Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

NIS-2-Geschäftsleitungsschulung

Vorläufige Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen nach dem NIS-2-Umsetzungsgesetzentwurf

Änderungshistorie

Version	*Datum*	*Beschreibung*
0.9	30.09.2025	initiale Veröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung Schulungspflicht für Geschäftsleitungen

Mit der Umsetzung der NIS-2-Richtlinie im BSIG („**BSIG-E**)[1] steigen die Anforderungen an Unternehmen, ihre Cybersicherheitsmaßnahmen systematisch zu planen, umzusetzen und zu überwachen. Besonders im Fokus steht dabei die Verantwortung der Geschäftsleitung: Sie muss gewährleisten, dass Cybersicherheit integraler Bestandteil der Geschäfte des Unternehmens und des Risikomanagements ist. Diese besondere Verantwortung der Geschäftsleitungen ist gesetzlich vorgeschrieben, ebenso wie eine Schulungspflicht für die Geschäftsleitungen.

In dieser vorläufigen Handreichung versucht das BSI, eine erste Hilfestellung für die Schulungspflicht nach § 38 Abs. 3 BSIG-E zu geben. Sowohl Schulungsanbieter als auch Geschäftsleitungen können sich daran orientieren.

Schulungsanbieter können ihre Schulung an diesen Informationen orientieren, um dem Verständnis des BSI vom Scope und Anspruch der Schulungen zu entsprechen. Hiermit geht allerdings keine rechtliche Verbindlichkeit einher.

Auch die beschulten Geschäftsleitungen können durch die Handreichung den Scope der Schulungsinhalte überprüfen.

In Anbetracht der bisher nicht erfolgten nationalen Umsetzung der NIS-2-Richtlinie kann und soll diese Handreichung keine abschließende Empfehlung für die Schulungen machen, sondern gibt das Verständnis des BSI zu den gesetzlichen Vorgaben aus § 38 Abs. 3 BSIG-E wieder.

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften in ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Zusammengefasst verpflichtet § 38 Abs. 1 BSIG-E die Geschäftsleitungen dazu, technisch-organisatorische Maßnahmen in den von ihnen geleiteten Einrichtungen umzusetzen und ihre Umsetzung zu überwachen. Sie können dafür auch in Haftung genommen werden, wenn sie ihren Verpflichtungen nicht nachkommen.

Um ihrer Verpflichtung nachkommen zu können, sieht das Gesetz daher eine Schulungspflicht für Geschäftsleitungen vor. Diese ist gesondert von den Schulungen für Mitarbeitende (nach § 30 Abs. 2 Nummer 7 BSIG-E) zu betrachten.

Schulungen nach § 38 Abs. 3 BSIG-E sollen die Geschäftsleitungen mindestens in drei Bereichen mit Kenntnissen und Fähigkeiten ausstatten:

[1] Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungsgesetz), BT-Drs. 21/1501.

Erkennung und Bewertung von Risiken

Die Geschäftsleitung muss in der Lage sein, an der Bewertung von Cybersicherheitsrisiken mitzuwirken. Dies soll nicht dazu führen, dass die Geschäftsleitungen technisch ebenso versiert sein müssen wie die Verantwortlichen für Netz- und Informationssicherheit in den Unternehmen. Sie muss aber in der Lage sein, Cybersicherheitsrisiken sinnvoll einschätzen zu können und entsprechende Maßnahmen treffen können.

Risikomanagementpraktiken

Die Geschäftsleitungen müssen technisch-organisatorische Risikomanagementmaßnahmen kennen. Mindestens sollten diese die nach § 30 Abs. 2 BSIG-E vorgesehenen Mindestmaßnahmen umfassen, sinnvollerweise aber auch alle darüberhinausgehenden Maßnahmen, die im Unternehmen implementiert sind oder deren Implementierung angedacht oder geplant wird.

Auch hier müssen die Geschäftsleitungen selbst nicht so versiert sein wie die technische Arbeits- und Entscheidungsebene. Vielmehr sollen Geschäftsleitungen verstehen, was mit den Einzelnen technisch-organisatorischen Maßnahmen gemeint ist und wie sich eine (Nicht-)Implementation betriebswirtschaftlich auswirkt.

Beurteilung der Auswirkungen von Risiken sowie Risikomanagementpraktiken

Entscheidend ist am Ende die Kombination der Kenntnisse und Fähigkeiten: Nur wenn Geschäftsleitungen die Risiken und die möglichen mitigierenden Maßnahmen kennen, können sie die Auswirkungen der Risiken und Risikomanagementmaßnahmen sinnvoll beurteilen.

Eine Geschäftsleitungsschulung sollte aus Sicht des BSI in jedem Fall diese drei miteinander verknüpften Aspekte adressieren. Ein Fokus etwa nur auf Risikomanagementmaßnahmen fällt hinter die gesetzlichen Anforderungen zurück und würde durch das BSI in Aufsichtsmaßnahmen auch als nicht ausreichend bewertet werden.

Dieses Dokument adressiert die folgenden Fragestellungen:

- Wer muss sich schulen lassen?
- Wie oft müssen die Schulungen durchgeführt werden?
- Wer sollte Schulungen durchführen?
- Was sollten die Schulungsinhalte sein?
- Wie fügt sich die Schulungspflicht in die gesetzlichen Grundlagen aus § 38 BSIG-E ein?

1.1 Adressaten der Schulungspflicht

Für wen genau die Schulungspflicht gilt, lässt sich direkt aus dem NIS-2-Umsetzungsgesetz (BT-Drs. 21/1501) ableiten.

Im Sinne dieses Gesetzentwurfes ist „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 BSIG-E gelten nicht als Geschäftsleitung. (s. § 2 Nr. 13 des Gesetzentwurf Stand 30.07.2025).

Unabhängig von dieser engen Definition kann es trotzdem sinnvoll sein, die Schulungspflicht auch auf andere Personen im Unternehmen auszuweiten, die in quasi-äquivalenten Positionen im Unternehmen arbeiten oder den Geschäftsleitungen zuarbeiten.

1.2 Intervall und Dauer von Schulungen

Das NIS-2-Umsetzungsgesetz gibt keine Intervalle zur Durchführung vor, aber in der Gesetzesbegründung eine Orientierung, wie oft Schulungen mindestens durchgeführt werden müssen.

Art. 20 Abs. 2 NIS-2-RL und § 38 Abs. 3 BSIG-E verlangen, dass Geschäftsleitungen und nach § 43 Abs. 3 BSIG-E Leitungen von bwE und wE „regelmäßig an Schulungen teilnehmen [müssen], um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können."

Regelmäßig ist nicht näher definiert. Der deutsche Gesetzgeber schreibt in der Begründung zum NIS-2-Umsetzungsgesetz: "Als „regelmäßig" im Sinne dieser Vorschrift gelten Schulungen, die mindestens alle drei Jahre angeboten werden. Für Einrichtungen der Bundesverwaltung gilt abweichend § 43 Abs. 2 BSIG-E."

Unabhängig von der gesetzlichen Definition von „regelmäßig" als alle drei Jahre ist entscheidend, dass der in § 38 Abs. 1 BSIG-E geforderten Verantwortung der Geschäftsleitung effektiv nachgekommen wird.

