Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Schulung für Geschäftsleitungen

Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen wichtiger Einrichtungen und besonders wichtiger Einrichtungen nach dem BSI-Gesetz sowie für freiwillige Schulungen von Geschäftsleitungen nicht-regulierter Unternehmen

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	17.04.2026	Aktualisierte Veröffentlichung
0.9	30.09.2025	initiale Veröffentlichung

Tabelle 1: Änderungshistorie

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

Danksagung

Das Bundesamt für Sicherheit in der Informationstechnik hat die vorläufige Handreichung nach Inkrafttreten des novellierten BSI-Gesetzes aktualisiert und in einer Abstimmung mit Verbänden die ersten Erfahrungen der Wirtschaft mit der Handreichung aufgenommen. Wir danken für das konstruktive Feedback.

- Bitkom e. V.
- Deutsche Industrie- und Handelskammer
- Gesellschaft für Informatik e. V.
- Verband Deutscher Maschinen- und Anlagenbau e. V.
- Zentralverband des Deutschen Handwerks e. V.
- ZVEI e. V., Verband der Elektro- und Digitalindustrie

Inhalt

1 Schulungen für Geschäftsleitungen

Cybersicherheit ist Chefinnen- und Chefsache. Mit der fortschreitenden Digitalisierung nehmen auch die Gefahren zu, denen sich Organisationen im digitalen Raum ausgesetzt sehen. Cyberrisiken und auch Cybervorfälle nehmen zu und eine effiziente Abwehr wird immer komplexer. Angemessener und wirksamer Schutz vor diesen Gefahren ist dennoch möglich, bedarf jedoch konstanter Pflege, Umsicht und vor allem der richtigen Entscheidungen.

Risikomanagement für Geschäftsleitungen

Budgetierung, Risikoerkennung und -abwägung sowie Konzepte zur Bewältigung von Cybersicherheitsvorfällen sind nur einige der essenziellen Bausteine für eine gelungene und gelebte Cybersicherheitskultur. Geschäftsleitungen müssen zu all diesen Bausteinen Entscheidungen treffen und verantworten und tragen damit maßgeblich zu der Gestaltung dieser Cybersicherheitskultur bei. Dazu müssen Geschäftsleitungen ihre besondere Verantwortung verstehen, Risiken korrekt einschätzen und die Hintergründe jeglicher Entscheidungsvorlagen nachvollziehen können, um die richtigen Entscheidungen treffen zu können.

Diese Handreichung soll nicht der Ausbildung der Geschäftsleitungen zu Expertinnen und Experten im Risikomanagement dienen, sondern bei der Sensibilisierung und Befähigung von Geschäftsleitungen unterstützen, sodass diese informierte und fundierte Entscheidungen im Kontext des Cyberrisikos treffen können.

Regulierung und gesetzliche Pflichten

Während das BSI allen Organisationen empfiehlt, eine gelebte Cybersicherheitskultur zu etablieren, sind einige Einrichtungen entsprechend gesetzlich verpflichtet. Mit der Umsetzung der NIS-2-Richtlinie im novellierten BSI-Gesetz (BSIG) steigen die Anforderungen an Einrichtungen, 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 der Organisation und des Risikomanagements ist und kann diese Aufgabe auch nicht delegieren. Diese besondere Verantwortung der Geschäftsleitungen ist gesetzlich vorgeschrieben, ebenso wie eine Schulungspflicht für die Geschäftsleitungen.

Inhalt und Ziel der Handreichung

In dieser Handreichung gibt das BSI eine erste Hilfestellung sowohl für die Schulungspflicht als auch für alle anderen Unternehmen und Organisationen, die Risikomanagement auf der höchsten Ebene etablieren wollen. Diese Empfehlungen können grundsätzlich von allen Einrichtungen angewendet werden, für die die Schulungspflicht aus § 38 Absatz 3 BSIG gilt.

Sowohl Schulungsanbieter als auch Geschäftsleitungen können sich an dieser Handreichung orientieren, um dem Verständnis des BSI im Hinblick auf den Scope und den Anspruch der Schulungen zu entsprechen. Eine rechtliche Verpflichtung zur Verwendung der Handreichung besteht nicht.

