NIS-2 für C-Levels

NIS-2 aus Leitungssicht: Anforderungen, Verantwortung und Handlungsfelder

Die legislative Einführung der NIS-2-Richtlinie ist mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes (NIS2UmsuCG) am 6. Dezember 2025 nunmehr auch in Deutschland abgeschlossen. Die NIS-2-Regulation bringt nicht nur technische und organisatorische Anforderungen für die betroffenen Unternehmen mit sich, sondern nimmt auch die Unternehmensleitungen in die Pflicht. In den meisten Veröffentlichungen zu NIS-2 findet die Inpflichtnahme der Leitungsebene nur beiläufig Beachtung und beschränkt sich auf Hinweise zu den Schulungspflichten und zum Sanktionsrahmen. Dieser Beitrag nimmt diesen bislang wenig vertieften Aspekt zum Anlass, die NIS-2-Aufsichtspflichten des TOP-Managements näher zu beleuchten.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Einleitung

Die fortschreitende Digitalisierung und die Zunahme komplexer Cyberbedrohungen machen eine systematische Regulierung der Cybersicherheit in Europa unerlässlich. Die NIS-2-Richtlinie (Network and Information Security Directive) der EU verfolgt das Ziel, die Cyberresilienz kritischer und wichtiger Einrichtungen in den Mitgliedstaaten deutlich zu stärken. Seit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes (NIS2UmsuCG) am 6. Dezember 2025 ist die Richtlinie auch in Deutschland rechtlich bindend [BGBl 2025].

Während die öffentliche Diskussion oft die technischen und organisatorischen Anforderungen an Unternehmen in den Mittelpunkt stellt, wird ein zentraler Aspekt bislang nur am Rande behandelt: **die unmittelbare Verantwortung der Unternehmensleitung.** Denn die NIS-2-Richtlinie nimmt die oberste Führungsebene ausdrücklich in die Pflicht, sowohl hinsichtlich strategischer Entscheidungen als auch im operativen Risikomanagement.

Die besondere Verantwortung der Unternehmensleitungen wird auch von der national zuständigen Aufsichtsbehörde hervorgehoben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont in einer Handreichung vom 30. September 2025 ausdrücklich die Pflicht der Geschäftsleitungen zur eigenen Fort- und Weiterbildung im Bereich der Informationssicherheit [BSI 2025]. Damit wird klargestellt, dass Leitungsorgane nicht lediglich formale Genehmigungsentscheidungen zu treffen haben, sondern sich aktiv und kontinuierlich mit den Anforderungen der NIS-2-Regulierung auseinandersetzen müssen. Die Einhaltung dieser Schulungspflichten ist zugleich Voraussetzung für eine wirksame Wahrnehmung der Leitungs- und Überwachungsverantwortung und kann im Fall von Defiziten sowohl für das Unternehmen als auch für einzelne Führungspersonen haftungs- und sanktionsrechtliche Relevanz entfalten.

Die persönliche Verantwortlichkeit ergibt sich vor allem aus den Aufsichtspflichten gemäß § 130 OWiG, die durch NIS-2 inhaltlich und hinsichtlich des Sanktionsrahmens konkretisiert werden. Die Anforderungen reichen von Auswahl- über Organisations- und Aufklärungspflichten bis hin zu Überwachungs- und Sanktionspflichten.

Ziel dieses Beitrags ist es, die Aufsichtspflichten des Top-Managements im Lichte der NIS-2-Richtlinie systematisch darzustellen und praxisnahe Handlungsfelder aufzuzeigen.

Bedeutung der NIS-2-Richtlinie für Leitungsorgane

Die Bedeutung der NIS-2-Richtlinie für Leitungsorgane lässt sich in die Bereiche **„Pflichten"** und **„Sanktionen"** unterteilen.

1. Pflichten der Leitungsorgane

Die NIS-2-Richtlinie legt den Fokus ausdrücklich auf die Verantwortung der obersten Führungsebene für die Cybersicherheit und Cyberresilienz ihrer Organisation. Leitungsorgane müssen die Einführung geeigneter Risikomanagementmaßnahmen veranlassen, die der Größe und Art des Unternehmens entsprechen und eine wirksame Abwehr gegen Cyberangriffe ermöglichen. Dabei sind Prozesse und technische Vorkehrungen zu etablieren, die die Widerstandsfähigkeit der Informationssysteme erhöhen.

