Downloaded from Blogs on 26.10.2026 06:06

By PwC Deutschland | 20 October 2026

IT-Sicherheit ist Chefsache: Die persönliche Verantwortung der Geschäftsleitung für Cyberrisiken

Cyberangriffe gehören zu den existentiellen Bedrohungen für die moderne Unternehmensführung. Mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes und der tiefgreifenden Reform des BSI-Gesetzes (BSIG) hat der Gesetzgeber die Anforderungen an das IT-Risikomanagement drastisch verschärft. Vorstände und Geschäftsführer stehen mehr denn je persönlich in der Pflicht. Dieser Beitrag zeigt auf, welche organisatorischen und haftungsrechtlichen Anforderungen die Geschäftsleitung nun zwingend beachten und erfüllen muss, wo ihr Ermessensspielraum endet und wie Aufgaben haftungssicher delegiert werden können.

Downloaded from Blogs on 26.10.2026 06:06

Content

Die neue regulatorische Landschaft: NIS-2, das reformierte BSIG und das KRITIS-DachG 3

Gesellschaftsrechtlicher Anknüpfungspunkt: Wo das Ermessen der Geschäftsleitung endet 3

Arbeitsteilung und Delegation: Gesamtverantwortung bleibt unübertragbar 4

1. Horizontale Delegation (Ressortverteilung im Kollegialorgan) 5
2. Vertikale Delegation (auf CISO, IT-Abteilung und Fachbereiche) 5
3. Besonderheiten im Konzern 5

Haftung im Ernstfall: Keine Außenhaftung, aber scharfe Binnenhaftung 6

Praxishinweis: Was Unternehmen jetzt tun sollten 6

Downloaded from Blogs on 26.10.2026 06:06

Verfasst von Dr. Thorsten Ehrhard und Dr. Georg Haas

*Dieser Beitrag ist Bestandteil unserer Reihe zur Organhaftung. Zuletzt ist am 5. August 2026 der Beitrag „**Organhaftung: BGH verschärft die Verantwortlichkeit des Aufsichtsrats – Urteil des II. Zivilsenats des BGH vom 14. Oktober 2025 (II ZR 78/24)**“ auf unserem Blog erschienen.*

Die neue regulatorische Landschaft: NIS-2, das reformierte BSIG und das KRITIS-DachG

Die Bedrohungslage durch Cyberkriminalität, Spionage und Sabotage – verschärft durch geopolitische Konflikte und den Einsatz Künstlicher Intelligenz – hat eine beispiellose Dynamik erreicht. Laut aktuellen Bitkom-Erhebungen beziffern sich die jährlichen Schäden in der deutschen Wirtschaft auf über 280 Milliarden Euro, wobei ein Großteil direkt auf Cyberattacken wie Ransomware zurückzuführen ist.

Der Gesetzgeber hat reagiert: Am 6. Dezember 2025 ist das Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie in Kraft getreten und hat das BSIG grundlegend novelliert. Dadurch hat sich der Kreis der betroffenen Unternehmen in Deutschland schlagartig um das Zehnfache auf schätzungsweise 30.000 Unternehmen erhöht. Diese teilen sich auf in:

- **Besonders wichtige Einrichtungen**: z. B. Großunternehmen in Schlüsselsektoren wie Energie, Transport oder digitale Infrastruktur ab 250 Mitarbeitern oder 50 Mio. Euro Umsatz,
- **Wichtige Einrichtungen**: mittelständische Unternehmen ab 50 Mitarbeitern oder 10 Mio. Euro Umsatz in regulierten Sektoren.

Gemäß § 30 Abs. 1 BSIG müssen diese Einrichtungen **geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen** (TOMs) ergreifen, um Störungen der IT-Systeme zu vermeiden und Auswirkungen von Vorfällen gering zu halten. § 30 Abs. 2 BSIG konkretisiert dies in Form von **zehn Mindestanforderungen**, die eine vollständige Cybersicherheitsarchitektur abbilden (u. a. Risikoanalysen, Vorfallsbewältigung, Back-up-Management, Lieferkettensicherheit, Verschlüsselung, Multi-Faktor-Authentifizierung und regelmäßige Schulungen). Betreiber kritischer Anlagen müssen zudem **Systeme zur Angriffserkennung** nach § 31 BSIG vorhalten.