Die Schulungsintervalle müssen dem Risiko angemessen sein und sich nach der Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen richten, wobei gewährleistet sein muss, dass informierte Entscheidungen getroffen werden können. Mindestens aber sollen die Schulungen alle drei Jahre stattfinden.

Sinnvolle Anhaltspunkte, von diesem Mindest-Intervall abzuweichen können sein:

- Wechsel in der Geschäftsleitung
- Signifikante Änderungen in den Geschäftsprozessen
- Signifikante Änderungen der Risikoexposition
- Signifikante Änderungen bei implementierten oder geplanten Risikomanagementmaßnahmen

Zur Dauer der Schulungen macht der Gesetzgeber keine Vorgaben, geht aber in der Gesetzesbegründung von durchschnittlich halbtägigen Schulungen (vier Stunden) aus.

Die Dauer einer Schulung kann je nach Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen die vom Gesetzgeber veranschlagten vier Stunden auch deutlich überschreiten. Es ist entscheidend, dass alle geforderten Kenntnisse und Fähigkeiten sinnvoll übermittelt werden.

1.3 Mögliche Schulungsanbieter

Aus Sicht des BSI können die Schulungen sowohl durch externe Schulungsanbieter, durch schon beauftragte Cybersicherheitsberatungsunternehmen als auch durch qualifiziertes internes Personal erfolgen. Wichtig dabei ist, dass nicht nur abstrakte Kenntnisse vermittelt werden, sondern dass diese immer auch die individuellen Begebenheiten der Einrichtung berücksichtigen, für die die Geschäftsleitung verantwortlich ist.

Insbesondere externe Schulungsanbieter müssen diese einrichtungsindividuellen Aspekte berücksichtigen, was u.U. höheren Aufwand bedeutet. Sinnvoll kann daher ein Modell sein, in dem allgemeine Inhalte von externen Anbietern oder Dienstleistern durch spezifische Inhalte ergänzt werden, die durch interne Cybersicherheitsexperten vermittelt werden.

1.4 Nachweis von Geschäftsleitungsschulungen

Eine Dokumentation über die Ableistung von Schulungen ist intern aufzubewahren und auf Verlangen den zuständigen Behörden bzw. „unabhängigen Stellen" (gem. § 61 Abs. 1 BSIG-E i.V.m. § 62 BSIG-E) vorzulegen.

Bei solchen Aufsichtsmaßnahmen des BSI nach §§ 61 und 62 BSIG-E werden in Audits, Prüfungen, Zertifizierungen oder Nachweisen (gemäß § 61 Abs. 3 BSIG-E) die Einhaltung der Verpflichtungen (u.a. auch die Schulungspflicht) für wichtige und besonders wichtige Einrichtungen überprüft bzw. nachgewiesen.

Eine aussagekräftige Dokumentation enthält daher mindestens Informationen zu den Schulungsteilnehmenden, der Dauer der Schulung und den behandelten Inhalten.

Eine Prüfung für die Schulungsteilnehmenden, um „ausreichende Kenntnisse und Fähigkeiten“ belegen zu können ist weder gesetzlich noch durch das BSI verpflichtend vorgesehen.

2 Mögliche Schulungsinhalte

Aus Sicht des BSI sollten die Schulungen so aufgebaut sein, dass die zentralen Inhalte (also die in § 38 Abs. 3 BSIG-E geforderten) sinnvoll eingebettet werden. Dies ist wichtig, um die Verantwortung der Geschäftsführung einerseits durch vorbereitende Schulungsinhalte zu kontextualisieren und andererseits durch ergänzende Schulungsinhalte zu illustrieren.

Die folgenden Schulungsinhalte geben eine Empfehlung des BSI wieder, wie den Anforderungen aus § 38 Abs. 3 BSIG-E entsprochen werden kann.

Übergreifendes Ziel der Schulung sollte sein, die besondere Rolle der Geschäftsleitung für die Cybersicherheit von Einrichtungen herauszustellen, die Geschäftsleitung zu sensibilisieren und sie sinnvoll auf ihre Rolle vorzubereiten.

Erläuterung zu den Empfehlungen der Schulungsinhalte
Die folgenden Kapitel enthalten Empfehlungen des BSI dahingehend wie eine Umsetzung des § 38 Abs. 3 BSIG-E in Schulungsinhalten aussehen könnte.

Es folgt einer Systematik von SOLL bzw. KANN-Empfehlungen

SOLL/SOLLEN:
Diese Empfehlungen bilden nach Verständnis des BSI zentrale Kenntnisse, die ein Geschäftsführer im Rahmen einer Geschäftsleitungsschulung erwerben sollte, ab und werden dringend empfohlen.

KANN/KÖNNEN:
Diese Empfehlungen bilden nach Verständnis des BSI ergänzende Kenntnisse ab, die ein Geschäftsführer im Rahmen einer Geschäftsleitungsschulung erwerben könnte, und werden fakultativ empfohlen.

2.1 Vorbereitende Inhalte

Als Grundlage für die Kerninhalte sollten Geschäftsleitungen einen kurzen Überblick über die NIS-2-Richtlinie sowie deren nationale Umsetzung erhalten. Dabei sind insbesondere die gesetzlichen Pflichten für wichtige und besonders wichtige Einrichtungen zu vermitteln. Zentral ist zudem das Verständnis der persönlichen Verantwortung der Geschäftsleitungen gemäß § 38 BSIG-E einschließlich ihrer Verpflichtung zur Umsetzung und Überwachung von Risikomanagementmaßnahmen sowie zur regelmäßigen Teilnahme an Schulungen. Diese vorbereitenden Inhalte schaffen die Grundlage für das Verständnis der nachfolgenden Schulungsschwerpunkte.

2.1.1 Überblick NIS-2-Richtlinie

- Geschäftsleitungen SOLLEN die übergreifenden Inhalte und Ziele der NIS-2-Richtlinie bzw. deren nationaler Umsetzung kennen.
- Geschäftsleitungen SOLL der Geltungsbereich der NIS-2-Richtlinie bzw. deren nationaler Umsetzung vermittelt werden.
- Geschäftsleitungen KANN die Historie der Cybersicherheitsgesetzgebung vermittelt werden.
- Geschäftsleitungen KANN die Interaktion der NIS-2-Richtlinie mit weiteren nationalen oder europäischen Cybersicherheitsregulierungen vermittelt werden.

2.1.2 Umsetzung und Dokumentation von Risikomanagementmaßnahmen

- Geschäftsleitungen SOLLEN einen Überblick über die Pflichten aus § 30 BSIG-E erhalten.
- Geschäftsleitungen SOLLEN wissen, dass Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen und dokumentieren müssen.

