

01.26

ZCG

Zeitschrift für
Corporate Governance

21. Jahrgang
Februar 2026
Seiten 1 – 52

www.ZCGdigital.de

Leitung und Überwachung in der Unternehmens- und Prüfungspraxis

Fachbeirat:

Prof. Dr. Alexander Bassen,
Universität Hamburg

Prof. Dr. Dr. h. c. Theodor Baums,
Johann Wolfgang Goethe-Universität
Frankfurt am Main

Prof. Dr. Thomas Berndt,
Universität St. Gallen

WP/StB Prof. Dr. Manfred Bolin,
International School of Management,
Dortmund

Prof. Dr. Gerrit Brösel,
FernUniversität in Hagen

Prof. Dr. Henning Herzog,
QIRM Institut für Regulation &
Management e.G.

Ulrich Hocker, Hauptgeschäftsführer
Deutsche Schutzvereinigung für
Wertpapierbesitz e. V.

Prof. Dr. Anja Hucke, Universität Rostock

Prof. Dr. Annette G. Köhler,
Universität Duisburg-Essen

Prof. Dr. Stefan Müller, Helmut Schmidt
Universität Hamburg

Henriette Peucker,
Geschäftsführende Vorständin
Deutsches Aktieninstitut e. V.

Prof. Dr. Patrick Velte,
Leuphana Universität Lüneburg

Prof. Dr. Axel von Werder,
Technische Universität Berlin

WP/StB Prof. Dr. Norbert Winkeljohann,
Norbert Winkeljohann Advisory &
Investments

Prof. Dr. Henning Zülch,
Handelshochschule Leipzig (HHL)

ZCG

Management

Diversität im Vorstand

[Schöning, 5]

ZCG

Recht

Cybersicherheit als Risiko und Governance-Pflicht

[Hessel, 11]

Organhaftung und D&O-Deckung

bei Insolvenzverschleppung

[Needham/Müller, 16]

ZCG

Prüfung

Qualität der Abschlussprüfung

[Quick/Álvarez Jiménez/Sánchez Toledano/

Sánchez Toledano, 21]

ZCG

Rechnungs- legung

Bilanzpolitische Gestaltungsspielräume

in der Kapitalflussrechnung

[Babel, 29]

Dieselgate-Kommunikation von Automobil-

herstellern

[Jabs/Wulf/Pfeifer, 35]

Omnibus I

[Baumüller, 40]

Cybersicherheit als Risiko und Governance-Pflicht

Gesetzliche Anforderungen und haftungsrelevante Risiken für Unternehmensleitung und Aufsichtsgremien

Stefan Hessel

Der vorliegende Beitrag zeigt auf, wie die NIS-2-Richtlinie und der Cyber Resilience Act als neue gesetzliche Anforderungen an Cybersicherheit in die Risikoberichterstattung eingebunden werden können und welche Risiken bei Verstößen drohen. Ziel ist es, Unternehmensleitung, Aufsichtsgremien, Prüferinnen und Prüfer dabei zu unterstützen, die neuen Anforderungen im Sinne einer anforderungsgerechten Corporate Governance zu erfüllen.

1. Cybersicherheit als Risikofeld

Vor dem Hintergrund zunehmender praktischer, aber vor allem auch regulatorischer Anforderungen, gewinnt Cybersicherheit als eigenständiges Risikofeld besondere Bedeutung. Die gesetzlichen Vorgaben enthalten verbindliche technische und organisatorische Maßnahmen, die unmittelbar in das Risikomanagementsystem eines Unternehmens integriert werden müssen. Verstöße gegen diese Anforderungen können Bußgelder und Schadensersatzansprüche nach sich ziehen, Reputationsschäden verursachen und persönliche Haftungsrisiken für Organmitglieder bedeuten. Cybersicherheit (Tabelle 1) ist somit kein rein technisches Thema, sondern auch wesentlicher Bestandteil einer wirksamen Unternehmensüberwachung und Risikosteuerung. Im Folgenden werden die neuen gesetzlichen Anforderungen an die Cybersicherheit einschließlich der wichtigsten Begriffe (Kapitel 2) erläutert und die Konsequenzen von Verstößen (Kapitel 3) dargestellt. Abschließend werden konkrete Handlungsempfehlungen für Unternehmensleitung und Aufsichtsorgane gegeben (Kapitel 4).

