

NIS2-Geschäftsleitungsschulung

Cyber Security ist Chefsache – und jetzt gesetzliche Pflicht



Warum Geschäftsleitungen nach NIS2 zur Schulung verpflichtet sind

Mit der nationalen Umsetzung der europäischen NIS2-Richtlinie wird Cybersicherheit in Deutschland ausdrücklich zur **Leitungsaufgabe** von Unternehmen erklärt. Cybersicherheit ist nicht länger eine ausschließlich operative oder technische Fragestellung, sondern integraler Bestandteil der unternehmerischen Gesamtverantwortung.

Der Gesetzgeber stellt in §38 BSIG klar: Die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen tragen die Verantwortung für die Umsetzung und fortlaufende Überwachung von Maßnahmen zur Cybersicherheit und können bei Pflichtverletzungen haftungsrechtlich belangt werden. Um sicherzustellen, dass Geschäftsleitungen dieser Verantwortung sachgerecht nachkommen können, schreibt das Gesetz eine regelmäßige Schulungspflicht vor.

Ziel der Schulung ist ausdrücklich keine technische Ausbildung, sondern die Befähigung der Geschäftsleitungen, Cyberrisiken als strategische Geschäftsrisiken zu erkennen, zu bewerten und in Managemententscheidungen einzubeziehen sowie Risikomanagementpraktiken zu beurteilen.

Fazit zur Schulungspflicht

NIS2 macht Cybersicherheit zur Chefsache. Die Geschäftsleitungsschulung ist kein Compliance-Formalismus, sondern ein zentrales Instrument zur Risikosteuerung und langfristigen Sicherung der Unternehmensresilienz.

Wesentliche Inhalte der NIS2-Geschäftsleitungsschulung

Bei den Schulungsinhalten orientieren wir uns an den Risikomanagementmaßnahmen aus §30 BSIG sowie den Handreichungen des BSI zur NIS2-Geschäftsleitungsschulung. Die Schulung gliedert sich in mehrere aufeinander aufbauende Inhaltsbereiche.

NIS2 Grundlagen

Zu Beginn werden die **rechtlichen Grundlagen der NIS2-Regulierung** vermittelt. Dazu zählen Zielsetzung und Geltungsbereich der Richtlinie, die nationalen Umsetzungsvorgaben, Pflichten für Einrichtungen und Geschäftsleitungen sowie Melde-, Registrierungs- und Dokumentationspflichten. Besonderes Augenmerk liegt auf der persönlichen Verantwortung der Geschäftsleitungen.

Vermittelte Kernkompetenzen

Im zweiten Schritt vermittelt die Schulung insbesondere drei Kernkompetenzen:

- 1) **Verständnis von Cyberrisiken:**
Geschäftsleitungen werden in die Lage versetzt, relevante Bedrohungen, Schwachstellen und Schadenspotenziale auf strategischer Ebene zu bewerten – einschließlich wirtschaftlicher, rechtlicher und reputativer Auswirkungen.
- 2) **Bewertung von Risikomanagementmaßnahmen:**
Vermittelt wird ein Überblick über gesetzlich geforderte Mindestmaßnahmen, den Stand der Technik sowie typische Zielkonflikte zwischen Sicherheit, Wirtschaftlichkeit und Betriebsfähigkeit. Ziel ist es, Maßnahmen fundiert steuern und überwachen zu können.
- 3) **Beurteilung der Auswirkungen auf das Unternehmen:**
Geschäftsleitungen lernen, wie sich Cybervorfälle und Sicherheitsmaßnahmen auf Geschäftsprozesse, Lieferketten, Meldepflichten, Haftung und Unternehmensstabilität auswirken.

Konkreter Transfer auf das individuelle Unternehmen

Ein besonderer Fokus liegt darauf, die vermittelten Inhalte auf die konkrete Risikolage, die bestehenden technischen und organisatorischen Maßnahmen (TOM) sowie die Geschäftsprozesse der jeweiligen Einrichtung zu beziehen. Dadurch wird sichergestellt, dass die Geschäftsleitung die Cyberrisiken und Sicherheitsmaßnahmen nicht nur abstrakt kennt, sondern deren Angemessenheit und **Wirksamkeit im eigenen Unternehmenskontext beurteilen** kann.

Empfohlener Teilnehmerkreis

Zusätzlich zu den gesetzlich verpflichtenden Personen empfehlen wir die Schulung auf Führungskräfte in vergleichbaren Positionen und Zuarbeitende der Geschäftsleitungen zu erweitern.

Unsere Leistungen

Die folgenden Leistungen unterstützen Dich bei der verpflichtenden NIS2-Schulung für Geschäftsleitungen. Möchtest Du ergänzende Inhalte in der Schulung, passen wir diese gerne an.

Dienstleistungen

1) NIS2-Geschäftsleitungsschulung (Foundation)

- Schulung der Geschäftsleitung zu NIS2, Cyberrisiken, Risikomanagementpraktiken und Auswirkungen auf das Unternehmen
- Halbtägiger Workshop oder alternativ Aufteilung in zwei Termine
- Teilnahme von bis zu 10 Führungskräften
- Aushändigung des Workshop-Handouts
- Nachweis über die Teilnahme und Schulungsinhalte

2) Unternehmensspezifischer Transfer (Advanced)

- Transfer der vermittelten Inhalte auf die konkrete Risikolage, die bestehenden technischen und organisatorischen Maßnahmen sowie die Geschäftsprozesse des Unternehmens
- Individueller Vorbereitungstermin mit Wissensträgern im Unternehmen, z. B. IT-Leitung, IT-Sicherheitsverantwortliche, Risikomanagement und CISO
- Unternehmensspezifische Vorbereitung der Schulung

3) Regelmäßiger Transfer (Professional)

- Regelmäßige Wiederholung kurzer Schulungssessions mit der Geschäftsleitung und den Führungskräften zu neuen und sich verändernden Cyberrisiken, Risikomanagementpraktiken und Auswirkungen auf das individuelle Unternehmen

Deine Ansprechpartner

Wir unterbreiten Dir gerne ein auf Dich abgestimmtes Angebot. Bei Interesse oder weitergehenden Fragen melde Dich gerne bei uns!



Andreas Holznagel
 Business Development Consulting Services
 +49 541 – 9632 5200
 andreas.holznagel@pco-online.de