- Geschäftsleitungen SOLLEN wissen, dass die Risikomanagementmaßnahmen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst geringhalten sollen.
- Geschäftsleitungen SOLLEN wissen, dass das Risikomanagement alle informationstechnischen Systeme, Komponenten und Prozesse, die Unternehmen für die Erbringung ihrer Dienste nutzen, adressieren muss.
- Geschäftsleitungen SOLLEN wissen, dass die Maßnahmen den jeweils aktuellen Stand der Technik einhalten sollen, einschlägige europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen müssen.
- Geschäftsleitungen SOLL die Bewertung der Verhältnismäßigkeit von Maßnahmen vermittelt werden.
- Geschäftsleitungen SOLLEN die Mindestanforderungen aus § 30 Abs. 2 BSIG-E vermittelt werden.

2.1.3 Melde- und Unterrichtungspflichten

- Geschäftsleitungen SOLLEN die Meldepflicht für erhebliche Sicherheitsvorfälle kennen.
- Geschäftsleitungen SOLL das dreistufige Melderegime mit früher Erstmeldung, Meldung und Abschlussmeldungen und deren Fristen vermittelt werden.
- Geschäftsleitungen SOLL die Möglichkeit von Zwischen- und Fortschrittsmeldungen im Meldeprozess vermittelt werden.
- Geschäftsleitungen SOLLEN die Meldeinhalte im Melderegime kennen.
- Geschäftsleitungen SOLLEN die Unterrichtungspflichten des BSI kennen.
- Geschäftsleitungen SOLLEN über Rückmeldungen des BSI bei Meldungen informiert werden.

2.1.4 Registrierungspflicht und ggf. besondere Registrierungspflichten

- Geschäftsleitungen SOLLEN die Registrierungspflicht und -frist für wichtige und besonders wichtige Einrichtungen kennen.
- Geschäftsleitungen KÖNNEN die verpflichtenden Angaben bei der Registrierung vermittelt werden.
- Geschäftsleitungen SOLLEN die Möglichkeit für Registrierungen durch das BSI kennen.
- Geschäftsleitungen SOLLEN über Änderung der Registrierungsangaben und deren Fristen informiert werden.
- Geschäftsleitungen SOLLEN ggf. über besondere Registrierungspflichten für Betreiber kritischer Anlagen informiert werden.
- Geschäftsleitungen SOLLEN ggf. über besondere Registrierungspflichten für Einrichtungen der Sektoren digitale Dienste und digitale Infrastrukturen informiert werden.

2.1.5 Pflichten für Geschäftsleitungen

- Geschäftsleitungen SOLLEN ihre Pflicht zur Umsetzung und Überwachung von Risikomanagementmaßnahmen kennen.
- Geschäftsleitungen SOLLEN die mögliche Haftung der Geschäftsleitungen für schuldhaft verursachte Schäden kennen.
- Geschäftsleitungen SOLLEN die Schulungspflicht kennen.
- Geschäftsleitungen SOLLEN mögliche Sanktionierungen bei Verstößen gegen Verpflichtungen für Einrichtungen oder Geschäftsleitungen kennen.

2.2 Kerninhalte

Die in § 38 Abs. 3 BSIG-E vorgesehene Schulungspflicht für Geschäftsleitungen verfolgt das Ziel, ausreichende Kenntnisse und Fähigkeiten im Bereich der Informationssicherheit zu vermitteln, damit die Geschäftsleitung ihrer gesetzlichen Verantwortung für die Umsetzung und Überwachung von Risikomanagementmaßnahmen nachkommen kann. Die drei zentralen Themenbereiche der Schulung – Erkennung und Bewertung von Risiken, Risikomanagementmaßnahmen sowie die Beurteilung ihrer Auswirkungen auf die von der Einrichtung erbrachten Dienste – ergeben sich direkt aus dem Gesetz und bilden den inhaltlichen Kern der Schulung.

Die Erkennung und Bewertung von Risiken ist Voraussetzung für jede fundierte Managemententscheidung im Bereich der Cybersicherheit. Geschäftsleitungen müssen in die Lage versetzt werden, wesentliche Bedrohungen, deren Eintrittswahrscheinlichkeiten und potenzielle Auswirkungen grundlegend zu verstehen und einzuordnen – nicht im technischen Detail, aber auf strategischer Ebene.

Darauf aufbauend erfordert die Kenntnis von Risikomanagementmaßnahmen ein Verständnis für Art, Zweck und Wirkweise technischer und organisatorischer Schutzmaßnahmen. Die gesetzlichen Mindestmaßnahmen nach § 30 Abs. 2 BSIG-E sowie sektorspezifische oder einrichtungsbezogene Ergänzungen müssen bekannt sein, um deren Umsetzung beurteilen und überwachen zu können.

Schließlich ist die Fähigkeit zur Beurteilung der Auswirkungen entscheidend, um Risiken und Maßnahmen im Kontext der betrieblichen Realität bewerten zu können. Dies betrifft insbesondere die Auswirkungen auf Verfügbarkeit, Integrität und Vertraulichkeit der Dienste sowie auf wirtschaftliche und regulatorische Rahmenbedingungen. Die reine Wissensvermittlung zu Risikoanalyse und Risikomanagementmaßnahmen ist nicht ausreichend. Geschäftsleitungen müssen auch und vor allem die Auswirkungen auf die betriebsinternen Prozesse und das ganzheitliche Risikomanagement der Einrichtung kennen und verstehen.

2.2.1 Risikoanalyse (Erkennung und Bewertung von Risiken)

- Geschäftsleitungen SOLLEN einen Überblick über Sinn, Ziele und zentrale Begriffe des Risikomanagements als systematischer Prozess zur Identifizierung, Bewertung und Steuerung von Risiken erhalten.
- Geschäftsleitungen SOLLEN verstehen, welche Rolle das Risikomanagement im Gesamtkontext der NIS-2-Richtlinie spielt.
- Geschäftsleitungen SOLLEN verstehen, dass Risikomanagement aus Risikoidentifikation, Risikoanalyse, Risikobehandlung und Risikoüberwachung besteht.
- Geschäftsleitungen SOLLEN wissen, dass es für das Risikomanagement etablierte nationale und internationale Standards gibt, an denen man sich orientieren kann.
- Geschäftsleitungen SOLLEN einen Überblick über Methoden und Ziele der Risikoanalyse erhalten.
- Geschäftsleitungen SOLLEN wissen, wie man Risiken für die Einrichtungen identifiziert.
- Geschäftsleitungen SOLLEN wissen, was (physische, digitale, menschliche, prozessuale, immaterielle) Assets sind und wie sie Assets der eigenen Einrichtung identifizieren können.
- Geschäftsleitungen SOLLEN einen Überblick über mögliche technische und physische Gefährdungen erhalten.
- Geschäftsleitungen SOLLEN einen Überblick über mögliche technische und physische Schwachstellen erhalten.
- Geschäftsleitungen SOLLEN mit den Grundbegriffen der Risikobewertung vertraut gemacht werden, z. B. Eintrittswahrscheinlichkeit, Schadensausmaß und Risikoakzeptanz.