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

Diese Handreichung soll keine abschließende Empfehlung für die Schulungen von Geschäftsleitungen darstellen, sondern das Verständnis des BSI für die notwendigen Schulungsinhalte sowohl für Geschäftsleitung aller Unternehmen als auch derer Einrichtungen, die die gesetzlichen Vorgaben erfüllen müssen, wiedergeben. Die Handreichung greift die essenziellen Fokuspunkte der gesetzlichen Vorgaben auf. Diese sind auch für nicht regulierte Einrichtungen relevant.

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 BSIG zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften 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 Absatz 1 BSIG die Geschäftsleitungen von regulierten Einrichtungen dazu, Risikomanagementmaßnahmen in den von ihnen geleiteten Einrichtungen umzusetzen und ihre Umsetzung zu überwachen. Kommen Geschäftsleitungen ihren Verpflichtungen nicht nach, können sie dafür ggf. haften. Für Geschäftsleitungen von Einrichtungen, die dieser Regulierung nicht unterliegen, gilt dies nicht. Dennoch empfiehlt das BSI allen Unternehmen, technisch-organisatorische Risikomanagementmaßnahmen umzusetzen.

Gesetzliche Schulungspflicht

Um ihren Verpflichtungen nachkommen zu können, sieht das Gesetz eine Schulungspflicht für Geschäftsleitungen vor. Diese ist gesondert von den Schulungen für Mitarbeitende (nach § 30 Absatz 2 Nummer 7 BSIG) zu betrachten.

Schulungen der Geschäftsleitungen schaffen über die reine Verpflichtung hinaus Mehrwerte für Personen und Einrichtungen. Das Auseinandersetzen mit der Thematik birgt das Potenzial und die Chance Steuerungsfähigkeit, Risikominimierung, Transparenz und Wettbewerbsfähigkeit der eigenen Einrichtung voranzubringen. Eine Nichtbeachtung der Pflicht oder ein Verzicht auf die freiwillige Schulung steigert besonders das finanzielle Risiko für Einrichtungen. Fehlen geeignete Maßnahmen gegen vermeidbare Risiken, kann ein Sicherheitsvorfall deutlich schneller existenzbedrohend sein.

Schulungen nach oder im Sinne von § 38 Absatz 3 BSIG sollen die Geschäftsleitungen mindestens in drei Bereichen mit Kenntnissen und Fähigkeiten ausstatten:

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 Einrichtungen. Trotzdem muss die Geschäftsleitung in der Lage sein, Cybersicherheitsrisiken sinnvoll einschätzen zu können und entsprechende Maßnahmen treffen können. Dies ist auch deshalb erforderlich, damit sie ausreichend finanzielle und personelle Ressourcen zu Umsetzung bereitstellen kann.

Risikomanagementpraktiken

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

Auch hier müssen die Geschäftsleitungen nicht selbst zu Expertinnen und Experten ausgebildet werden, sondern dafür sorgen, dass die richtigen Kompetenzen an den richtigen Stellen der Einrichtungen verfügbar sind und mit ausreichenden Mitteln ausgestattet sind. Dazu sollen Geschäftsleitungen verstehen, was mit den geforderten bzw. empfohlenen 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 – Erkennung und Bewertung von Risiken, Beurteilung der Auswirkung der Risiken und Risikomanagementpraktiken - adressieren. Ein Fokus etwa nur auf Risikomanagementmaßnahmen fällt hinter die gesetzlichen Anforderungen zurück und würde durch das BSI im Rahmen von Aufsichtsmaßnahmen auch als nicht ausreichend bewertet werden.

Diese Handreichung adressiert die folgenden Fragestellungen:

- Wer soll oder muss sich schulen lassen?
- Wie oft sollen oder müssen die Schulungen durchgeführt werden?
- Was können Formate für die Schulungen sein?
- Wer sollte Schulungen durchführen?
- Was sollten die Schulungsinhalte sein?
- Wie fügt sich die Schulungspflicht in die übergreifenden Regulierungen des BSIG ein?

1.1 Adressaten der Schulungspflicht

Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen sind in § 38 Absatz 3 BSIG verpflichtet, sich regelmäßig schulen zu lassen. Im Sinne des BSIG ist die „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 gelten nicht als Geschäftsleitung. (§ 2 Nummer 13 BSIG). Für Einrichtungen der Bundesverwaltung gilt statt § 38 Absatz 3 gleichlautend, § 43 Absatz 2 BSIG.