2. Cybersicherheitsrechtliche Anforderungen

Ziel des Cybersicherheitsrechts ist der Schutz von Netz- und Informationssysteme vor Cyberbedrohungen. Auf europäischer Ebene regeln der Cyber Resilience Act¹ (CRA) und die NIS-2-Richtlinie² (NIS-2-RL) zwei komplementäre Regelungsebenen:

- ▶ Der CRA legt produktbezogene Cybersicherheitsanforderungen fest.
- ▶ Die NIS-2-Richtlinie normiert i. V. m. dem jeweiligen nationalen Umsetzungsgesetz der Mitgliedstaaten unternehmensbezogene Pflichten zur Gewährleistung eines angemessenen Informationssicherheitsniveaus.

2.1 Cyber Resilience Act

Der CRA etabliert einen sektorübergreifenden Rechtsrahmen für Cybersicherheit von Produkten mit digitalen Elementen. Die Verordnung gilt unmittelbar in allen

Cybersicherheit umfasst alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.³

Cyberbedrohung bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzerinnen und Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.⁴

Netz- und Informationssysteme sind

- a) ein elektronisches Kommunikationsnetz im Sinne des Art. 2 Nr. 1 EECC-Richtlinie (EU) 2018/1972,
- b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
- c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.⁵

Tabelle 1: Cybersicherheit, Cyberbedrohung, Netz- und Informationssysteme

Mitgliedstaaten der EU und wird schrittweise bis zum 11.12.2027 eingeführt.

2.1.1 Anwendungsbereich

Der CRA adressiert Hersteller, Importeure und Händler von Produkten (Tabelle 2) mit digitalen Elementen.⁶ Ein Produkt mit digitalen Elementen ist ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungs-lösungen, einschließlich Software- oder Hardwarekomponen-

3 Art. 3 Nr. 3 CRA bzw. Art. 6 Nr. 3 NIS-2-RL i. V. m. Art. 2 Nr. 1 Verordnung (EU) 2019/881.

4 Art. 3 Nr. 46 CRA bzw. Art. 6 Nr. 10 NIS-2-RL i. V. m. Art. 2 Nr. 8 Verordnung (EU) 2019/881.

5 Art. 2 Nr. 2 NIS-2-RL i. V. m. Art. 4 Nr. 1 Richtlinie (EU) 2016/1148.

6 Art. 2, 13, 19, 20 CRA.

Stefan Hessel

Rechtsanwalt, LL.M., Partner und Head of Digital Business bei der Wirtschaftskanzlei Reuschlaw, Kontakt: stefan.hessel@reuschlaw.de

1 Verordnung (EU) 2024/2847.

2 Richtlinie (EU) 2022/255.

► Durch den CRA werden neue Anforderungen an die Produktsicherheit gestellt. ◀

ten, die getrennt in Verkehr gebracht werden sollen.⁷

Nach dem Marktortprinzip unterfällt jedes Produkt mit digitalen Elementen, das im Rahmen einer gewerblichen Tätigkeit auf dem EU-Markt zum Vertrieb oder zur Nutzung in Verkehr gebracht wird, dem CRA. Der Anwendungsbereich sieht u. a. Ausnahmen für Medizinprodukte und digitale Produkte für die nationale Sicherheit oder militärische Zwecke vor.⁸

Der CRA unterteilt die betroffenen Produkte in verschiedene Kategorien. Produkte mit digitalen Elementen⁹ stellen nach Angaben der EU-Kommission den Großteil der betroffenen Produkte dar.¹⁰ Die restlichen 10 % sind „wichtige Produkte mit digitalen Elementen“¹¹ und „kritische Produkte mit digitalen Elementen“¹².