- Geschäftsleitungen SOLLEN wissen, dass auch sogenannte „nicht-technische Risiken“ (z. B. durch menschliches Fehlverhalten, Lieferkettenprobleme oder organisatorische Schwächen) Teil der Risikobetrachtung sein können.
- Geschäftsleitungen SOLLEN die möglichen Schadensarten (finanziell, reputativ, betrieblich, rechtlich, technisch, personenbezogen etc.) kennen.
- Geschäftsleitungen SOLLEN verstehen, dass die Risikobewertung nicht nur technische Aspekte betrifft, sondern auch wirtschaftliche, rechtliche und reputative Folgen berücksichtigen muss.
- Geschäftsleitungen SOLLEN wissen, dass Risikomanagement ein kontinuierlicher Prozess ist, der regelmäßige Überprüfung und Anpassung erfordert.

2.2.2 Risikomanagementmaßnahmen

- Geschäftsleitungen SOLLEN die in § 30 Abs. 2 BSIG-E genannten Mindestmaßnahmen kennen und deren Bedeutung für ihre Einrichtung nachvollziehen können.
- Geschäftsleitungen SOLLEN einen Überblick über Risikomanagementmaßnahmen bekommen, der sich auf ihre Rolle als Management-Ebene und nicht auf tiefe technische Aspekte fokussiert.
- Geschäftsleitungen SOLLEN einen Überblick über Strategien zur Risikobehandlung (z. B. Vermeidung, Minderung, Übertragung, Akzeptanz) erhalten.
- Geschäftsleitungen SOLLEN verstehen, dass die Risikobehandlungsstrategien Übertragung und Akzeptanz für wichtige und besonders wichtige Einrichtungen eher nicht akzeptabel sind.
- Geschäftsleitungen SOLLEN grundlegende Prinzipien und Ziele von Maßnahmen zur Risikominderung kennen.
- Geschäftsleitungen SOLLEN über alle weiteren Risikomanagementmaßnahmen informiert sein, die in der Einrichtung bereits implementiert wurden oder deren Einführung geplant ist.
- Geschäftsleitungen SOLLEN auch Alternativen zu bestehenden oder geplanten Maßnahmen kennen, um die Angemessenheit der getroffenen Entscheidungen besser einschätzen zu können.
- Geschäftsleitungen SOLLEN verstehen, dass technische und organisatorische Maßnahmen aufeinander abgestimmt und regelmäßig überprüft werden müssen.
- Geschäftsleitungen SOLLEN wissen, dass Maßnahmen den Stand der Technik einhalten und verhältnismäßig sein müssen.
- Geschäftsleitungen SOLLEN einschätzen können, wie sich technische und organisatorische Maßnahmen auf Geschäftsprozesse, Ressourcenbedarf und Resilienz der Einrichtung auswirken.
- Geschäftsleitungen SOLLEN mit typischen Zielkonflikten im Risikomanagement (z. B. Sicherheit vs. Wirtschaftlichkeit) vertraut gemacht werden, um fundierte Entscheidungen mittragen zu können.
- Geschäftsleitungen SOLLEN wissen, dass Maßnahmen dokumentiert, nachvollziehbar begründet und kontinuierlich weiterentwickelt werden müssen.

2.2.3 Auswirkungen von Risiken und Risikomanagementmaßnahmen

- Geschäftsleitungen SOLLEN die Fähigkeit entwickeln, Risiken und geeignete Maßnahmen gemeinsam zu bewerten und daraus Handlungserfordernisse für die Dienstleistungserbringung abzuleiten.
- Geschäftsleitungen SOLLEN beurteilen können, welche Auswirkungen bestimmte Risiken auf die Verfügbarkeit, Integrität und Vertraulichkeit der erbrachten Dienste haben können.
- Geschäftsleitungen SOLLEN verstehen, wie sich Sicherheitsvorfälle konkret auf die Leistungserbringung, Kundenbeziehungen und gesetzliche Verpflichtungen der Einrichtung auswirken können.

- Geschäftsleitungen SOLLEN die potenziellen wirtschaftlichen, rechtlichen und reputativen Folgen unzureichender Risikobehandlung einschätzen können.
- Geschäftsleitungen SOLLEN erkennen, wie sich präventive und reaktive Maßnahmen zur Risikobehandlung auf Betriebsabläufe und Dienstkontinuität auswirken.
- Geschäftsleitungen SOLLEN verstehen, welche Abhängigkeiten zwischen IT-Systemen, Prozessen und Dienstleistungen bestehen und wie sich Störungen in einem Bereich auf andere auswirken können (Dominoeffekte).
- Geschäftsleitungen SOLLEN in die Lage versetzt werden, Cybersicherheitsrisiken als Geschäftsrisiken einzuordnen und entsprechende Managemententscheidungen zu treffen oder zu unterstützen.
- Geschäftsleitungen SOLLEN bewerten können, wie sich Investitionen in Cybersicherheit auf die langfristige Stabilität und Resilienz der Einrichtung auswirken.
- Geschäftsleitungen SOLLEN verstehen, dass eine unzureichende Umsetzung von Risikomanagementmaßnahmen zu aufsichtsrechtlichen Maßnahmen oder Haftungsrisiken führen kann.
- Geschäftsleitungen SOLLEN die Auswirkungen unterschiedlicher Risikobehandlungsstrategien (z. B. Risikotransfer vs. Risikominderung) auf die Dienstqualität und -verfügbarkeit beurteilen können.
- Geschäftsleitungen SOLLEN in die Lage versetzt werden, Zielkonflikte zwischen Sicherheitsmaßnahmen und Dienstleistungserbringung zu erkennen und ausgewogen zu bewerten.
- Geschäftsleitungen SOLLEN verstehen, dass die Bewertung von Risiken und Maßnahmen in den Kontext der strategischen Gesamtverantwortung fällt und Grundlage für haftungs- und aufsichtsrelevante Entscheidungen ist.
- Geschäftsleitungen SOLLEN Risikomanagementmaßnahmen in das ganzheitliche Risikomanagement der Einrichtung einbinden.
- Geschäftsleitungen SOLL vermittelt werden, dass ausreichend Ressourcen (Budget, Personal) für die Umsetzung des Risikomanagements bereitgestellt werden müssen.

2.3 Ergänzende Inhalte

Ergänzend zu den Kerninhalten sollten Schulungen sektor- und einrichtungsspezifische Anforderungen berücksichtigen, um den Bezug zur konkreten Praxis herzustellen. Darüber hinaus erhöhen Szenarien, Übungen und Fallstudien die Anwendungsorientierung der Schulung und unterstützen die Geschäftsleitungen dabei, Risiken und Maßnahmen im eigenen Organisationskontext besser einschätzen zu können.

2.3.1 Sektor- und einrichtungsspezifische Inhalte

Ergänzend zu den allgemeinen Kerninhalten ist es sinnvoll, sektor- und einrichtungsspezifische Inhalte zu berücksichtigen. Nur wenn Geschäftsleitungen die Anforderungen, typischen Risiken und regulatorischen Rahmenbedingungen ihres jeweiligen Sektors kennen, können sie Risiken realistisch einschätzen und geeignete Maßnahmen mittragen. Dies umfasst insbesondere die besonderen Pflichten sowie relevante branchenspezifische Vorgaben, wie z. B. B3S, ISO-Normen oder sektorspezifische Sicherheitskataloge. Ebenso relevant sind die typischen Bedrohungsszenarien des jeweiligen Sektors sowie die zentralen IT-gestützten Geschäftsprozesse der eigenen Einrichtung. Die Vermittlung dieser Inhalte unterstützt eine wirksame, kontextbezogene Risikobewertung und fördert die Entscheidungsfähigkeit der Geschäftsleitung im spezifischen Organisationskontext.