Alle Personen, die dieser Definition entsprechen, sind schulungspflichtig. Das BSI geht davon aus, dass die Schulungspflicht in der großen Mehrheit der Einrichtungen mehrere Personen trifft. Die Schulungspflicht ist eng verankert mit der gesetzlichen Pflicht der Geschäftsleitung, Risikomanagementmaßnahmen umzusetzen und deren Umsetzung zu überwachen. Die Schulungen sollen die Adressaten befähigen, dieser gesetzlichen Pflicht nachzukommen.

Weitere Adressaten

Es kann sinnvoll sein, die Schulungspflicht im Sinne des BSIG, bzw. die Schulungen für Geschäftsleitungen von nicht regulierten Einrichtungen auf weitere Personen auszuweiten, die den Geschäftsleitungen zuarbeiten, oder anderweitige Entscheidungsvollmacht innehaben.

1.2 Intervall und Dauer von Schulungen

Das BSIG macht zu Intervall und Dauer der verpflichtenden Schulungen von Geschäftsleitungen keine konkreten Vorgaben über den Begriff „*regelmäßig*“ hinaus.

§ 38 Absatz 3 BSIG (für wichtige (wE) und besonders wichtige Einrichtungen (bwE)) und § 43 Absatz 2 BSIG (für Einrichtungen der Bundesverwaltung) verlangen, dass (Geschäfts-) 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."*

Das BSI empfiehlt regulierten und nicht-regulierten Einrichtungen gleichermaßen die Schulungs-Intervalle und -Dauer dem Risiko angemessen zu wählen und sich nach der Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen zu richten, wobei gewährleistet sein muss, dass informierte Entscheidungen getroffen werden können.

Das BSI empfiehlt eine ausführliche initiale Schulung mit anschließenden regelmäßigen Folgeschulungen, um Geschäftsleitungen für ihre Aufgabe und Verantwortung (nach § 38 Absatz 1 BSIG) zu sensibilisieren. Sollten bereits eingespielte und akzeptierte regelmäßige Schulungsformate bestehen, können diese selbstverständlich um die Inhalte dieser Empfehlung erweitert werden.

Entscheidende Anhaltspunkte für die Wahl der Art und Dauer sowie des Intervalls der nachfolgenden Schulungen sollten in jedem Fall sein:

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

Die Dauer einer Schulung und das Intervall der Wiederholungen solcher Schulungen kann je nach Risikoexposition der Einrichtung und individuellen Fähigkeiten der Geschäftsleitungen gewählt werden. Es ist entscheidend, dass alle geforderten Kenntnisse und Fähigkeiten sinnvoll übermittelt werden.

Ob die Schulungsinhalte in regulierten Einrichtungen dabei in nur einer Schulung oder aufgeteilt auf mehrere Schulungen vermittelt werden, steht den Betroffenen frei. Wichtig ist, dass Geschäftsleitungen die Dauer und das Intervall der Schulungen stets an den oben genannten Kriterien ausgerichtet wählen sowie eine lückenlose Dokumentation über Datum, Zeitraum und Inhalte der durchgeführten Schulungen führen.

1.3 Schulungsformate

Risikomanagement und die Rolle der Geschäftsleitung dabei kann sehr abstrakt und wenig greifbar sein. Schulungen sollten die vermittelten Inhalte anhand von Beispielszenarien, interaktiven Übungen oder in Case Studies handhabbarer machen.

Es gibt verschiedene Ansätze und Modelle, der Schulungspflicht nachzukommen. Geschäftsleitungen müssen nicht unbedingt mehrstündige Unterrichtsblöcke absolvieren, wenn Risikomanagement auch in alternativen Formaten vermittelt werden kann. Insbesondere interaktive oder zeitlich dezentrale Formate sind gut geeignet, um den entscheidenden Bezug zwischen den Schulungsinhalten und Risikomanagement in der gelebten Praxis zu vermitteln.

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.