2.1.2 Wesentliche Pflichten der Hersteller, Einführer und Händler

Die Wirtschaftsakteure treffen entlang der Lieferkette abgestufte Pflichten zur Gewährleistung der Cybersicherheit der betroffenen Produkte.

Durch den CRA werden neue Anforderungen an die Produktsicherheit gestellt. Hersteller müssen nach Art. 13 Abs. 1 CRA beim Inverkehrbringen des Produkts gewährleisten, dass das Produkt gem. den grundlegenden Anforderungen in Anhang I Teil I CRA konzipiert, entwickelt und hergestellt worden ist. Danach müssen Produkte ohne bekannte Schwachstellen hergestellt werden und über automatische Sicherheitsupdates, eine sichere Standardkonfiguration und geeignete Kontrollmechanismen zum Schutz vor unbefugtem Zugriff verfügen. Hersteller müssen darüber hinaus nach Art. 13 Abs. 8 CRA während der erwarteten Produktlebensdauer und während des Unter-

Hersteller ist eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, monetarisiert oder unentgeltlich.¹³

Bevollmächtigter ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die von einem Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben wahrzunehmen.¹⁴

Einführer ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in Verkehr bringt.¹⁵

Händler ist eine natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem EU-Markt bereitstellt, mit Ausnahme des Herstellers oder des Einführers.¹⁶

Quasi-Hersteller ist eine natürliche oder juristische Person, bei der es sich nicht um den Hersteller, Einführer oder Händler handelt und die eine wesentliche Änderung an dem Produkt mit digitalen Elementen vornimmt und das Produkt auf den Markt bringt.

Tabelle 2: Hersteller, Bevollmächtigter, Einführer, Händler, Quasi-Hersteller

stützungszeitraums sicherstellen, dass Schwachstellen des Produkts nach den grundlegenden Anforderungen in Anhang I Teil II CRA behandelt werden. Zu den weiteren Pflichten des Herstellers gehört die Bewertung von Cyberrisiken vor der Markteinführung und die Überwachung des Produkts für die gesamte Lebensdauer.¹⁷

Einführer und Händler unterfallen nachgelagerten Pflichten. Sie müssen sicherstellen, dass die Produkte mit digitalen Elementen den Sicherheitsanforderungen genügen, das Konformitätsbewertungsverfahren durchlaufen haben und die relevanten Dokumentationen und dass Nachweise vorhanden sind.¹⁸

2.1.3 Konformitätsbewertung

Die Konformitätsbewertung dient dem Nachweis der Erfüllung der grundlegenden Cybersicherheitsanforderungen aus Anhang I Teil I CRA durch das Produkt mit digitalen Elementen und dem Nachweis der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen aus Anhang I Teil II CRA. Je nach Kritikalität des Produkts mit digitalen Elementen (normal/wichtig/kritisch) gelten unterschiedliche Anforderungen an das Konformitätsbewertungsverfahren.¹⁹ Es kann entweder als internes Kontrollverfahren, als EU-Baumusterprüfverfahren und Konformität mit dem EU-Baumuster, als externe Konformitätsbewertung auf Grundlage einer umfassenden Qualitätssicherung oder als Europäisches Zertifizierungsschema für Cybersicherheit durchgeführt werden.

2.1.4 Meldepflichten

Die Meldepflichten für Hersteller werden in Art. 14 CRA vorgegeben. Danach müssen Hersteller jede aktiv ausgenutzte Schwachstelle und jeden schwerwiegenden Vorfall (Tabelle 3), der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt und von dem sie Kenntnis erlangen, der zuständigen Aufsichtsbehörde melden.

Der CRA sieht ein abgestuftes Meldesystem mit entsprechenden Fristen vor. Eine Frühwarnung hat unverzüglich, jedenfalls aber innerhalb von 24 Stunden zu erfolgen. Innerhalb von 72 Stunden müssen zudem allgemeine Informationen über das Produkt mit digitalen Elementen, über die Art der Ausnutzung der betreffenden Schwachstelle bzw. des Vorfalls sowie über ergriffene Korrektur- oder Risikominderungsmaßnahmen übermittelt werden. Spätestens nach 14 Tagen muss dann ein Abschlussbericht mit weiterführenden Informationen vorgelegt werden.