Darüber hinaus verpflichtet die Richtlinie die Leitung zur kontinuierlichen Aufsicht und Überwachung dieser Maßnahmen. Dies bedeutet, dass es nicht ausreicht, einmalig Regelungen einzuführen; vielmehr müssen Führungskräfte sicherstellen, dass die festgelegten Maßnahmen dauerhaft umgesetzt und regelmäßig auf ihre Wirksamkeit geprüft werden. Ein weiteres zentrales Element ist die persönliche Teilnahme der Leitungsorgane an Schulungen zur Cybersicherheit und Cyberresilienz. Nur so können sie ihre Rolle als Vorbild wahrnehmen und gleichzeitig die Sicherstellung geeigneter Schulungen für alle Mitarbeiter gewährleisten.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

2. Sanktionen bei Verstößen

Die NIS-2-Richtlinie sieht strikte Sanktionen vor, um die Umsetzung der Pflichten durch die Unternehmensleitung sicherzustellen. Bei Verstößen können gegen Unternehmen empfindliche Geldbußen verhängt werden: Für besonders wichtige Einrichtungen bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes und für wichtige Einrichtungen bis zu 7 Millionen Euro oder 1,4 Prozent des Umsatzes. Diese Bußgelder sind so ausgestaltet, dass sie auch für größere Unternehmen spürbar sind und eine abschreckende Wirkung entfalten.

Darüber hinaus besteht die Möglichkeit einer persönlichen Haftung von Mitgliedern der Leitungsorgane gemäß § 130 OWiG. Dies unterstreicht, dass sich einzelne Führungskräfte nicht hinter der juristischen Person des Unternehmens verstecken können. Im Falle besonders gravierender Verstöße oder fehlender Eignung kann betroffenen Führungskräften sogar untersagt werden, künftig weiterhin Leitungsfunktionen im Unternehmen wahrzunehmen. Die Sanktionen sollen so sicherstellen, dass Cybersicherheit auf höchster Managementebene als Pflicht und nicht als freiwillige Aufgabe verstanden wird.

Die fünf Dimensionen der Aufsichtspflichten gemäß § 130 OWiG

Das zentrale rechtliche Fundament für die persönliche Verantwortung von Leitungsorganen bildet § 130 des Ordnungswidrigkeitengesetzes (OWiG). Dieser Paragraf bezieht sich auf die Verletzung der Aufsichtspflicht in Betrieben und Unternehmen und konkretisiert die Anforderungen in Form von fünf Handlungsfeldern:

1. Auswahlpflichten

Im Rahmen der Auswahlpflichten ist die Unternehmensleitung verpflichtet, Personen mit Leitungs- oder Überwachungsaufgaben so auszuwählen, dass sie fachlich und persönlich zur Einhaltung der unternehmensbezogenen Rechtsvorgaben, also insbesondere im Bereich der IT- und Cyber-Sicherheit, in der Lage sind. Vor dem Hintergrund der NIS-2-Richtlinie umfasst dies die Auswahl von Führungskräften, die über ausreichende Kenntnisse in Cybersicherheit, Risikomanagement und den für das Unternehmen relevanten Sicherheitsanforderungen verfügen. Dabei ist sicherzustellen, dass die ausgewählten Personen in der Lage sind, organisatorische und technische Maßnahmen gemäß NIS-2 wirksam umzusetzen und fortlaufend anzupassen.

Die bedeutsamsten Merkmale zur Erfüllung der Auswahlpflichten sind in der nachfolgenden Tabelle aufgeführt:

#	Merkmale zur Sicherstellung einer geeigneten Personalauswahl
1	Standardisiertes Auswahlverfahren
2	Transparente Personalakquise
3	Aus- und Fortbildungsprogramm
4	Führungserfahrung im Fachgebiet

Tabelle 1: Merkmale zur Erfüllung der OWiG-Auswahlpflichten

Skizzierung eines Fallbeispiels:

Ein mittelständisches Unternehmen führt ein neues Auswahlverfahren ein: Offene IT-Stellen mit Führungsverantwortung werden über zielgerichtete Ausschreibungen in Fachportalen besetzt. Vorausgesetzt werden ein abgeschlossenes Hochschulstudium in einem IT- oder informationssicherheitsrelevanten Fach sowie mindestens drei Jahre einschlägige Führungserfahrung im Bereich IT-Sicherheit. In einer zweiten Auswahlrunde finden strukturierte Interviews mit der Compliance-Abteilung statt, in denen die Eignung im Hinblick auf regulatorische und gesetzliche Anforderungen ergründet wird.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