2.3.2 Szenarien, Übungen und Fallstudien

Risikomanagement und die Rolle der Geschäftsleitungen können sehr abstrakt und wenig greifbar sein. Schulungen können die vermittelten Inhalte mit Hilfe von Beispielszenarien, interaktiven Übungen oder Fallstudien handhabbarer machen. Diese Formate ermöglichen es den Geschäftsleitungen, das erworbene Wissen auf konkrete Situationen zu übertragen und die eigene Entscheidungs- und Beurteilungskompetenz realitätsnah zu erproben. Besonders wirksam sind Beispiele, die typische Bedrohungslagen, Schwachstellen oder Entscheidungssituationen im eigenen Sektor oder der konkreten Einrichtung abbilden. Ziel ist es, die Wechselwirkungen zwischen Risiken, Maßnahmen und Auswirkungen nachvollziehbar zu machen und die Fähigkeit zu fördern, Risiken unternehmerisch einzuordnen und tragfähige Entscheidungen auf Basis begrenzter Informationen zu treffen.

3 Leitfragen für Geschäftsleitungen

Die nachfolgenden Leitfragen stellen eine Empfehlung des BSI dar, die Geschäftsleitungen dabei unterstützen soll, die in der NIS-2-Richtlinie geforderten Pflichten angemessen zu überwachen und zu verwalten. Es soll einen kompakten Überblick darüber geben, welche Fragen im Rahmen von Schulungen der Geschäftsleitung beantwortet werden sollten – und mit welchen Antworten die Geschäftsleitung sich nicht zufriedengegeben darf. Die enthaltenen Informationen beschränken sich hierbei bewusst auf die wesentlichen Grundlagen, um eine klare Orientierung zu bieten.

Die folgenden Leitfragen bieten eine strukturierte Hilfestellung zur Schulung von Geschäftsleitungen – praxisnah und verantwortungsorientiert. Im Mittelpunkt stehen die in Kapitel 2 beschriebenen Schulungsinhalte sowie die zehn Maßnahmen des Cyberrisikomanagements gemäß NIS-2, zu denen jeweils zentrale Leitfragen formuliert wurden. Diese Fragen sollen helfen, das eigene Verantwortungsbewusstsein zu schärfen, Umsetzungslücken zu erkennen und den Dialog mit internen und externen Sicherheitspartnern zu führen.

Ziel ist es, Verantwortlichkeiten und Wirkungszusammenhänge deutlich zu machen, nicht, technische Details zu vermitteln. Die Geschäftsleitung trägt die strategische Verantwortung für die Umsetzung dieser Maßnahmen und muss daher wissen, worauf sie besonderes Augenmerk legen sollte. Die nachfolgenden Fragen und Einschätzungen dienen als Orientierung, welche Aspekte gezielt nachgefragt, bewertet und fortlaufend verbessert werden sollten.

Um diesen Anspruch in der Praxis greifbar zu machen, wurde jede der zehn Maßnahmen in Form einer strukturierten Leitfrage aufbereitet. Diese Methodik stellt der Geschäftsleitung eine zentrale Frage, die direkt auf die Umsetzungspflichten der jeweiligen Maßnahme zielt. Eine kurze Darstellung der jeweiligen Relevanz („Warum diese Frage wichtig ist“), ein exemplarisches Beispiel für eine zielführende, zukunftsorientierte Antwort sowie Hinweise auf typische Reaktionen, die ein vertieftes Nachfragen erforderlich machen, ergänzen jede Leitfrage. Diese Struktur soll dabei helfen, den Überblick zu behalten, Verantwortlichkeiten zu klären und die eigene Steuerungsfähigkeit systematisch weiterzuentwickeln.

3.1 Überblick NIS-2-Richtlinie

Frage:
Wie stellen wir sicher, dass die Geschäftsleitung die Inhalte, Ziele und den Geltungsbereich der NIS-2-Richtlinie kennt und versteht?

Warum diese Frage wichtig ist:
Nur wenn die Inhalte und Ziele der NIS-2-Richtlinie verstanden werden, kann die Geschäftsleitung ihre Verantwortung strategisch einordnen und die Umsetzung der Pflichten steuern. Das Wissen um den Geltungsbereich ist entscheidend, um festzustellen, welche Teile der Regulierung für die eigene Einrichtung relevant sind.

Hilfreiche Antwort:
Wir haben eine verständliche Übersicht erstellt, die die Ziele der NIS-2 (z. B. Stärkung der Cybersicherheit, Harmonisierung in Europa) sowie die für uns geltenden Pflichten erläutert. Diese Übersicht wird regelmäßig überprüft, in Schulungen vermittelt und mit branchenspezifischen Vorgaben abgeglichen.

Antworten, die weitere Nachfrage erfordern:

- „Wir wissen nicht genau, was mit NIS-2 erreicht werden soll.“
- „Der Geltungsbereich ist uns unklar.“
- „Wir verlassen uns darauf, dass nur die IT-Abteilung sich damit beschäftigt.“

3.2 Umsetzung und Dokumentation von Risikomanagementmaßnahmen

Frage:
Wie stellen wir sicher, dass unsere Risikomanagementmaßnahmen den gesetzlichen Anforderungen aus § 30 BSIG-E entsprechen, dokumentiert sind und regelmäßig auf ihre Wirksamkeit geprüft werden?

Warum diese Frage wichtig ist:
Die Umsetzung und Dokumentation von Risikomanagementmaßnahmen sind eine Kernpflicht. Ohne systematische Dokumentation können weder Nachweise gegenüber Aufsichtsbehörden geführt noch Verbesserungen im Sicherheitsniveau sichergestellt werden.

Hilfreiche Antwort:
Unsere Risikomanagementmaßnahmen decken alle relevanten Systeme, Prozesse und Komponenten ab, sind dokumentiert und werden regelmäßig gegen den Stand der Technik sowie gegen die Mindestanforderungen aus § 30 BSIG-E geprüft. Ergebnisse fließen in unser Informationssicherheitsmanagementsystem (ISMS) und in Geschäftsleitungsberichte ein.

Antworten, die weitere Nachfrage erfordern:

- „Wir haben keine systematische Dokumentation."
- „Das erledigt die IT-Abteilung, wir haben keinen Überblick."
- „Wir prüfen nicht regelmäßig den Stand der Technik gegen."

3.3 Melde- und Unterrichtungspflichten

Frage:
Wie stellen wir sicher, dass wir klar definieren können, was ein erheblicher Sicherheitsvorfall ist, und dass solche Vorfälle fristgerecht und vollständig nach dem vorgeschriebenen Melderegime an die zuständigen Aufsichtsbehörden gemeldet werden?

Warum diese Frage wichtig ist:
Die NIS-2 sieht ein verbindliches, fristgebundenes Meldesystem vor. Versäumnisse können zu Sanktionen führen und das Vertrauen von Partnern und Kunden beeinträchtigen. Nur wenn klar ist, welche Vorfälle meldepflichtig sind und wie das Melderegime funktioniert, kann die Einrichtung rechtssicher handeln.