7 Art. 3 Nr. 1 CRA.

8 Art. 2 Abs. 2 und 5 CRA.

9 Art. 6 CRA.

10 Europäische Kommission, Cyber Resilience Act – Impact assessment, 15.9.2022, <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment> (Abruf: 25.11.2025).

11 Art. 7 CRA.

12 Art. 8 CRA.

13 Art. 3 Nr. 13 CRA.

14 Art. 3 Nr. 15 CRA.

15 Art. 3 Nr. 16 CRA.

16 Art. 3 Nr. 17 CRA.

17 Art. 13 Abs. 2 und 3 CRA.

18 Art. 19, 20 CRA.

19 Art. 32 CRA.

► Die NIS-2-Richtlinie verpflichtet bestimmte Einrichtungen zur Implementierung geeigneter und verhältnismäßiger technischer, organisatorischer und operativer Maßnahmen. ◀

Eine **Schwachstelle** ist eine Schwäche, Anfälligkeit oder Fehlfunktion eines Produkts mit digitalen Elementen, die bei einer Cyberbedrohung ausgenutzt werden kann.²⁰

Eine **aktiv ausgenutzte Schwachstelle** ist eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat.²¹

Ein **Sicherheitsvorfall** ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt.²²

Ein **Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen** ist ein Sicherheitsvorfall, der sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen.²³

Tabelle 3: Schwachstelle, Sicherheitsvorfall

2.2 NIS-2-Richtlinie

Die NIS-2-Richtlinie verpflichtet bestimmte Einrichtungen zur Implementierung geeigneter und verhältnismäßiger technischer, organisatorischer und operativer Maßnahmen. Die Richtlinie wurde am 27.12.2022 im EU-Amtsblatt veröffentlicht und sollte von den Mitgliedstaaten bis zum 17.10.2024 in nationales Recht umgesetzt werden. Ein Großteil der Mitgliedstaaten hat diese Umsetzungsfrist jedoch nicht eingehalten, weshalb die EU-Kommission mehrere Vertragsverletzungsverfahren eingeleitet hat.²⁴ In Deutschland wurde das NIS-2-Umsetzungsgesetz am 5.12.2025 im Bundesgesetzblatt verkündet und ist, einen Tag später, am 6.12.2025 ohne Übergangsfrist in Kraft getreten.²⁵

20 Art. 3 Nr. 40 CRA.

21 Art. 3 Nr. 42 CRA.

22 Art. 3 Nr. 43 CRA i.V.m. Art. 6 Nr. 6 NIS-2-RL.

23 Art. 3 Nr. 44 CRA.

24 Europäische Kommission, Cybersicherheit und Resilienz kritischer Einrichtungen: Vertragsverletzungsverfahren gegen Deutschland und weitere Mitgliedstaaten, 28.11.2024, https://germany.representation.ec.europa.eu/news/cybersicherheit-und-resilienz-kritischer-einrichtungen-vertragsverletzungsverfahren-gegen-2024-11-28_de (Abruf: 25.11.2025).

25 BGBl. 2025 I Nr. 301 vom 5.12.2025, <https://www.recht.bund.de/bgbl/1/2025/301/VO.html> (Abruf: 5.12.2025).

2.2.1 Anwendungsbereich

Anknüpfungspunkt der NIS-2-Richtlinie ist der Begriff der Einrichtung, wobei Adressat der unternehmensbezogenen Pflichten stets die juristische Person ist. Eine Einrichtung ist eine natürliche oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann.²⁶

Voraussetzung für eine Anwendbarkeit ist, dass die Einrichtung ihre Dienste in der EU erbringt oder ihre Tätigkeit in der EU ausübt.²⁷ Darüber hinaus muss die Einrichtung grundsätzlich den Schwellenwert eines mittleren Unternehmens der Empfehlung 2003/361/EG der Europäischen Kommission erreichen.²⁸ Nach dieser Size-Cap-Rule muss die Einrichtung mindestens 50 Beschäftigte haben oder einen Jahresumsatz von 10 Mio. Euro und eine Jahresbilanzsumme von 10 Mio. Euro aufweisen. Nach Art. 2 Abs. 2 NIS-2-RL kann die Richtlinie auch unabhängig von der Größe Anwendung finden. Über die räumliche Anwendbarkeit und die Size-Cap-Rule hinaus muss die Einrichtung einem der in den Anhängen I oder II der NIS-2-Richtlinie genannten 18 Wirtschaftssektoren unterfallen.