Parallel und teilweise überlappend fordert das KRITIS-Dachgesetz (KRITIS-DachG) einen **physischen „All-Gefahren-Ansatz“** (Schutz vor Sabotage, Naturkatastrophen etc.). Hiernach ist gemäß § 12 KRITIS-DachG mindestens alle vier Jahre eine **anlagenbezogene Risikoanalyse** durchzuführen.

Gesellschaftsrechtlicher Anknüpfungspunkt: Wo das Ermessen der Geschäftsleitung endet

Downloaded from Blogs on 26.10.2026 06:06

Das Thema Cybersicherheit betrifft keineswegs nur direkt regulierte Branchen. Nach allgemeinen gesellschaftsrechtlichen Grundsätzen (§ 93 Abs. 1 AktG, § 43 Abs. 1 GmbHG) ist jeder Geschäftsleiter verpflichtet, die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.

- **§ 91 Abs. 2 AktG** verpflichtet den Vorstand zur Einrichtung eines Risikofrüherkennungssystems zur Identifikation bestandsgefährdender Risiken. IT- und Cyberrisiken werden von der herrschenden Meinung als solche bestandsgefährdenden Entwicklungen eingestuft.
- **§ 91 Abs. 3 AktG** verlangt von Vorständen börsennotierter Gesellschaften überdies ein angemessenes und wirksames internes Kontroll- (IKS) und Risikomanagementsystem (RMS).
- Diese Pflichten gelten über die Leitbildfunktion und Ausstrahlungswirkung der spezialgesetzlichen Regelungen auf der Grundlage der allgemeinen Sorgfaltspflichten des **§43GmbHG** in gleicher Weise für Geschäftsführer einer GmbH.

Dabei entfaltet insbesondere der gesetzliche Mindeststandard des § 30 Abs. 2 BSIG eine **erhebliche Leitbildfunktion** für das gesamte Gesellschaftsrecht. Je näher ein nicht direkt reguliertes Unternehmen in Bezug auf Größe, Branche und Risikoprofil an die gesetzlichen Schwellenwerte heranreicht, desto eher dienen die dort genannten zehn Mindestmaßnahmen als Orientierungsrahmen für die allgemeine zivilrechtliche Sorgfaltspflicht.

Hinsichtlich des Haftungsschutzes durch die **Business Judgment Rule** (BJR) im Sinne des §93Abs.1S.2AktG ist streng zwischen dem „Ob“ und dem „Wie“ zu unterscheiden:

1. **„Ob“**: Soweit ein Unternehmen in den Anwendungsbereich des BSIG, des KRITIS-DachG oder anderer Spezialgesetze fällt, hat die Geschäftsleitung keinen Ermessensspielraum hinsichtlich des „Ob“ der Implementierung der gesetzlich geforderten Maßnahmen. Die Umsetzung ist eine gesetzlich gebundene Pflichtaufgabe (Legalitätspflicht). Ein Verzicht auf einzelne Mindestmaßnahmen aus Kosten-Nutzen-Erwägungen stellt eine haftungsbegründende Pflichtverletzung dar und ist nicht durch die BJR geschützt.
2. **„Wie“**: Bei der konkreten technischen Ausgestaltung, der Auswahl von IT-Sicherheitsdienstleistern, Softwareprodukten oder der organisatorischen Verortung verbleibt der Geschäftsleitung ein unternehmerisches Organisationsermessen. Solange diese Entscheidungen auf Grundlage angemessener Informationen, frei von Interessenkonflikten und im vermeintlichen Wohl der Gesellschaft getroffen und sauber dokumentiert werden, greift der Haftungsschutz der BJR.

Arbeitsteilung und Delegation: Gesamtverantwortung bleibt unübertragbar

Der Aufbau eines Cybersicherheitsmanagements erfordert hochgradiges Fachwissen. Die Geschäftsleitung muss die Aufgaben daher im betrieblichen Alltag verteilen. Das Gesetz und die Rechtsprechung

Downloaded from Blogs on 26.10.2026 06:06

unterscheiden hierbei zwei Dimensionen:

1. Horizontale Delegation (Ressortverteilung im Kollegialorgan)

Die Zuweisung der operativen Cybersicherheit an ein bestimmtes Mitglied der Geschäftsleitung (z.B. IT-Vorstand) ist im Rahmen einer **ordnungsgemäßen Ressortverteilung** zulässig und ratsam. Dies beschränkt die primäre Handlungsverantwortung auf das zuständige Mitglied.