Hilfreiche Antwort:
Wir haben Kriterien zur Einstufung erheblicher Sicherheitsvorfälle definiert und in unsere Prozesse integriert. Festgelegte Meldeabläufe stellen sicher, dass Erstmeldungen innerhalb von 24 Stunden sowie Folge- und Abschlussmeldungen nach definierten Fristen erfolgen. Zuständigkeiten, Eskalationsketten und Inhalte sind dokumentiert und in Notfallübungen erprobt. Rückmeldungen des BSI werden systematisch ausgewertet.

Antworten, die weitere Nachfrage erfordern:

- „Uns ist nicht klar, was als erheblicher Vorfall gilt."
- „Die Verantwortung ist nicht eindeutig geklärt."
- „Wir haben keinen Prozess, der regelt, wann und wie gemeldet werden muss."

3.4 Registrierungspflicht

Frage:
Wie stellen wir sicher, dass unsere Einrichtung fristgerecht registriert ist und Änderungen der Registrierungsangaben rechtzeitig an die zuständigen Aufsichtsbehörden übermittelt werden?

Warum diese Frage wichtig ist:
Die Registrierung ist eine gesetzliche Pflicht und Voraussetzung für die Teilnahme am Informationsaustausch. Fehler oder Versäumnisse können Sanktionen nach sich ziehen und die Handlungsfähigkeit im Krisenfall einschränken.

Hilfreiche Antwort:
Die Registrierung wurde fristgerecht durchgeführt und ist dokumentiert. Änderungen bei Verantwortlichen oder Kontaktdaten werden durch einen festgelegten Prozess laufend aktualisiert und an das BSI übermittelt.

Antworten, die weitere Nachfrage erfordern:

- „Wir sind uns nicht sicher, ob die Registrierung abgeschlossen wurde."
- „Es ist nicht festgelegt, wer für die Aktualisierung verantwortlich ist."
- „Wir haben keine Übersicht, welche Angaben registriert sind und wann sie angepasst werden müssen."

3.5 Pflichten für Geschäftsleitungen

Frage:
Wie nehmen wir als Geschäftsleitung unsere Pflichten zur Umsetzung und Überwachung von Risikomanagementmaßnahmen wahr, und inwieweit sind wir uns der Haftung, Schulungspflichten und möglichen Sanktionen bei Verstößen bewusst?

Warum diese Frage wichtig ist:
Die Geschäftsleitung trägt die rechtliche und persönliche Verantwortung für die Umsetzung der NIS-2-Anforderungen. Nur wenn diese Pflichten verstanden und aktiv wahrgenommen werden, können Haftungsrisiken vermieden und die Einrichtung rechtssicher gesteuert werden.

Hilfreiche Antwort:
Die Geschäftsleitung überprüft regelmäßig die Umsetzung von Risikomanagementmaßnahmen, nimmt selbst an verpflichtenden Schulungen teil und lässt sich regelmäßig über Risiken, Maßnahmen und deren Wirksamkeit berichten. Wir sind uns über die mögliche persönliche Haftung und über mögliche Sanktionen bewusst und berücksichtigen diese in unseren Entscheidungen.

Antworten, die weitere Nachfrage erfordern:

- „Das liegt vollständig in der Verantwortung der IT-Abteilung."
- „Wir haben uns mit Haftung oder Sanktionen nicht beschäftigt."
- „Schulungen für die Geschäftsleitung halten wir nicht für notwendig."

3.6 Risikomanagementmaßnahmen

Frage:
Wie stellen wir sicher, dass unsere Risikomanagementmaßnahmen den gesetzlichen Mindestanforderungen entsprechen, wirksam sind und im Einklang mit dem Stand der Technik regelmäßig überprüft und weiterentwickelt werden?

Warum diese Frage wichtig ist:
Risikomanagementmaßnahmen bilden das Herzstück der NIS-2-Anforderungen. Ohne klare Strategien zur Behandlung von Risiken (Vermeidung, Minderung, Übertragung, Akzeptanz) und deren kontinuierliche Anpassung an neue Bedrohungen bleiben die Schutzmaßnahmen wirkungslos. Die Geschäftsleitung muss wissen, welche Maßnahmen existieren, wie sie wirken und wie sie dokumentiert werden.

Hilfreiche Antwort:
Wir setzen die in § 30 Abs. 2 BSIG-E genannten Mindestmaßnahmen um und ergänzen diese durch weitere, auf unsere Einrichtung zugeschnittene Maßnahmen. Alle Maßnahmen werden dokumentiert, auf

Wirksamkeit überprüft und regelmäßig gegen den Stand der Technik validiert. Zielkonflikte (z. B. Sicherheit vs. Wirtschaftlichkeit) werden transparent gemacht und in der Geschäftsleitung entschieden.

Antworten, die weitere Nachfrage erfordern:

- „Wir wissen nicht, welche Mindestmaßnahmen nach § 30 Abs. 2 BSIG-E verpflichtend sind."
- „Wir haben keinen Überblick über die Wirksamkeit oder den aktuellen Stand unserer Maßnahmen."
- „Zielkonflikte zwischen Sicherheit und Geschäftsinteressen werden bei uns nicht systematisch betrachtet."

Die einzelnen Risikomanagementmaßnahmen stehen im besonderen Fokus der mit NIS-2 verbundenen Pflichten. Nachfolgend sind ebenfalls Leitfragen zu den einzelnen Cyberrisikomanagementmaßnahmen aufgeführt.

3.6.1 Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

Frage:
Wie stellen wir sicher, dass unsere Risikoanalyse regelmäßig erfolgt und auf aktuelle Bedrohungslagen sowie Sicherheitsstandards abgestimmt ist?

Warum diese Frage wichtig ist:
Eine fundierte Risikoanalyse ist die Grundlage für alle weiteren Sicherheitsmaßnahmen. Sie hilft, Risiken zu erkennen, zu bewerten und angemessen zu behandeln. Die NIS-2 fordert ein systematisches Vorgehen, das nicht nur technisch, sondern auch organisatorisch getragen wird.

Hilfreiche Antwort:
Wir haben ein dokumentiertes und etabliertes Verfahren zur Risikoanalyse, das mindestens jährlich durchgeführt wird. Es wird durch aktuelle Bedrohungsinformationen (z. B. CERT-Bund, BSI) ergänzt. Die Ergebnisse fließen direkt in unser ISMS ein und werden mit der Geschäftsführung abgestimmt.

Antworten, die weitere Nachfrage erfordern:

- „Das macht unsere IT, da haben wir keinen Überblick."
- „Wir haben letztes Jahr mal eine Analyse gemacht, das sollte noch passen."
- „Das ist mit unserer ISO-Zertifizierung schon abgedeckt."

3.6.2 Bewältigung von Sicherheitsvorfällen

Frage:
Haben wir einen klaren und regelmäßig getesteten Reaktionsplan für Sicherheitsvorfälle?