Die Einrichtungen werden in wesentliche und wichtige Einrichtungen klassifiziert. Eine wesentliche Einrichtung ist eine Einrichtung der in Anhang I genannten Art (Sektoren mit hoher Kritikalität), wenn diese die Schwellenwerte eines großen Unternehmens der Empfehlung 2003/361/EG der Europäischen Kommission erreicht.²⁹ Dies ist der Fall, wenn das Unternehmen mindestens 250 Beschäftigte oder einen Jahresumsatz von mehr als 50 Mio. Euro und eine Jahresbilanzsumme von mehr als 43 Mio. Euro aufweist. Eine wichtige Einrichtung ist ein Unternehmen der in Anhang I oder II aufgeführten Art (sonstige kritische Sektoren), das nicht als wesentliche Einrichtung gilt.³⁰

26 Art. 6 Nr. 38 NIS-2-RL.

27 Art. 2 Abs. 1 NIS-2-RL.

28 Art. 2 Abs. 1 NIS-2-RL.

29 Art. 3 Abs. 1 NIS-2-RL.

30 Art. 3 Abs. 2 NIS-2-RL.

Das deutsche NIS-2-Umsetzungsgesetz sieht in § 28 Abs. 3 BSIG (neu) eine von der NIS-2-Richtlinie abweichende Regelung zu Nebentätigkeiten vor. Obwohl es keinen Rückhalt für eine entsprechende Regelung in der NIS-2-Richtlinie gibt, hat der deutsche Gesetzgeber entschieden, dass geringfügige Nebentätigkeiten nicht zu einer Einstufung als besonders wichtige (d. h. wesentliche) oder wichtige Einrichtung führen sollen. Eine Einstufung als vernachlässigbare Nebentätigkeit ist möglich, wenn die folgenden Voraussetzungen erfüllt sind:

- **Nebentätigkeit:** Es muss sich um eine Nebentätigkeit handeln. Die Haupttätigkeiten eines Unternehmens sind nie vernachlässigbar. Dies gilt insbesondere für Tätigkeiten, die in einer Satzung oder einem vergleichbaren Dokument genannt werden.
- **Geringfügigkeit:** Überschreitet eine Nebentätigkeit für sich genommen die Schwellenwerte für mittlere Unternehmen (mindestens 50 Beschäftigte oder ein Jahresumsatz und eine Jahresbilanz von über 10 Mio. Euro), ist die Tätigkeit nicht vernachlässigbar.
- **Verhältnismäßigkeit:** Dass eine geringfügige Nebentätigkeit vorliegt, ist für sich genommen nicht ausreichend. Vielmehr muss geprüft werden, ob durch das Vorliegen einer geringfügigen Tätigkeit eine unverhältnismäßige Regulierung entsteht. Dies ist insbesondere dann nicht der Fall, wenn von der Tätigkeit ein relevantes Risiko für die Cybersicherheit ausgeht.

2.2.2 Governance und Haftung

Durch die NIS-2-Richtlinie wird die Cybersicherheit zur Cheffinnen- und Chefsache. Leitungsorgane einer betroffenen Einrichtung werden ausdrücklich in die Pflicht genommen. Sie müssen die ergriffenen Risikomanagementmaßnahmen billigen, deren Umsetzung überwachen und an Schulungen zur Cybersicherheit teilnehmen.³¹ Zudem haften die Leitungsorgane persönlich bei Verstößen gegen ihre Managementpflichten entsprechend der gesetzlichen Vorschriften

31 Art. 20 Abs. 1 und 2 NIS-2-RL.

des nationalen Rechts.³² Nach Art. 32 Abs. 5 lit. b NIS-2-RL ist ebenfalls ein vorübergehender Ausschluss der Leitungsorgane möglich.