2. Organisationspflichten

Im Rahmen der Organisationspflichten ist die Unternehmensleitung verpflichtet, eine betriebliche Struktur zu schaffen, die sicherstellt, dass relevante IT-Sicherheitsanforderungen wirksam erfüllt werden. Vor dem Hintergrund der NIS-2-Richtlinie umfasst dies insbesondere die Einrichtung eines strukturierten Informationssicherheitsmanagements (ISMS), die Definition klarer Verantwortlichkeiten, die Implementierung technischer und organisatorischer Maßnahmen zur Risikoprävention sowie die regelmäßige Kontrolle und Anpassung dieser Maßnahmen. Ziel ist es, Cyberrisiken frühzeitig zu erkennen, Sicherheitsvorfälle zu vermeiden und die rechtlichen Vorgaben der NIS-2-Richtlinie kontinuierlich umzusetzen.

Die bedeutsamsten Merkmale zur Erfüllung der Organisationspflichten sind in der nachfolgenden Tabelle aufgeführt:

#	Merkmale zur Sicherstellung einer geeigneten betrieblichen Organisation
1	Geschäftsordnung nebst Verteilungsplan
2	Aufgaben- und Verantwortungsprofile für alle Mitarbeiter
3	Vertretungsregelungen (24/7 hinsichtlich der NIS-2-Meldepflichten)
4	Konsistente Projektorganisation und Betriebsorganisation

Tabelle 2: Merkmale zur Erfüllung der OWiG-Organisationspflichten

Skizzierung eines Fallbeispiels:

In einem Krankenhausbetrieb wird eine neue Projektstruktur eingeführt, bei der alle IT-Projekte standardmäßig einen „Cybersecurity-Verantwortlichen" enthalten. Zudem wird ein Schichtplan erstellt, der sicherstellt, dass bei Sicherheitsvorfällen jederzeit ein meldeberechtigter Vertreter erreichbar ist. Die Verantwortlichkeiten werden in einer neuen Geschäftsordnung transparent abgebildet.

3. Aufklärungspflichten

Im Rahmen der Aufklärungspflichten ist die Unternehmensleitung verpflichtet sicherzustellen, dass die gesamte Belegschaft über die Anforderungen und Risiken im Zusammenhang mit der NIS-2-Richtlinie informiert ist. Dazu gehört insbesondere die regelmäßige und zielgruppengerechte Schulung in Bezug auf IT-Sicherheitsmaßnahmen, Meldepflichten, Vorfallmanagement sowie das Erkennen und Vermeiden von Cyberbedrohungen. Die Organisation hat geeignete Kommunikationsstrukturen zu schaffen, die es ermöglichen, sicherheitsrelevante Informationen und Vorfälle zeitnah zu erfassen, weiterzugeben und wirksam zu bearbeiten.

Die bedeutsamsten Merkmale zur Erfüllung der Aufklärungspflichten sind in der nachfolgenden Tabelle aufgeführt:

#	Merkmale zur Sicherstellung einer geeigneten Kommunikation und Aufklärung
1	Etablierung von Transparenz hinsichtlich Aufgaben und Vorschriften
2	Regelmäßige Informationsveranstaltungen
3	Schulungs- und Fortbildungspläne
4	Strukturierte Feedback-Mechanismen

Tabelle 3: Merkmale zur Erfüllung der OWiG-Aufklärungspflichten

Skizzierung eines Fallbeispiels:

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Eine Behörde organisiert vierteljährlich Pflichtveranstaltungen zur Cybersicherheit, in denen sowohl technische als auch rechtliche Aspekte behandelt werden. Zusätzlich wird ein internes Wiki gepflegt, das alle relevanten Richtlinien erläutert. Die Belegschaft kann über ein anonymes Feedbacksystem Rückfragen stellen oder Probleme melden.