Warum diese Frage wichtig ist:
Ein effektiver Incident-Response-Plan kann Schäden und Ausfallzeiten erheblich reduzieren. Die Unternehmensleitung muss wissen, ob bei einem Vorfall Kommunikationswege, Eskalationsstufen und Entscheidungsbefugnisse klar definiert sind.

Hilfreiche Antwort:
Wir verfügen über ein Incident-Response-Framework mit definierten Rollen, Eskalationsketten und regelmäßigen Übungen. Der Plan umfasst technische Reaktion, Kommunikation, Dokumentation und Lessons Learned.

Antworten, die weitere Nachfrage erfordern:

- „Wir reagieren im Einzelfall spontan."
- „Die IT kümmert sich darum."

- „Wir hatten noch keinen Vorfall, daher ist das bisher kein Thema."

3.6.3 Aufrechterhaltung des Betriebs (Backup, Wiederherstellung, Krisenmanagement)

Frage:
Wie stellen wir sicher, dass unsere Betriebsprozesse bei einem Vorfall schnell wiederhergestellt werden können?

Warum diese Frage wichtig ist:
Ausfälle können fatale Folgen haben – besonders bei kritischen Anlagen. Nur wer regelmäßig Backups prüft und Wiederherstellungsprozesse testet, kann im Ernstfall die Betriebsfähigkeit aufrechterhalten.

Hilfreiche Antwort:
Unsere Backup-Strategie basiert auf dem 3-2-1-Prinzip. Wiederherstellungstests erfolgen quartalsweise, und es gibt ein abgestimmtes Krisenmanagement-Konzept mit Notfallkommunikation, Zuständigkeiten und Eskalationslogik.

Antworten, die weitere Nachfrage erfordern:

- „Wir sichern in der Cloud, das reicht."
- „Wiederherstellung? Haben wir noch nie getestet."
- „Der Notfallplan ist veraltet, aber wir arbeiten daran."

3.6.4 Sicherheit der Lieferkette

Frage:
Wie prüfen und steuern wir die IT-Sicherheitsmaßnahmen unserer Dienstleister und Lieferanten?

Warum diese Frage wichtig ist:
Angreifende nutzen zunehmend Schwachstellen bei Dritten als Einfallstor. Die Lieferkette ist ein häufiger blinder Fleck, obwohl dort oft sensible Daten und kritische Schnittstellen liegen.

Hilfreiche Antwort:
Wir führen Risikoanalysen bei Dritten durch, definieren Sicherheitsanforderungen in Verträgen und überprüfen diese regelmäßig (z. B. durch Audits oder Zertifikate). Zugriffe werden dokumentiert und minimiert.

Antworten, die weitere Nachfrage erfordern:

- „Wir vertrauen unseren Anbietern."
- „Jede Abteilung regelt das individuell."
- „Es gibt keine Übersicht, wer auf was zugreifen kann."

3.6.5 Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen

Frage:
Wie stellen wir sicher, dass Sicherheitsanforderungen bei der Beschaffung und Entwicklung von IT-Systemen berücksichtigt werden?

Warum diese Frage wichtig ist:
Sicherheit muss „by Design" mitgedacht werden – nicht erst nachträglich. Schwachstellen im Lebenszyklus von Systemen bergen hohe Risiken und können schwerwiegende Folgen haben.

Hilfreiche Antwort:
Unsere Beschaffungsrichtlinie beinhaltet Sicherheitsanforderungen. Entwicklungsprozesse folgen Secure-

Development-Prinzipien (z. B. OWASP). Schwachstellenmanagement und Patchzyklen sind etabliert und dokumentiert.

Antworten, die weitere Nachfrage erfordern:

- „Sicherheit kommt erst später dran."
- „Wir haben keinen Überblick über ungepatchte Systeme."
- „Lieferanten sind für Updates verantwortlich."

3.6.6 Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

Frage:
Wie bewerten wir, ob unsere Maßnahmen zur Cybersicherheit tatsächlich wirksam sind?

Warum diese Frage wichtig ist:
Nur durch Messung und Bewertung lassen sich Maßnahmen steuern, verbessern und priorisieren. Ohne Feedbackschleife bleibt Cybersicherheit reaktiv statt strategisch.

Hilfreiche Antwort:
Wir haben KPIs und KRIs definiert (z. B. Zeit bis zur Erkennung, Zeit bis zur Reaktion, Anzahl offener Schwachstellen), die regelmäßig berichtet und mit der Geschäftsführung diskutiert werden. Die Wirksamkeit wird jährlich auditiert.

Antworten, die weitere Nachfrage erfordern:

- „Wir messen nichts, aber bisher lief alles gut."
- „Unsere Sicherheitsmaßnahmen sind sowieso Standard."
- „Das wäre zu aufwendig."

3.6.7 Cyberhygiene und Schulungen

Frage:
Wie stellen wir sicher, dass alle Mitarbeitenden sicherheitsbewusst handeln?

Warum diese Frage wichtig ist:
Der Mensch ist oft das schwächste Glied. Ohne Schulung und klare Vorgaben sind technische Schutzmaßnahmen leicht zu umgehen oder unwirksam.

Hilfreiche Antwort:
Alle Mitarbeitenden durchlaufen verpflichtende Schulungen zur Cyberhygiene (jährlich wiederholt). Es gibt Awareness-Kampagnen, Phishing-Tests und klar kommunizierte Verhaltensrichtlinien.

Antworten, die weitere Nachfrage erfordern:

- „Nur die IT-Abteilung bekommt Schulungen."
- „Wir schicken ein PDF mit Tipps rum."
- „Wir hatten einmal ein Training, das reicht."

3.6.8 Einsatz von Kryptografie und Verschlüsselung

Frage:
Welche Verfahren setzen wir ein, um sensible Informationen zu verschlüsseln?

Warum diese Frage wichtig ist:
Verschlüsselung ist ein zentrales Mittel zum Schutz von Vertraulichkeit und Integrität. Fehlen klare Vorgaben, kann es zu Datenverlust oder Datenlecks kommen – auch unbeabsichtigt.

Hilfreiche Antwort:
Wir verwenden anerkannte, starke Verschlüsselungsverfahren (z. B. AES-256, TLS 1.3). Es gibt Vorgaben für Verschlüsselung bei Datenübertragung und -speicherung sowie eine zentrale Schlüsselverwaltung.

Antworten, die weitere Nachfrage erfordern:

- „Wir verschlüsseln nur E-Mails nach Bedarf."
- „Unsere Tools verschlüsseln automatisch, hoffen wir."
- „Das ist ein Thema für später."

3.6.9 Sicherheit des Personals, Zugriffskontrolle und Asset-Management

Frage:
Wie regeln und dokumentieren wir, wer worauf Zugriff hat – und warum?

Warum diese Frage wichtig ist:
Zugriffsrechte definieren den möglichen Schaden eines Angreifenden. Überprivilegierungen, fehlende Rezertifizierungen oder vergessene Zugänge sind häufige Schwachstellen.

Hilfreiche Antwort:
Unsere Rollen- und Berechtigungskonzepte basieren auf dem Least-Privilege-Prinzip. Rechte werden regelmäßig rezertifiziert, Veränderungen automatisch erfasst. Ein zentrales Asset-Inventar existiert.

