Unternehmen ab.

Wie das Informationssystem ausgestaltet wird, liegt im Ermessen des Vorstands. In der Praxis berichten die Vorstandsmitglieder in den Vorstandssitzungen über die wichtigsten Vorgänge in ihrem Bereich. Zeigen Berichte des zuständigen

Vorstandsmitglieds keine Unregelmäßigkeiten auf, können die ressortfremden Vorstandsmitglieder davon ausgehen, dass die Geschäfte ordnungsgemäß ablaufen.[3]

3 Konsequenz

Wie gezeigt, führt der Grundsatz der Gesamtverantwortung zu einer umfassenden Haftung jedes einzelnen Vorstandsmitglieds. Der gängigen Praxis der Ressortaufteilung folgt zwar in beschränktem Maße eine Verantwortungsbegrenzung zwischen den Vorstandsmitgliedern, die auch eine zumindest teilweise Haftungsbegrenzung nach sich ziehen kann. Aber selbst bei Delegation von Pflichten und Aufteilung von Zuständigkeiten verbleibt eine ausreichende Resthaftung, denn jedes Vorstandsmitglied hat die Tätigkeit der Vorstandkollegen zu überwachen und bei Hinweisen auf Missstände tätig zu werden.

Angesichts dieses ausbalancierten Haftungs- und Verantwortungsgefüges erscheint es nicht erforderlich, die Schulungspflicht auf die ressortfremden Vorstandsmitglieder auszuweiten. Die Schulungspflicht für das ressortverantwortliche Vorstandsmitglied genügt.

[3] BGH, 1 StR 280/99 vom 6. April 2000.

Kontakt

Klaus-Dieter Sohn
Chefjustiziar und Leiter Organisation
Telefon +49 69 92915-61
sohn@dai.de

Büro Frankfurt:
Deutsches Aktieninstitut e.V.
Senckenberganlage 28
60325 Frankfurt am Main

EU-Verbindungsbüro:
Deutsches Aktieninstitut e.V.
Rue Marie de Bourgogne 58
1000 Brüssel

Hauptstadtbüro:
Deutsches Aktieninstitut e.V.
Behrenstraße 73
10117 Berlin

Lobbyregister Deutscher Bundestag: R000613
EU-Transparenzregister: 38064081304-25
www.dai.de

Das Deutsche Aktieninstitut setzt sich für einen starken Kapitalmarkt ein, damit sich Unternehmen gut finanzieren und ihren Beitrag zum Wohlstand der Gesellschaft leisten können.

Unsere Mitgliedsunternehmen repräsentieren rund 90 Prozent der Marktkapitalisierung deutscher börsennotierter Aktiengesellschaften. Wir vertreten sie im Dialog mit der Politik und bringen ihre Positionen über unser Hauptstadtbüro in Berlin und unser EU-Verbindungsbüro in Brüssel in die Gesetzgebungsprozesse ein.

Als Denkfabrik liefern wir Fakten für führende Köpfe und setzen kapitalmarktpolitische Impulse. Denn von einem starken Kapitalmarkt profitieren Unternehmen, Anleger und Gesellschaft.