Für die übrigen, ressortfremden Mitglieder wandelt sich die Pflicht jedoch in eine **Beobachtungs- und Überwachungspflicht** um. Sie dürfen auf die ordnungsgemäße Erfüllung vertrauen, solange keine Warnsignale oder Unregelmäßigkeiten erkennbar sind. Bei erkennbaren Defiziten oder anhaltenden Sicherheitslücken lebt die Pflicht zum sofortigen Einschreiten und zur Befassung des Gesamtorgans für alle Mitglieder zwingend wieder auf (aktuell BGH, Urteil vom 09.11.2023 - III ZR 105/22).

2. Vertikale Delegation (auf CISO, IT-Abteilung und Fachbereiche)

Trotz des missverständlichen Wortlauts in § 38 Abs. 1 BSIG, wonach die Geschäftsleitung Risikomanagementmaßnahmen „umzusetzen“ hat, ist auch eine vertikale **Delegation an nachgeordnete Mitarbeiter** (z. B. einen Chief Information Security Officer – CISO) oder externe IT-Dienstleister gesellschaftsrechtlich zulässig und in der Praxis unumgänglich. Durch die Delegation entfällt jedoch nicht die Verantwortung der Geschäftsleitung. Vielmehr wandelt sich die Handlungs- in eine spezifische **Delegationssorgfaltspflicht**. Die Geschäftsleitung treffen insoweit strenge Pflichten:

- **Sorgfältige Auswahl**: Der Delegat (z. B. CISO) muss fachlich und persönlich uneingeschränkt geeignet sein.
- **Klare Instruktion und Aufgabenzuweisung**: Aufgaben, Kompetenzen, Berichtswege und Eskalationsschwellen müssen unmissverständlich schriftlich definiert werden.
- **Laufende Überwachung**: Die Geschäftsleitung muss ein funktionierendes Berichts- und Informationssystem etablieren. Sie muss Stichproben vornehmen und die Wirksamkeit der Maßnahmen (z.B. durch die Interne Revision) regelmäßig prüfen lassen.

Die **Letztentscheidung und strategische Letztverantwortung** verbleiben zwingend beim Geschäftsleitungsorgan (Letztverantwortungsprinzip). Geschäftsleiter müssen sich die wesentlichen Maßnahmen und Konzepte vorlegen lassen, diese verstehen und ausdrücklich billigen, und die maßgeblichen **Grundentscheidungen** selbst treffen.

Zudem normiert § 38 Abs. 3 BSIG eine **persönliche, nicht delegierbare Schulungspflicht** der Geschäftsleitung zur Erlangung grundlegender Kenntnisse im Cyber-Risikomanagement (vorgeschlagenes Intervall: mindestens alle drei Jahre).

Downloaded from Blogs on 26.10.2026 06:06

3. Besonderheiten im Konzern

Sicherheitsinfrastrukturen werden in Konzernen häufig zentralisiert gebündelt (z. B. über ein konzernweites Security Operations Center oder einen Group CISO). Rechtlich gilt jedoch das Prinzip der **dezentralen Eigenverantwortung**: Die Geschäftsleitung jeder einzelnen Tochtergesellschaft bleibt persönlich für die IT-Sicherheit ihres eigenen Unternehmens verantwortlich und haftbar. Zentrale Konzernvorgaben dürfen nicht blind übernommen werden; die lokale Geschäftsleitung muss sicherstellen, dass diese den spezifischen lokalen operativen und regulatorischen Anforderungen genügen und dass klare, vertraglich geregelte Eskalationswege im Krisenfall bestehen.