Folgende Formate sind eine nicht vollständige Liste von Beispielen für Schulungsformate abseits von klassischen Schulungen im „Frontalunterricht“. Diese Formate können beliebig kombiniert oder abgewandelt werden:

Risikomanagement-Quarterly

Ein fester Termin jedes Quartal, in dem der/die Informationssicherheitsbeauftragte (ISB) mit der gesamten Geschäftsleitung an konkreten Problemen und Fragestellungen der Einrichtung Konzepte des Risikomanagements und der Informationssicherheit vermittelt.

Tabletop Exercise/Planspiel

Moderierte Übung anhand von typischen Szenarien im Risikomanagement, um die wechselseitigen Beziehungen von Informationssicherheit (Risiken/Maßnahmen) und Management-Entscheidungen aufzuzeigen.

Audit-Simulation

Eine typische Prüfungssituation entsprechend der Methodik relevanter Audits (z. B. ISO 27001-Audit, KRITIS-Nachweisprüfung, künftiges Audit nach § 61 BSIG etc.) wird mit Beteiligung der Geschäftsleitungen als Spielern (Teilnehmenden) simuliert.

Management Red-/Blue-Teaming

Abwandlung von herkömmlichen Cyber-Übungen: Blue Team spielt Unternehmenssteuerung/Geschäftsleitung, Red Team spielt Angreifer/Krisenentwicklung. Fokus nicht auf tatsächliche technische Simulation, sondern Management-Entscheidungen vor/während Krisensituationen durch das Erleben von möglichen Angriffsszenarien und dem Erkennen geeigneter Maßnahmen.

Szenarien

Illustrierung von abstrakten Inhalten in konkreten sektor- und einrichtungsspezifischen Szenarien sollten regelmäßiger Bestandteil von Schulungen sein, um den Bezug zur eigenen Einrichtung und die Relevanz der vermittelten Inhalte darzulegen.

Übungen

Krisen-/Notfallübungen sind sinnvoll, nicht nur als Teil von Schulungen. Dies ist insbesondere effektiv, wenn die Geschäftsleitung und die IT-Sicherheitsexpertinnen und -Experten Übungsszenarien gemäß ihrer jeweiligen Rolle gemeinsam beüben.

Case-Studies

Das Aufzeigen von Entscheidungen und Fehlentscheidungen im Risikomanagement anhand von konkreten Case-Studies ist eine weitere sinnvolle Möglichkeit, Inhalte zu konkretisieren und deren Relevanz für Geschäftsleitungen greifbarer zu machen.

Live-Hacking

Um Risiken konkret und unmittelbar aufzuzeigen, kann ein Live-Hacking effektiv sein. Diese Demonstration ist eher als Zusatz zu anderen Schulungsformaten zu sehen.

1.4 Mögliche Schulungsanbieter

Aus Sicht des BSI können die Schulungen sowohl durch externe Schulungsanbieter, wie bspw. Cybersicherheitsberatungsunternehmen, als auch durch interne fachliche Stellen 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. Dabei ist eine ganzheitliche Betrachtung der Einrichtung notwendig um auf alle individuellen Gegebenheiten eingehen zu können. Die unternehmensindividuellen Inhalte sollten dabei u. a. kritische Geschäftsprozesse, Governance-Strukturen, die aktuelle Risikolage sowie konkrete Entscheidungsanlässe betrachten.

Externe Schulungsanbieter

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.

Schulung durch interne Stellen

Bei internen Schulungen sollten Einrichtungen umgekehrt die unabhängige Wissensgrundlage nicht aus den Augen verlieren. Erfolgt die Schulung ausschließlich durch interne Stellen, besteht die Gefahr struktureller Erkenntnisdefizite: Die Geschäftsleitung erfährt, wie Prozesse umgesetzt werden, kann jedoch deren rechtliche und risikotechnische Angemessenheit nicht eigenständig beurteilen. Beiträge externer, unabhängiger Risiko-, Compliance- und Rechtsexpertise können daher ein wesentlicher Bestandteil effektiver Governance sein.