4. Überwachungspflichten

Im Rahmen der Überwachungspflichten ist die Unternehmensleitung verpflichtet, die Wirksamkeit aller im Zusammenhang mit der NIS-2-Richtlinie ergriffenen technischen und organisatorischen Maßnahmen regelmäßig zu kontrollieren. Dies umfasst die Überprüfung von Sicherheitsvorgaben, die Funktionsfähigkeit von Melde- und Reaktionsprozessen bei Sicherheitsvorfällen sowie die Einhaltung interner und gesetzlicher IT-Sicherheitsstandards. Bei festgestellten Schwachstellen oder Verstößen sind unverzüglich geeignete Korrekturmaßnahmen zu ergreifen, um die Cybersicherheit des Unternehmens nachhaltig zu gewährleisten.

Die bedeutsamsten Merkmale zur Erfüllung der Überwachungspflichten sind in der nachfolgenden Tabelle aufgeführt:

#	Merkmale zur Sicherstellung einer geeigneten Überwachung
1	Etablierung von Kontroll- und Überwachungsverfahren
2	Etablierung eines internen Meldesystems
3	Systematische Identifikation von Fehlverhalten
4	Etablierung von Transparenz bei delokalisierten Arbeitsmodellen

Tabelle 4: Merkmale zur Erfüllung der OWiG-Überwachungspflichten

Skizzierung eines Fallbeispiels:

In einem IT-Dienstleistungsunternehmen wird ein zentrales Meldesystem eingeführt, über das sicherheitsrelevante Vorfälle automatisiert an das Management gemeldet werden. Zusätzlich erfolgen regelmäßige Prüfungen mobiler Arbeitsplätze, um Schwachstellen zu identifizieren.

5. Sanktionspflichten

Im Rahmen der Sanktionspflichten ist die Unternehmensleitung verpflichtet, bei Verstößen gegen die Anforderungen der NIS-2-Richtlinie, wie etwa bei unzureichenden IT-Sicherheitsmaßnahmen oder verspäteten Meldungen von Sicherheitsvorfällen, wirksame und verhältnismäßige Maßnahmen zu ergreifen. Dazu zählen disziplinarische Konsequenzen gegenüber verantwortlichen Mitarbeitenden sowie organisatorische Anpassungen, um Wiederholungen zu verhindern. Ziel ist es, die Einhaltung der NIS-2-Pflichten nachhaltig durchzusetzen, ein Fehlverhalten klar zu sanktionieren und die Cybersicherheitskultur im Unternehmen zu stärken.

Die bedeutsamsten Merkmale zur Erfüllung der Sanktionspflichten sind in der nachfolgenden Tabelle aufgeführt:

#	Merkmale eines geeigneten Sanktionsregimes
1	Nachhaltige Betonung der Einhaltung von Regeln („Tone from the Top“)
2	Konsequente Ahndung von Verstößen
3	Etablierung transparenter und nachvollziehbarer Sanktionen
4	Regelmäßige Bestandsaufnahme von Verstößen

Tabelle 5: Merkmale zur Erfüllung der OWiG-Sanktionspflichten

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Skizzierung eines Fallbeispiels:

In einem Forschungsinstitut werden wiederholte Verstöße einer mitarbeitenden Person gegen geltende Sicherheitsrichtlinien festgestellt. Nach vorherigen Verwarnungen wird der Zugriff auf sicherheitskritische Systeme dauerhaft entzogen. Dieser Fall wird anonymisiert im Intranet als Lehrbeispiel veröffentlicht, um der Belegschaft die Konsequenzen von Non-Compliance bewusst zu machen.

Praktische Konsequenzen für die Unternehmensleitung

Die NIS-2-Richtlinie verlangt von der Unternehmensführung nicht nur formale Compliance, sondern ein echtes Risikobewusstsein und eine nachhaltige Sicherheitskultur. Die nachfolgend aufgeführten Handlungsempfehlungen beruhen auf ersten praktischen Erfahrungswerten des Autorenteams aus der Begleitung von NIS-2-Umsetzungsprojekten betroffener Organisationen. Aufgrund der noch jungen Rechtslage und der gerade angelaufenen nationalen Umsetzung in Deutschland können derzeit noch keine empirisch belastbaren Erkenntnisse vorliegen. Gleichwohl lassen sich die Handlungsempfehlungen konsistent aus den Anforderungen der NIS-2-Richtlinie ableiten und stehen im Einklang mit der aktuellen rechtswissenschaftlichen Literatur zum Management von Cybersecurity in Unternehmen, vgl. bspw. [Bittner et al. 2021] und [Schuck 2024]:

#	TOP 5 NIS-2-Handlungsempfehlungen
1	Einrichtung eines Cybersecurity-Governance-Boards
2	Pflicht zur kontinuierlichen Weiterbildung der Leitungsebene
3	Verankerung von Cybersecurity in der Unternehmensstrategie
4	Aufbau robuster Krisen- und Reaktionsmechanismen
5	Verantwortungszuweisung und Kontrolle innerhalb der Organisation

Tabelle 6: TOP 5 NIS-2-Handlungsempfehlungen für die Leitungsebene

Herausforderungen und Erfolgsfaktoren

Die Umsetzung der NIS-2-Richtlinie ist komplex, insbesondere für kleinere Einrichtungen oder Organisationen mit begrenzten Ressourcen. Unabhängig davon gelten die Anforderungen an das Leitungsorgan uneingeschränkt für alle betroffenen Organisationen – auch dort, wo die IT-Funktion nur mit geringen Kapazitäten ausgeformt ist. Größen- oder strukturbedingte Erleichterungen sieht die Richtlinie nicht vor.

Die erfolgreiche Umsetzung hängt gemäß den ersten praktischen Erfahrungswerten des Autorenteams aus der Begleitung von NIS-2-Umsetzungsprojekten betroffener Organisationen vor allem von folgenden Faktoren ab:

#	Erfolgsfaktoren
1	Top-down-Commitment
2	Interdisziplinäre Zusammenarbeit
3	Klare Verantwortlichkeiten und Governance
4	Systematische Dokumentation und Nachvollziehbarkeit
5	Bewusstseinsbildung und Kulturwandel

Tabelle 7: Erfolgsfaktoren für die NIS-2-Umsetzung

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Fazit

Die NIS-2-Richtlinie stellt einen Paradigmenwechsel in der Cybersicherheitsregulierung dar, indem sie die Unternehmensleitung ausdrücklich in die Verantwortung nimmt. Durch die klare Ausdifferenzierung von Auswahl-, Organisations-, Aufklärungs-, Überwachungs- und Sanktionspflichten wird die Rolle der Leitungsebene nicht nur konkretisiert, sondern haftungsrechtlich unterlegt.

Für Unternehmen bedeutet dies, dass Cybersicherheit nicht länger als reine IT-Angelegenheit betrachtet werden kann. Entscheidend ist, dass sie integraler Bestandteil der Unternehmensführung ist, d. h. strategisch verankert, regelmäßig überprüft und aktiv vorgelebt wird. Nur so kann der steigenden Bedrohungslage wirksam begegnet und regulatorischen Anforderungen rechtskonform entsprochen werden. Gleichzeitig bietet eine konsequente Umsetzung auch Chancen: Sie stärkt die Resilienz der Organisation, schafft Vertrauen bei Kunden und Partnern und kann langfristig zum Wettbewerbsvorteil werden.

Literatur

[Bittner et al. 2021] Bittner, M.; Guntermann, A.; Müller, C.; Rostam, D.: Cybersecurity als Unternehmensleitungsaufgabe. In: Schriften zum IT-Sicherheitsrecht, Band 2; Nomos, Baden-Baden, 2021.

[BSI 2025] Bundesamt für Sicherheit in der Informationstechnik, „NIS-2-Geschäftsleitungsschulung", Version 0.9 („Initiale Veröffentlichung" vom 30. September 2025; online abrufbar unter: (*https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=3*; Zugriff am 8. Oktober 2025).

[BGBl 2025] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025; online abrufbar unter:
(https://www.recht.bund.de/eli/bund/bgbl-1/2025/301; Zugriff am 8. Dezember 2025).

[Schuck 2024] Schuck, J.: Cyberrisiken und Unternehmensorganisation. In: Abhandlungen zum Deutschen und Europäischen Gesellschafts- und Kapitalmarktrecht, Band 246; Duncker & Humblot, Berlin, 2024.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Autorenteam

- Dirk Diefenbach (WP, StB), BDO AG Wirtschaftsprüfungsgesellschaft
- Christian Ewel (CISA, CRISC), Flick Gocke Schaumburg Partnerschaft mbB
- Marc Weber (CISA, CGEIT, CRISC), selbständiger Unternehmensberater, Mitherausgeber der IT-Governance

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen? Dann schreiben Sie uns bitte an: FG_digital-trust@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapters? Dann besuchen Sie uns jetzt auf: https://www.isaca.de/publikationen/publikationen/alle-publikationen.html