NIS2 Geschäftsleitungsschulung

Verantwortung, Bewertung und Steuerung von Informationssicherheit

Schulung für Geschäftsführung und Management · Normative Grundlage: NIS2 (EU) 2022/2555 · BSIG · BSI-Standards

Folie 2

Was Sie heute mitnehmen

In den nächsten 4 Stunden erarbeiten wir gemeinsam:

- **Ich verstehe Risiken auf Business-Ebene**
- **Ich kenne die wichtigsten Maßnahmen**
- **Ich weiß, welche Fragen ich stellen muss**
- **Ich kann Entscheidungen begründen**
- **Ich weiß, dass Nachweis entscheidend ist**

Folie 3

Regulatorischer Kontext

NIS2

NIS2 als EU-Richtlinie

BSIG

Umsetzung in deutsches Recht (BSIG)

Relevanz

Relevanz für Unternehmen ab mittlerer Größe

Folie 4

Rolle der Geschäftsleitung

Verantwortung für Umsetzung

Verantwortung für Umsetzung von Sicherheitsmaßnahmen

Überwachung der Wirksamkeit

Überwachung der Wirksamkeit implementierter Maßnahmen

Keine Delegation

Keine Delegation der Verantwortung

Die Verantwortung der Geschäftsleitung ist gesetzlich verankert und nicht delegierbar – weder an die IT-Abteilung noch an externe Dienstleister.

Folie 5

Kernpflichten – Übersicht

Risikomanagement

Systematische Identifikation und Bewertung von Risiken

Incident Management

Strukturierter Umgang mit Sicherheitsvorfällen

Betriebsfähigkeit

Sicherstellung der Betriebsfähigkeit

Nachweisfähigkeit

Dokumentation und Nachweis aller Maßnahmen

Folie 6

Schulungspflicht

Gesetzliche Grundlage

Art. 20(2)(b) NIS2 verpflichtet die Geschäftsleitung zur Teilnahme an Schulungen zur Informationssicherheit.

Anforderungen im Überblick

- Teilnahme der Geschäftsleitung an Schulungen
- Ziel: ausreichendes Verständnis der Risiken und Maßnahmen
- Nachweis erforderlich

Folie 7

Was geprüft wird – Audit-Perspektive

Im Rahmen von BSI-Prüfungen und Audits wird die Geschäftsleitung zu folgenden Punkten befragt:

1

Verständnis der Risiken

Verständnis der für das Unternehmen relevanten Risiken

2

Kenntnis der Maßnahmen

Kenntnis relevanter Maßnahmen zur Risikominimierung

3

Bewertungsfähigkeit

Fähigkeit zur Bewertung von Auswirkungen auf das Unternehmen

Folie 8

Risikoverständnis

Risiken betreffen Geschäftsprozesse

Informationssicherheitsrisiken sind keine rein technischen Risiken – sie betreffen unmittelbar die Geschäftsprozesse.

IT-Ausfälle = Geschäftsrisiken

IT-Ausfälle sind gleichzeitig Geschäftsrisiken mit operativen, finanziellen und rechtlichen Folgen.