1.5 Nachweis von Geschäftsleitungsschulungen

Die regelmäßige Teilnahme an Geschäftsleitungsschulungen sollten Einrichtungen nachvollziehbar und aussagekräftig dokumentieren. Eine Dokumentation über die Ableistung von Schulungen nach § 38 Absatz 3 BSIG ist intern aufzubewahren und auf Verlangen dem BSI bzw. den vom BSI beauftragten „*unabhängigen Stellen*“ (gem. § 61 Absatz 1 BSIG i. V. m. § 62 BSIG) vorzulegen. Bei solchen Aufsichtsmaßnahmen des BSI nach §§ 61 und 62 BSIG werden in Audits, Prüfungen, Zertifizierungen oder Nachweisen (gemäß § 61 Absatz 3 BSIG) die Einhaltung der Verpflichtungen (u. a. auch die Schulungspflicht) für wichtige und besonders wichtige Einrichtungen überprüft bzw. nachgewiesen.

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

Eine aussagekräftige Dokumentation enthält mindestens folgende Informationen:

- Angaben zum Schulungsanbieter/interne Stelle
- Angaben zu den beschulten Teilnehmenden (Name, Rolle/Funktion in der Organisation)
- Datum, Uhrzeit, Dauer der Schulungseinheiten
- Behandelte Unterrichtsinhalte/-formate und Bezüge zu den gesetzlichen Vorgaben aus § 38 Absatz 3 BSIG

Eine solche aussagekräftige Dokumentation kann nur die regelmäßige Teilnahme an Schulungen belegen, nicht aber die Vermittlung ausreichender Kenntnisse und Fertigkeiten.

Vielmehr wird sich der Lernerfolg der Schulungen in den Dokumentationen zur Entscheidungsfindung und Umsetzung aller anderen Pflichten des BSIG, insbesondere der Umsetzung der Risikomanagementmaßnahmen, widerspiegeln: Die Geschäftsleitung hat dann „ausreichend Kenntnissen und Fähigkeiten“ erlangt, wenn sie aktiv und nachvollziehbar an Entscheidungen im Risikomanagement mitwirkt und somit ihrer gesetzlichen Pflicht aus § 38 Absatz 1 BSIG nachkommt.

2 Empfehlungen für Schulungsinhalte

Übergreifendes Ziel

Wichtige und besonders wichtige Einrichtungen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen umsetzen und deren Geschäftsleitungen müssen ihren gesetzlichen Pflichten zur Umsetzung der Maßnahmen und zur Überwachung der Umsetzung nachkommen können. Die Befähigung der Geschäftsleitungen dazu ist das eigentliche und übergreifende Ziel der Geschäftsleitungsschulungen.

Empfehlungen statt Vorgaben

Die folgenden Schulungsinhalte geben eine Empfehlung des BSI wieder, wie den Anforderungen aus § 38 Absatz 3 BSIG entsprochen werden kann. Die Empfehlung gilt aber ebenso für alle Geschäftsleitungen von nicht regulierten Einrichtungen. Aus Sicht des BSI sollten alle Schulungen so aufgebaut sein, dass die Kerninhalte (also die in § 38 Absatz 3 BSIG geforderten) sinnvoll eingebettet werden. Dies ist wichtig, um die Verantwortung der Geschäftsführung durch unterstützende Schulungsinhalte zu kontextualisieren und zu illustrieren.

Priorisierung der Inhalte

Bei der Vermittlung dieser Inhalte muss personen- und funktionsangemessen priorisiert werden: Nicht allen Personen, die zur Geschäftsleitung gehören, müssen die gleichen Inhalte in gleicher Detailtiefe vermittelt werden. Schulungsinhalte müssen sich primär am übergreifenden Ziel orientieren, die Geschäftsleitungen auf ihre gesetzliche Rolle vorzubereiten. Wenn bei Geschäftsleitungen in Teilbereichen schon „ausreichende Kenntnisse und Fähigkeiten“ vorliegen, müssen diese in Schulungen oder Folgeschulungen nicht vermittelt werden. Diese Entscheidungen und deren Begründung müssen Einrichtungen aber nachvollziehbar dokumentieren.

Erläuterung zu den Empfehlungen der Schulungsinhalte

Die folgenden Kapitel enthalten Empfehlungen des BSI dahingehend wie eine Umsetzung des § 38 Absatz 3 BSIG oder eine freiwillige Orientierung daran in Schulungsinhalten aussehen könnte.

Es folgt einer Systematik von SOLL bzw. KANN-Empfehlungen.

SOLL/SOLLEN:

Diese Empfehlungen bilden nach Verständnis des BSI zentrale Inhalte einer Geschäftsleitungsschulung ab und werden dringend empfohlen.