2.2.3 Risikomanagementmaßnahmen

Nach Art. 21 NIS-2-Richtlinie müssen die betroffenen Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten. Die konkrete Auswahl der Risikomanagementmaßnahmen hat unter Berücksichtigung des Stands der Technik und auf Grundlage einer Verhältnismäßigkeitsprüfung zu erfolgen.

Daneben enthält Art. 21 Abs. 2 NIS-2-RL einen Katalog an Maßnahmen, die Unternehmen mindestens ergreifen müssen. Dazu gehören Konzepte in Bezug auf die Risikoanalyse, die Bewältigung von Sicherheitsvorfällen, die Aufrechterhaltung des Betriebs, die Sicherheit der Lieferkette, grundlegende Verfahren im Bereich der Cyberhygiene, Konzepte und Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung, Konzepte für die Zugriffskontrolle und das Management von Anlagen, ggf. auch gesicherte Notfallkommunikationssysteme.

2.2.4 Berichtspflichten und -fristen

Nach Art. 23 NIS-2-RL muss bei erheblichen Sicherheitsvorfällen unverzüglich die Aufsichtsbehörde informiert werden. Ein erheblicher Sicherheitsvorfall liegt vor, wenn

- ▶ er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
- ▶ er andere natürliche oder juristische Personen durch erhebliche materielle

oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.³³

Die NIS-2-Richtlinie sieht ein mehrstufiges Meldesystem mit bis zu fünf Berichten pro Vorfall vor. Die Frühwarnung muss unverzüglich bzw. spätestens 24 Stunden nach Kenntnis erfolgen. Nach 72 Stunden haben eine Aktualisierung der Frühwarnung und eine erste Bewertung des Sicherheitsvorfalls zu erfolgen. Ggf. ist ein Zwischenbericht vorzulegen. Schließlich ist spätestens nach einem Monat ein Abschlussbericht vorzulegen. Daneben sieht Art. 23 Abs. 2 NIS-2-RL eine Pflicht vor, den Empfängern der Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitzuteilen, die diese auf die Bedrohung hin ergreifen können.

3. Risiken für Unternehmen

Verstöße gegen die gesetzlichen Bestimmungen zur Cybersicherheit können Konsequenzen wie Behördenmaßnahmen, empfindliche Geldbußen und Schadensersatzforderungen nach sich ziehen.

3.1 Behördenmaßnahmen

3.1.1 Cyber Resilience Act

Zur wirksamen Durchsetzung der Vorschriften des CRA bestimmt jeder Mitgliedstaat eine oder mehrerer Marktüberwachungsbehörden.³⁴ Den Marktüberwachungsbehörden ist Zugang zu den Daten zu gewähren, die für die Bewertung der Konzeption, Entwicklung, Herstellung und Behandlung von Schwachstellen erforderlich sind, einschließlich der betreffenden internen Unterlagen.³⁵ Zudem können die Marktüberwachungsbehörden eine Anordnungsverfügung treffen, innerhalb einer angemessenen Frist alle geeigneten Korrekturmaßnahmen zu ergreifen, um die Konformität des Produkts herzustellen, das Produkt vom Markt zu nehmen oder es zurückzurufen.³⁶ Schließlich können diese auch die Bereitstellung des Produkts auf dem Markt untersagen oder einschränken, so-