Haftung im Ernstfall: Keine Außenhaftung, aber scharfe Binnenhaftung

Kommt es infolge einer unzureichenden Cybersicherheitsorganisation zu einem Cyberangriff und entstehen dem Unternehmen hierdurch Schäden (z. B. durch Betriebsstillstand oder behördliche Bußgelder), droht der Geschäftsleitung eine persönliche Inhaftnahme:

- **Innenhaftung gegenüber der Gesellschaft**: Nach § 38 Abs. 2 BSIG i. V. m. § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG haftet die Geschäftsleitung dem Unternehmen persönlich für schuldhafte Pflichtverletzungen. Da im Streitfall die Geschäftsleitung beweisen muss, dass sie die Sorgfalt eines ordentlichen Geschäftsleiters angewandt hat (Beweislastumkehr, §93Abs.2Satz2AktG), ist eine lückenlose Dokumentation von Risikoanalysen, Vorstandsbeschlüssen und Wirksamkeitskontrollen die wichtigste Absicherung gegen Haftungsansprüche.
- **Ausschluss der deliktischen Außenhaftung**: Eine persönliche Außenhaftung der Geschäftsleiter direkt gegenüber geschädigten Dritten (z. B. Kunden, deren Daten gestohlen wurden) gemäß § 823 Abs. 2 BGB i.V.m. § 30 BSIG ist im Ergebnis mit guten Gründen abzulehnen. In Übertragung der gefestigten Rechtsprechung des BGH zu aufsichtsrechtlichen Organisationspflichten dürfte § 30 BSIG kein Schutzgesetz im Sinne des Deliktsrechts darstellen. Die Norm dient der ordnungspolitischen Gefahrenabwehr und dem Schutz der Allgemeinheit; der Schutz individueller Vermögenswerte ist lediglich ein nicht anspruchsbegründender „Gesetzesreflex“.

Für die notwendige **Überwachung durch den Aufsichtsrat** gilt: Die Berichts- und Informationspflichten des Vorstands an den Aufsichtsrat sind zwingende Bringschulden. Bei mangelhafter IT-Risikoberichterstattung haftet der Vorstand; der Aufsichtsrat wiederum ist bei unklaren Berichten zu proaktiven Nachforschungen verpflichtet (aktuell BGH, Urteil vom 14.10.2025 - II ZR 78/24 – siehe dazu den Beitrag „**Organhaftung: BGH verschärft die Verantwortlichkeit des Aufsichtsrats**“ auf unserem Blog).

Praxishinweis: Was Unternehmen jetzt tun sollten

Zur Absicherung vor Haftungsrisiken und zur Stärkung der digitalen Resilienz sollten Unternehmen

Downloaded from Blogs on 26.10.2026 06:06

kurzfristig einen **strukturierten Cybersecurity Legal Check** initiieren:

1. **Regulatorischen Scope bestimmen**: Prüfen, ob das Unternehmen als „wichtige“ oder „besonders wichtige“ Einrichtung unter das reformierte BSIG fällt oder ob eine Leitbildwirkung für allgemeine gesellschaftsrechtliche Organisationspflichten greift.
2. **TOMs & Mindestanforderungen abgleichen**: Die bestehenden IT-Sicherheitsvorkehrungen detailliert an den zehn Mindestanforderungen des § 30 Abs. 2 BSIG spiegeln und Lücken schließen.
3. **Delegationsstrukturen schriftlich fixieren**: Vertikale Delegationen (Aufgaben des CISO) präzise und überschneidungsfrei definieren und ein transparentes Berichts- und Eskalationswesen etablieren.
4. **Schulungsverpflichtung umsetzen**: Zwingende und regelmäßige Teilnahme der gesamten Geschäftsleitung an Cybersicherheitsschulungen einplanen und nachweisen.
   Entscheidungen dokumentieren: Alle IT-Risikoabwägungen (insbesondere Kosten-Nutzen-Verhältnismäßigkeiten beim „Wie“) sowie Auditberichte manipulationssicher dokumentieren, um der gesellschaftsrechtlichen Beweislastumkehr zu begegnen.
5. **Versicherungsschutz prüfen**: Abschluss einer speziellen Cyber-Versicherung (inklusive eventueller Lösegeld-Klauseln bei Ransomware-Angriffen) unter enger Abstimmung der vertraglichen Obliegenheiten prüfen.

Kontaktieren Sie uns

Dr. Thorsten Ehrhard

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

Dr. Georg Haas

Senior Manager Frankfurt am Main
Tel.: +49 69 9585-1250
E-Mail:**georg.haas@pwc.com**

Keywords

Gesetzgebung