KANN/KÖNNEN:

Diese Empfehlungen bilden nach Verständnis des BSI ergänzende Inhalte einer Geschäftsleitungsschulung ab und werden fakultativ empfohlen.

Die Empfehlungen sind als Checkliste gestaltet. Externe/interne Schulungsanbieter bzw. beschulte Geschäftsleitungen können so überprüfen, ob die Schulungen alle abstrakten Empfehlungen des BSI in konkrete Inhalte übertragen und vermittelt haben.

2.1 Kerninhalte

Die in § 38 Absatz 3 BSIG 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.

Kerninhalte der Schulung sind: Erkennung und Bewertung von Risiken, Risikomanagementmaßnahmen sowie die Beurteilung ihrer Auswirkungen.

Dieses Prinzip lässt sich ebenso auf freiwillige Schulungen für Geschäftsleitungen von nicht regulierten Einrichtungen übertragen und die nachfolgend empfohlenen Inhalte gelten für alle Einrichtungen gleichermaßen.

Risiken, Maßnahmen und Auswirkungen

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 Absatz 2 BSIG 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.

Sektor- und einrichtungsspezifische Inhalte

Ergänzend zu den allgemeinen Kerninhalten ist es sinnvoll, sektor- und einrichtungsspezifische Inhalte zu berücksichtigen. Ziel der Schulung ist es, die besondere Rolle der Geschäftsleitung für die Cybersicherheit von Einrichtungen herauszustellen, die Geschäftsleitung für ihre gesetzlichen Aufgaben zu sensibilisieren und sie sinnvoll auf ihre Rolle vorzubereiten. Nach und während der Schulungen muss daher ein Transfer auf die eigene Einrichtung und den eigenen Sektor stattfinden. 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 beispielsweise branchenspezifische Sicherheitsstandards (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 eigenen Organisationsrahmen.

2.1.1 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, wie Risiken identifiziert, bewertet und überwacht werden.
- Geschäftsleitungen SOLLEN zentrale Risikoquellen, Schwachstellen und Schutzbedarfe kennen und im Kontext der eigenen Einrichtung verstehen.
- Geschäftsleitungen SOLLEN mit den Grundbegriffen der Risikobewertung vertraut gemacht werden, beispielsweise Eintrittswahrscheinlichkeit, Schadensart und -ausmaß und Risikoakzeptanz.
- Geschäftsleitungen SOLLEN verstehen, dass Risikomanagement ein kontinuierlicher Prozess ist, der regelmäßige Überprüfung und Anpassung erfordert.

2.1.2 Risikomanagementpraktiken (Risikomanagementmaßnahmen)

- 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 die Maßnahmen alle informationstechnischen Systeme, Komponenten und Prozesse, die Einrichtungen für die Erbringung ihrer Dienste nutzen, adressieren müssen.
- Geschäftsleitungen SOLLEN wissen, dass die Maßnahmen den jeweils aktuellen Stand der Technik einhalten sollen, einschlägige europäischen und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen müssen.
- Geschäftsleitungen SOLLEN verstehen, wie Maßnahmen ausgewählt, umgesetzt, priorisiert und überprüft werden.
- Geschäftsleitungen SOLLEN einen Überblick über Strategien zur Risikobehandlung (beispielsweise Vermeidung, Minderung, Übertragung, Akzeptanz) erhalten.
- Geschäftsleitungen SOLLEN einen ihrer Funktion und Rolle angemessenen Überblick über wesentliche (implementierte und geplante) Maßnahmen der eigenen Einrichtung haben.
- Geschäftsleitungen SOLLEN wissen, dass Maßnahmen dokumentiert, nachvollziehbar begründet und kontinuierlich weiterentwickelt werden müssen.

2.1.3 Auswirkungen von Risiken und Risikomanagementmaßnahmen

- Geschäftsleitungen SOLLEN betriebliche, wirtschaftliche und regulatorische Auswirkungen einschätzen können.
- Geschäftsleitungen SOLLEN Risiken und Maßnahmen gemeinsam bewerten können.
- Geschäftsleitungen SOLLEN Cybersicherheitsrisiken als Geschäftsrisiken einordnen können.
- Geschäftsleitungen SOLLEN verstehen, dass Abhängigkeiten zwischen IT-Systemen, Prozessen und Dienstleistungen bestehen können und beispielhaft verstehen, wie sich Störungen in einem Bereich auf andere auswirken können.
- Geschäftsleitungen SOLLEN in die Lage versetzt werden, Zielkonflikte zwischen Sicherheitsmaßnahmen und Dienstleistungserbringung zu erkennen und ausgewogen zu bewerten.