▶ Die NIS-2-Richtlinie sieht ein mehrstufiges Meldesystem mit bis zu fünf Berichten pro Vorfall vor. ◀

wie das Produkt vom Markt zurücknehmen oder zurückrufen.³⁷

3.1.2 NIS-2-Richtlinie

Die NIS-2-Richtlinie enthält ebenfalls einen umfangreichen Katalog von Überwachungs- und Durchsetzungsmaßnahmen, die nationale Behörden ergreifen können. In Deutschland ist die zuständige nationale Behörde das Bundesamt für Sicherheit in der Informationstechnik (BSI). Bei wesentlichen Einrichtungen sieht der Katalog eine stärkere Ex-ante-Kontrolle im Vorfeld konkreter Gefährdungen vor. Dazu gehören die Möglichkeit von Stichprobenkontrollen und die Anordnung von regelmäßigen und gezielten Sicherheitsüberprüfungen.³⁸ Bei wichtigen Einrichtungen fehlt die Befugnis zu Stichprobenkontrollen zu Gunsten externer nachträglicher Aufsichtsmaßnahmen.³⁹ Typische Aufsichtsbefugnisse wie das Verlangen von Nachweisen über die Umsetzung von Cybersicherheitskonzepten oder die Anforderung von Daten, Unterlagen und sonstigen Informationen bestehen für beide Einrichtungstypen.⁴⁰

3.2 Bußgelder

3.2.1 Cyber Resilience Act

Der CRA sieht ein abgestuftes Bußgeldkonzept vor, bei dem je nach Art und Schwere des Verstoßes Bußgelder in unterschiedlicher Höhe verhängt werden können. Nach Art. 64 Abs. 2 CRA können bei Verstoß gegen die Cybersicherheitsanforderungen oder Meldepflichten Bußgelder von bis zu 15 Mio. Euro oder bis zu 2,5% des weltweiten Umsatzes des vorangegangenen Geschäftsjahres verhängt werden. Bei Verstößen gegen die Pflichten für Bevollmächtigte, Einführer und Händler drohen Geldbußen von bis zu 10 Mio. Euro oder bis zu 2% des gesamten weltweiten Umsatzes des vorangegangenen Geschäftsjahres. Schließlich werden bei falschen, unvollständigen oder irreführenden Angaben gegenüber notifizierten Stellen und Marktüberwachungsbehörden

33 Art. 23 Abs. 3 NIS-2-RL.

34 Art. 52 CRA.

35 Art. 53 CRA.

36 Art. 54 Abs. 1 UAbs. 2 CRA.

37 Art. 54 Abs. 5 CRA.

38 Art. 32 NIS-2-RL.

39 Art. 33 NIS-2-RL.

40 Art. 32, 33 NIS-2-RL.

32 Art. 20 Abs. 1 NIS-2-RL.

► Cybersicherheit ist eine zentrale Governance-Pflicht und fester Bestandteil der Risiko-berichterstattung. ◀

den Geldbußen von bis zu 5 Mio. Euro oder bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres fällig.

3.2.2 NIS-2-Richtlinie

Grundsätzlich können die Mitgliedstaaten den genauen Bußgeldrahmen in ihrer Umsetzung der NIS-2-Richtlinie selbst bestimmen, allerdings sieht die NIS-2-Richtlinie mindestens vorzusehende Höchstbeträge vor. Der Höchstbetrag bei wesentlichen Einrichtungen beträgt mindestens 10 Mio. Euro oder mindestens 2 % des gesamten weltweit erzielten Umsatzes des Unternehmens, zu dem die wesentliche Einrichtung gehört.⁴¹ Bei wichtigen Einrichtungen betragen die entsprechenden mindestens vorzusehenden Höchstbeträge 7 Mio. Euro oder 1,4 % des gesamten weltweit erzielten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört.⁴²

3.2.3 Schadensersatz

Weder der Cyber Resilience Act (CRA) noch die NIS-2-Richtlinie enthalten Anspruchsgrundlagen für individuelle Ansprüche auf Schadensersatz bei Verstößen gegen die gesetzlichen Anforderungen oder bei Informationssicherheitsvorfällen. Allerdings können Verstöße gegen die in diesen Regelwerken verankerten Pflichten zivilrechtliche Haftungsfolgen nach sich ziehen, etwa über die allgemeinen Haftungsregelungen des Vertrags- und Deliktsrechts.