Antworten, die weitere Nachfrage erfordern:

- „Jeder kann überall drauf zugreifen, das ist einfacher."
- „Zugriffe werden manuell gepflegt – wenn wir es schaffen."
- „Wir haben kein zentrales Asset-Register."

3.6.10 Multi-Faktor-Authentifizierung und gesicherte Kommunikation

Frage:
Nutzen wir für kritische Systeme und Kommunikation durchgängig starke Authentifizierungs- und Verschlüsselungsverfahren?

Warum diese Frage wichtig ist:
Ein verlorenes Passwort darf keinen Komplettzugriff ermöglichen. Multi-Faktor-Authentifizierung (MFA), verschlüsselte Kommunikation und Notfallkanäle sind essenziell, um Spionage, Sabotage oder Erpressung zu verhindern.

Hilfreiche Antwort:
Wir setzen MFA unternehmensweit ein, besonders für kritische Systeme und externen Zugriff. Interne Kommunikation (Text, Audio, Video) erfolgt über gesicherte Kanäle. Notfallkommunikation ist redundant abgesichert.

Antworten, die weitere Nachfrage erfordern:

- „Passwort reicht uns."
- „Wir prüfen MFA gerade."
- „Die Geschäftsführung nutzt private Messenger."

3.7 Risikoanalyse (Erkennung und Bewertung von Risiken)

Frage:
Wie stellen wir sicher, dass unsere Risikoanalyse alle relevanten Assets, Bedrohungen, Schwachstellen und

Schadensarten umfasst – und dabei auch nicht-technische Risiken berücksichtigt und die Ergebnisse regelmäßig aktualisiert werden?

Warum diese Frage wichtig ist:
Eine umfassende Risikoanalyse ist die Grundlage jeder Entscheidung im Risikomanagement. Nur wenn technische wie nicht-technische Risiken erkannt und bewertet werden, können wir fundierte Maßnahmen ergreifen. Die Aktualität der Analyse ist entscheidend, da Bedrohungen und Schwachstellen sich laufend ändern.

Hilfreiche Antwort:
Wir haben ein dokumentiertes Verfahren, das regelmäßig durchgeführt wird, alle relevanten Systeme, Prozesse und Ressourcen und sich an nationalen sowie internationalen Standards (z. B. ISO 27005) orientiert. Nicht-technische Risiken wie organisatorische Schwächen oder Lieferkettenprobleme sind Teil der Analyse. Ergebnisse werden mindestens jährlich überprüft und mit der Geschäftsleitung abgestimmt.

Antworten, die weitere Nachfrage erfordern:

- „Unsere Risikoanalyse beschränkt sich nur auf IT-Systeme."
- „Wir konzentrieren uns bei der Bewertung ausschließlich auf technische Auswirkungen."
- „Wir haben keine festen Intervalle für die Aktualisierung der Analyse."

3.8 Auswirkungen von Risiken und Risikomanagementmaßnahmen

Frage:
Wie bewerten wir als Geschäftsleitung die Auswirkungen identifizierter Risiken und umgesetzter Maßnahmen auf Verfügbarkeit, Integrität, Vertraulichkeit und die wirtschaftliche Stabilität unserer Einrichtung?

Warum diese Frage wichtig ist:
Nur wenn Risiken und Maßnahmen im betrieblichen, rechtlichen und wirtschaftlichen Kontext verstanden werden, können fundierte Managemententscheidungen getroffen, Ressourcen richtig priorisiert und Haftungsrisiken vermieden werden.

Hilfreiche Antwort:
Wir führen regelmäßige Business-Impact-Analysen durch, die technische, organisatorische, rechtliche und wirtschaftliche Folgen berücksichtigen. Abhängigkeiten und Dominoeffekte werden analysiert, Investitionen in Cybersicherheit werden strategisch bewertet und die Ergebnisse in das ganzheitliche Risikomanagement integriert.

Antworten, die weitere Nachfrage erfordern:

- „Uns ist nicht klar, welche Auswirkungen Risiken über die reine IT hinaus haben können."
- „Wir wissen nicht, wie sich Störungen in einem Bereich auf andere Geschäftsprozesse auswirken könnten."
- „Wir haben keine Methode, um die wirtschaftlichen oder rechtlichen Folgen eines Vorfalls systematisch einzuschätzen."

3.9 Sektor- und einrichtungsspezifische Inhalte

Frage:
Wie berücksichtigen wir branchenspezifische Anforderungen, Bedrohungsszenarien und zentrale Geschäftsprozesse unserer Einrichtung im Risikomanagement?

Warum diese Frage wichtig ist:
Jede Branche hat eigene Risiken und regulatorische Rahmenbedingungen. Ohne diese Kenntnisse kann die Geschäftsleitung Risiken nicht realistisch einschätzen und keine wirksamen Maßnahmen mittragen.

Hilfreiche Antwort:
Wir orientieren uns an branchenspezifischen Sicherheitsstandards (z. B. B3S, ISO, sektorspezifische Sicherheitskataloge). Zudem analysieren wir regelmäßig die typischen Bedrohungsszenarien unseres Sektors und gleichen sie mit unseren zentralen Geschäftsprozessen ab. Diese Erkenntnisse fließen direkt in die Risikobewertung und in die Entscheidungen der Geschäftsleitung ein.

Antworten, die weitere Nachfrage erfordern:

- „Uns ist nicht bekannt, dass es branchenspezifische Vorgaben oder Standards gibt."
- „Wir wissen nicht, welche Bedrohungsszenarien für unseren Sektor typisch sind."
- „Die Rolle unserer zentralen Geschäftsprozesse in der Risikobetrachtung ist uns nicht klar."

3.10 Szenarien, Übungen und Fallstudien

Frage:
Wie üben wir als Geschäftsleitung den Umgang mit typischen Bedrohungslagen und Entscheidungssituationen, damit unsere Reaktions- und Beurteilungsfähigkeit realistisch getestet werden kann?

Warum diese Frage wichtig ist:
Theoretisches Wissen reicht nicht aus – erst durch Szenarien und Übungen zeigt sich, ob Prozesse, Rollen und Schnittstellen im Ernstfall funktionieren. So wird die Fähigkeit gestärkt, Risiken unternehmerisch einzuordnen und fundierte Entscheidungen auch unter Unsicherheit zu treffen.

Hilfreiche Antwort:
Wir führen regelmäßig (mindestens einmal jährlich) Szenario-Übungen oder Planspiele durch, die typische Bedrohungslagen unserer Branche abbilden. Dabei werden Entscheidungswege, Kommunikationsprozesse und Eskalationslogik getestet. Ergebnisse werden dokumentiert und dienen als Grundlage für Verbesserungsmaßnahmen.

Antworten, die weitere Nachfrage erfordern:

- „Wir haben bisher keine Szenarien oder Übungen durchgeführt."
- „Uns ist nicht klar, wie solche Übungen ablaufen und welchen Nutzen sie haben."
- „Es gibt keine feste Planung, wann und wie die Geschäftsleitung in Übungen einbezogen wird."