2.2 Unterstützende Inhalte

Als Grundlage für die Kerninhalte sollten Geschäftsleitungen einen kurzen Überblick über die Regulierung des BSIG erhalten. Dabei sind insbesondere die gesetzlichen Pflichten für wichtige und besonders wichtige Einrichtungen und deren Geschäftsleitungen zu vermitteln. Diese Inhalte gehen nach Verständnis des BSI über die verpflichtenden Inhalte aus § 38 Absatz 3 hinaus, sind aber eine entscheidende kontextualisierende Information. Diese unterstützenden Inhalte zu den gesetzlichen Pflichten für regulierte Einrichtungen haben keine Relevanz für nicht regulierte Unternehmen.

- Geschäftsleitungen SOLLEN die übergreifenden Inhalte und Ziele der Regulierung von Einrichtungen durch das BSIG kennen.
- Geschäftsleitungen KANN die Historie der nationalen und europäischen Cybersicherheitsgesetzgebung vermittelt werden.
- Geschäftsleitungen KANN die Interaktion der Regulierung durch das BSIG mit weiteren, für die jeweilige Einrichtung relevanten, nationalen oder europäischen Cybersicherheitsregulierungen vermittelt werden.
- Geschäftsleitungen SOLLEN die Meldepflicht und -fristen für erhebliche Sicherheitsvorfälle kennen.

- Geschäftsleitungen SOLLEN die Registrierungspflicht und -frist für wichtige und besonders wichtige Einrichtungen kennen.
- Geschäftsleitungen KÖNNEN ggf. über besondere Registrierungspflichten für Betreiber kritischer Anlagen und Einrichtungen der Sektoren digitale Dienste und digitale Infrastrukturen informiert werden.
- 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 Pflicht kennen, regelmäßig an Geschäftsleitungsschulungen teilzunehmen.

3 Leitfragen für Geschäftsleitungen

Mit der Umsetzung der NIS-2-Richtlinie und damit einhergehenden Novellierung des BSIG steigen die Anforderungen an Einrichtungen, ihre Cybersicherheitsmaßnahmen systematisch zu planen, umzusetzen und die Umsetzung zu überwachen. Besonders im Fokus steht dabei die Verantwortung der Geschäftsleitung: Sie muss gewährleisten, dass Cybersicherheit integraler Bestandteil der Geschäfte der Einrichtung und des Risikomanagements ist.

Um die Pflichten der Geschäftsleitung wirkungsvoll wahrzunehmen und die Risikomanagementmaßnahmen wirksam in die eigene Organisation zu integrieren, reicht es nicht aus, technische Maßnahmen oder einzelne Vorschriften isoliert zu betrachten. Es braucht strukturiertes Nachfragen, strategische Einbindung und kontinuierliche Überprüfung – gesteuert aus der Geschäftsleitung.

Dieses Dokument stellt eine Empfehlung des BSI dar, die Geschäftsleitungen dabei unterstützen soll, die im novellierten BSIG geforderten Pflichten angemessen zu überwachen und zu verwalten. Es soll einen kompakten Überblick darüber geben, welche Fragen zu den Inhalten im Rahmen von Schulungen der Geschäftsleitung beantwortet werden sollten – und mit welchen Antworten sich nicht zufriedengegeben werden 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 BSIG, 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 nicht, technische Details zu vermitteln, sondern Verantwortlichkeit und Wirkung zu verdeutlichen: Geschäftsleitungen tragen die strategische Verantwortung für die Umsetzung dieser Maßnahmen – und müssen wissen, worauf sie achten müssen. Die hier dargestellten Fragen und Einschätzungen geben Orientierung, was sie konkret nachfragen, bewerten und verbessern 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 Erläuterung ihrer Relevanz („Warum diese Frage wichtig ist“), ein Beispiel für eine hilfreiche (zukunftsgerichtete) Antwort sowie Hinweise auf typische Reaktionen, bei denen weiter nachgehakt werden sollte („Antworten, die weitere Nachfragen erfordern“) ergänzen jede Frage. Diese Struktur soll dabei helfen, den Überblick zu behalten, Verantwortlichkeiten zu klären und die eigene Steuerungsfähigkeit systematisch weiterzuentwickeln.