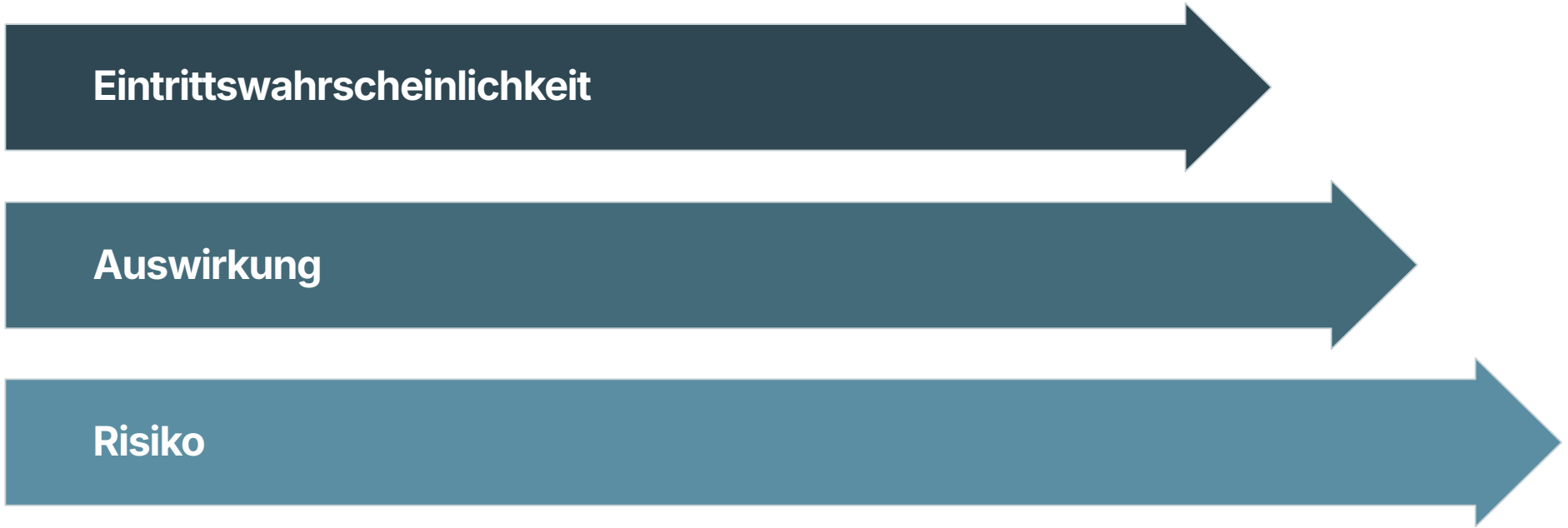
Bewertung auf Management-Ebene

Bewertung auf Management-Ebene notwendig – nicht delegierbar an die IT.

Folie 9

Risikomodell

> **Risiko = Eintrittswahrscheinlichkeit × Auswirkung**



Dieses Grundmodell bildet die Basis für die Risikobewertung auf Managementebene. Beide Faktoren müssen regelmäßig bewertet und dokumentiert werden.

Folie 10

Auswirkungen auf das Unternehmen

Betriebsunterbrechung

Ausfall kritischer Systeme und Prozesse

Finanzielle Auswirkungen

Direkte Kosten, Bußgelder, Umsatzverluste

Rechtliche Konsequenzen

Haftung der Geschäftsleitung, behördliche Maßnahmen

Reputationsschäden

Vertrauensverlust bei Kunden und Partnern

Folie 11

Maßnahmen – Struktur

Organisatorische Maßnahmen

- Richtlinien und Prozesse
- Zuständigkeiten
- Schulungen

Technische Maßnahmen

- Systemsicherheit
- Zugriffskontrollen
- Monitoring

Kontinuierliche Überprüfung

- Regelmäßige Audits
- Wirksamkeitskontrolle
- Anpassung bei Bedarf

Organisatorische Maßnahmen, technische Maßnahmen sowie kontinuierliche Überprüfung bilden gemeinsam das Fundament eines wirksamen Sicherheitsmanagements.

Folie 12

Meldepflicht (§32 BSIG)

Erhebliche Vorfälle

Erhebliche Vorfälle müssen gemeldet werden – die Einschätzung der Erheblichkeit liegt in der Verantwortung der Geschäftsleitung.

Strukturierter Ablauf

Strukturierter Ablauf erforderlich – von der Erkennung bis zur abschließenden Meldung an das BSI.

Klare Verantwortlichkeiten

Klare Verantwortlichkeiten notwendig – wer meldet, wann und in welcher Form.

§32 BSIG regelt die Meldepflichten für erhebliche Sicherheitsvorfälle gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Meldezeiten – Übersicht

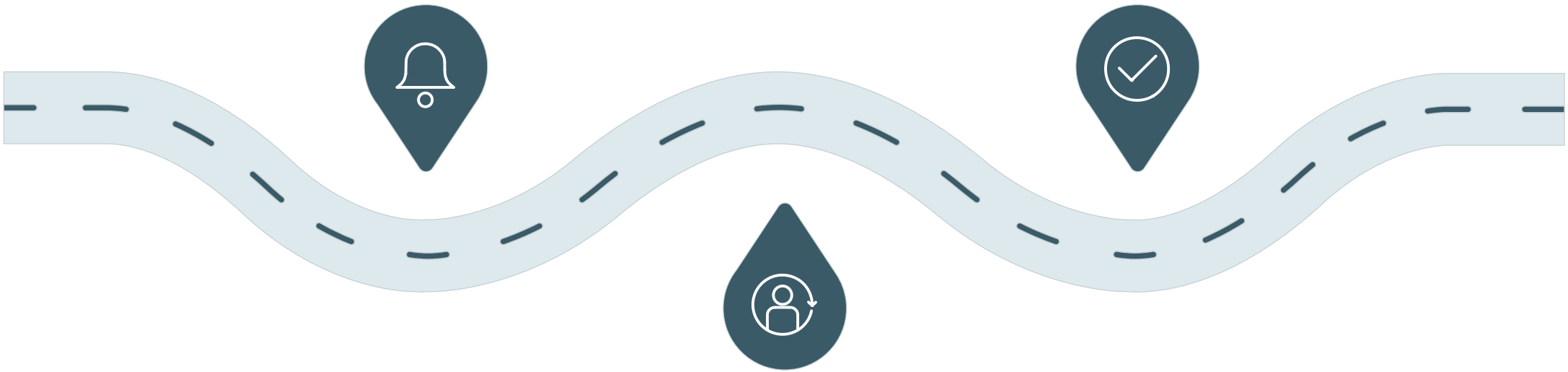
Fokus auf Verständnis – ohne technische Details:

Frühmldg

Erste Meldung nach Erkennung

Abschlussmldg

Finaler Bericht und Abschluss



Folgemldg

Aktualisierte Informationen ergänzen

01

Frühmeldung

Erste Meldung unmittelbar nach Erkennung eines erheblichen Vorfalls

02

Folgemeldung

Aktualisierte Meldung mit weiteren Informationen zum Vorfall

03

Abschlussmeldung

Abschließende Meldung nach vollständiger Aufarbeitung des Vorfalls

Folie 14

Beispielszenario

Vorfall: Ausfall zentraler Systeme

Leitfrage 1

Welche Prozesse sind betroffen?

Leitfrage 2

Welche Auswirkungen entstehen?

Leitfrage 3

Welche Maßnahmen greifen?

Folie 15

Typische Fehleinschätzungen

> **~~„Das ist ein IT-Thema"~~**
>
> Informationssicherheit ist eine Führungsaufgabe. Die Verantwortung liegt bei der Geschäftsleitung, nicht bei der IT-Abteilung.

> **~~„Wir sind nicht betroffen"~~**
>
> NIS2 und BSIG gelten für Unternehmen ab mittlerer Größe in relevanten Sektoren – eine Prüfung der eigenen Betroffenheit ist zwingend erforderlich.

> **~~„Es gibt keine konkreten Risiken"~~**
>
> Ohne systematische Risikoanalyse können keine fundierten Aussagen über das Risikoniveau getroffen werden.

Folie 16

Gute Steuerung

Risiken sind dokumentiert

Alle identifizierten Risiken sind schriftlich erfasst und bewertet.

Maßnahmen sind definiert

Für jedes Risiko sind konkrete Maßnahmen festgelegt und umgesetzt.

Verantwortlichkeiten sind klar

Jede Aufgabe ist einer verantwortlichen Person zugeordnet.

Folie 17

Mindestanforderungen

Grundlage wirksamer Compliance

Diese drei Mindestanforderungen bilden die Basis für eine nachweisbare Erfüllung der gesetzlichen Pflichten nach NIS2 und BSIG.

Übersicht kritischer Systeme

Übersicht kritischer Systeme und Prozesse liegt vor

Definierte Prozesse für Vorfälle

Definierte Prozesse für Vorfälle sind dokumentiert und bekannt

Dokumentierte Zuständigkeiten

Dokumentierte Zuständigkeiten sind aktuell und verbindlich

Folie 18

Aufgaben der Geschäftsleitung

Regelmäßige Befassung mit Risiken

Regelmäßige Befassung mit Risiken – mindestens jährlich, bei wesentlichen Änderungen anlassbezogen

Bewertung von Maßnahmen

Bewertung von Maßnahmen hinsichtlich Wirksamkeit und Angemessenheit

Sicherstellung der Umsetzung

Sicherstellung der Umsetzung durch geeignete organisatorische Strukturen

Folie 19

Nachweis der Schulung

Teilnehmer dokumentiert

Alle Teilnehmer der Schulung sind namentlich dokumentiert – mit Datum und Unterschrift.

Inhalte festgehalten

Die vermittelten Inhalte sind schriftlich festgehalten und dem Schulungsnachweis beigefügt.

Regelmäßige Wiederholung

Regelmäßige Wiederholung der Schulung ist sicherzustellen – empfohlen mindestens einmal jährlich.

Der Schulungsnachweis ist im Rahmen von BSI-Prüfungen und Audits vorzulegen. Eine lückenlose Dokumentation ist daher zwingend erforderlich.

Abschluss

Verantwortung wahrnehmen. Sicherheit gestalten.

Diese Schulung wurde durchgeführt gemäß Art. 20(2)(b) der NIS2-Richtlinie (EU) 2022/2555 sowie den Anforderungen des BSIG (§32, §38) und den BSI-Standards 200-2, 200-3 und 200-4.

Normative Grundlagen

NIS2-Richtlinie (EU) 2022/2555 · BSIG §32, §38 · BSI-Standards 200-2, 200-3, 200-4

Zielgruppe

Geschäftsführung und Management von KMU

Schulungsnachweis

Teilnahme, Inhalte und Datum sind zu dokumentieren und aufzubewahren.