4. Handlungsempfehlungen

Durch den CRA und die NIS-2-Richtlinie wird Cybersicherheit auch gesetzlich zur

zentralen Führungsaufgabe, die von Vorstand und Geschäftsführung aktiv gesteuert werden muss. Es empfiehlt sich daher, Cybersicherheit als festen Bestandteil der Unternehmensstrategie zu verankern und regelmäßig auf Ebene der Geschäftsleitung und in Aufsichts- und Beiratsgremien zu thematisieren. Essenziell ist auch die klare Zuweisung von Verantwortlichkeiten, etwa durch die Bestellung eines Chief Information Security Officers (CISO) mit direkter Berichtslinie an die Geschäftsleitung, außerdem die regelmäßige Überwachung und kritische Hinterfragung der Wirksamkeit der getroffenen Maßnahmen durch die Kontrollgremien.

Ein systematisches und dokumentiertes Risikomanagement für Cyberrisiken ist Pflicht. Dazu gehören regelmäßige Risikoanalysen, die Bewertung der aktuellen Bedrohungslage und die Ableitung und Umsetzung angemessener technischer und organisatorischer Maßnahmen. Mithilfe einer Gap-Analyse können der Umsetzungsstand der Anforderungen aus CRA und NIS-2 ermittelt, bestehende Lücken identifiziert und gezielte Maßnahmen abgeleitet werden. Auch die Lieferkette muss in das Risikomanagement einbezogen werden. Verträge mit Lieferanten und Dienstleistern sollten auf Cybersicherheitsklauseln überprüft und bei Bedarf angepasst werden. Zudem ist die Implementierung klarer Meldeprozesse für Sicherheitsvorfälle wesentlich, um die gesetzlichen Meldefristen zuverlässig einhalten zu können. Die Geschäftsleitung sollte dem Aufsichtsrat regelmäßig über den Stand der Cybersicherheit, relevante Vorfälle und getroffene Compliance-Maßnahmen berichten.

Ein weiterer zentraler Aspekt ist die Sensibilisierung und Schulung: Geschäftsleitung und Aufsichtsgremien sind ver-

pflichtet, regelmäßig an Schulungen zu Cybersicherheit und den gesetzlichen Anforderungen teilzunehmen. Gleichzeitig sollte eine Unternehmenskultur gefördert werden, in der Cybersicherheit als gemeinschaftliche Aufgabe verstanden wird und alle Mitarbeitenden aktiv eingebunden sind. Schließlich empfiehlt es sich, die Wirksamkeit der Cybersicherheitsmaßnahmen mindestens jährlich zu überprüfen und an neue Bedrohungen und regulatorische Entwicklungen anzupassen. Bei Bedarf sollte externe Expertise hinzugezogen werden.

5. Fazit

Cybersicherheit ist eine zentrale Governance-Pflicht und fester Bestandteil der Risikoberichterstattung. CRA und NIS-2 setzen komplementäre Maßstäbe: Der CRA adressiert produktbezogene Sicherheitspflichten über den gesamten Lebenszyklus. Nach der NIS-2-Richtlinie werden betroffene Einrichtungen zu angemessenen technischen, organisatorischen und operativen Maßnahmen verpflichtet. Beide Rechtsakte heben jedoch die Verantwortung der Leitungsorgane hervor und verlangen Meldungen bei gravierenden Sicherheitsvorfällen. Gemeinsam haben die Rechtsakte auch, dass die Marktüberwachungs- bzw. Aufsichtsbehörden über weitreichende Eingriffsbefugnisse verfügen. Bei Nichtbeachtung der gesetzlichen Anforderungen drohen hohe Bußgelder und zivilrechtliche Haftungsrisiken, obwohl die Rechtsakte keine eigenständigen Schadensersatzansprüche enthalten. Für die Umsetzung von CRA und NIS-2 in der Praxis empfiehlt sich insbesondere eine strategische Verankerung der Cybersicherheit in der Geschäftsführung bzw. auf Vorstands- und Aufsichtsratsbene.

41 Art. 34 Abs. 4 NIS-2-RL.

42 Art. 34 Abs. 5 NIS-2-RL.