3.1 Überblick NIS-2-Regulierung

Frage:

Wie stellen wir sicher, dass die Geschäftsleitung die Inhalte, Ziele und den Geltungsbereich des BSIG kennt und versteht?

Warum diese Frage wichtig ist:

Nur wenn die Inhalte und Ziele des BSIG 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 des BSIG sowie die für uns geltenden Pflichten erläutert. Diese Übersicht wird regelmäßig überprüft, in Schulungen vermittelt und mit branchenspezifischen Vorgaben abgeglichen.

Antworten, die weitere Nachfragen erfordern:

- „Wir wissen nicht genau, was mit der Regulierung durch das BSIG 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 entsprechen, dokumentiert sind und regelmäßig auf ihre Wirksamkeit geprüft werden?

Warum diese Frage wichtig ist:

Die Umsetzung und Dokumentation von Risikomanagementmaßnahmen ist 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 geprüft. Ergebnisse fließen in unser Informationssicherheitsmanagementsystem (ISMS) und in Geschäftsleitungsberichte ein.

Antworten, die weitere Nachfragen erfordern:

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

3.3 Melde- und Unterrichtungspflichten

Frage:

Wie stellen wir sicher, dass wir wissen, 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:

Das BSIG 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 Nachfragen 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 Nachfragen 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 wie 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 -Anforderungen des BSIG. 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 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 Nachfragen 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 BSIG-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 Absatz 2 BSIG 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 (beispielsweise Sicherheit vs. Wirtschaftlichkeit) werden transparent gemacht und in der Geschäftsleitung entschieden.

Antworten, die weitere Nachfragen erfordern:

- „Wir wissen nicht, welche Mindestmaßnahmen nach § 30 Absatz 2 BSIG 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 im Kontext der mit dem BSIG 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. Das BSIG 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 (beispielsweise CERT-Bund, BSI) ergänzt. Die Ergebnisse fließen direkt in unser ISMS ein und werden mit der Geschäftsführung abgestimmt.

Antworten, die weitere Nachfragen 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 Einrichtungsleitung 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 Nachfragen 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 Nachfragen 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 (beispielsweise durch Audits oder Zertifikate). Zugriffe werden dokumentiert und minimiert.

Antworten, die weitere Nachfragen 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 (beispielsweise OWASP). Schwachstellenmanagement und Patchzyklen sind etabliert und dokumentiert.

Antworten, die weitere Nachfragen 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 Cyber-Sicherheit tatsächlich wirksam sind?

Warum diese Frage wichtig ist:

Nur durch Messung und Bewertung lässt sich steuern, verbessern und priorisieren. Ohne Feedbackschleife bleibt Cybersicherheit reaktiv statt strategisch.

Hilfreiche Antwort:

Wir haben KPIs und KRIs definiert (beispielsweise 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 Nachfragen 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 Nachfragen 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 (beispielsweise AES-256, TLS 1.3). Es gibt Vorgaben für Verschlüsselung bei Datenübertragung und -speicherung sowie eine zentrale Schlüsselverwaltung.

Antworten, die weitere Nachfragen 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 durch einen 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 Nachfragen 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 einrichtungsweit ein, besonders für kritische Systeme und externen Zugriff. Interne Kommunikation (Text, Audio, Video) erfolgt über gesicherte Kanäle. Notfallkommunikation ist redundant abgesichert.

Antworten, die weitere Nachfragen 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 dass 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 fundierte Maßnahmen ergriffen werden. 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 abdeckt und an nationale sowie internationale Standards (beispielsweise ISO 27005) angelehnt ist. 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 Nachfragen 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 getroffener 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 Nachfragen 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 (beispielsweise 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 Nachfragen 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 Case-Studies

Frage:

Wie üben wir als Geschäftsleitung den Umgang mit typischen Bedrohungslagen und Entscheidungssituationen, um unsere Reaktions- und Beurteilungsfähigkeit realistisch zu testen?

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 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 Nachfragen 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."