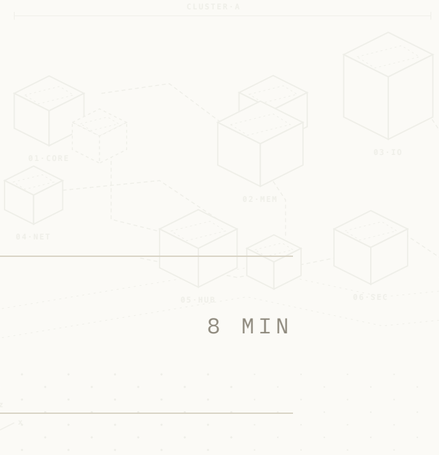
§ 00 — EINFÜHRUNG & ÜBERBLICK

NIS2 & Lieferkettensicherheit.

Was Unternehmen wissen müssen — auch wenn sie *nicht direkt betroffen* sind.

Fünf Kapitel für *eine Stunde NIS2.*



i.	Was ist NIS2?	Hintergrund, EU-Kontext, das neue BSIG.	8 MIN
ii.	Wer ist direkt betroffen?	Einrichtungstypen, Sektoren, Schwellenwerte.	7 MIN
iii.	Was müssen Betroffene tun?	Registrierung, Meldepflichten, Risikomanagement.	8 MIN
iv.	Indirekte Betroffenheit & Lieferkette	Warum auch nicht-betroffene Unternehmen unter Druck geraten.	7 MIN
v.	Die zehn Mindestmaßnahmen — § 30 BSIG	Vollständiger Durchgang, praxisnah erklärt.	15 MIN

§ 01 — KAPITEL I

I.

Was ist NIS2 — und warum kommt sie *jetzt?*

Hintergrund, EU-Kontext und das neue BSI-Gesetz vom Dezember 2025.

§ 01.1 — DIE NEUE EU-CYBERSICHERHEITSRICHTLINIE

Höhere Anforderungen, schärfere *Durchsetzung.*

NIS2 ist die überarbeitete EU-Richtlinie zur Netz- und Informationssicherheit (Richtlinie (EU) 2022/2555). Sie ersetzt NIS1 von 2016 und setzt deutlich höhere Anforderungen.

IN KRAFT	UMSETZUNG DE	REICHWEITE	BUSSGELD
EU-Richtlinie 2022/2555	BSIG – BGBl. I Nr. 301	~ 29.000 Einrichtungen	bis 10 Mio. € oder 2 % Umsatz
Januar 2023, EU-weit verbindlich.	5. Dezember 2025.	Tausende Unternehmen in DE.	weltweiter Konzernumsatz.

WARUM JETZT?

- → Cyberangriffe nehmen exponentiell zu — Kosten weltweit über 8 Billionen US-$ (2023).
- → NIS1 war zu wenig harmonisiert, mit zu vielen Lücken in der Durchsetzung.
- → Lieferketten als kritischer Angriffspunkt — SolarWinds, Log4Shell und Folgevorfälle.

Was sich *geändert* hat.

BISHER

NIS1 · 2016 – 2022

- × Nur „Betreiber wesentlicher Dienste".
- × Enge Sektordefinition.
- × Ca. 2.000 Einrichtungen in Deutschland.
- × Keine Geschäftsleitungshaftung.
- × Wenig EU-weit harmonisiert.
- × Geringe Bußgelder.

NEU

NIS2 · BSIG 2025

- → Besonders wichtige *und* wichtige Einrichtungen.
- → 18 Sektoren — teils sehr viel weiter als vermutet.
- → Schätzungsweise *29.000+* Einrichtungen in DE.
- → Persönliche Haftung der Geschäftsleitung — auch ohne Schaden.
- → Starke EU-Harmonisierung.
- → Bußgelder bis *10 Mio. €*.

Besonders wichtig vs. *wichtig.*

KATEGORIE A

Besonders wichtige Einrichtungen

§ 28 ABS. 1 BSIG

- Betreiber kritischer Anlagen nach BSI-KritisV — Energie, Wasser, Ernährung, IT/TK, Gesundheit, Finanzen, Verkehr, Abfall.
- Qualifizierte Vertrauensdiensteanbieter, TLD-Registrare, DNS-Anbieter.
- TK-Anbieter ≥ 50 MA *oder* > 10 Mio. € Umsatz/Bilanz.
- Sonstige: ≥ 250 MA *oder* > 50 Mio. € Umsatz *und* > 43 Mio. € Bilanz.
- In Anlage 1 BSIG genannte Sektoren (KRITIS-nah).

KATEGORIE B

Wichtige Einrichtungen

§ 28 ABS. 2 BSIG

- Vertrauensdiensteanbieter (ohne Qualifikation).
- TK-Anbieter < 50 MA *und* ≤ 10 Mio. € Umsatz/Bilanz.
- Sonstige: ≥ 50 MA *oder* > 10 Mio. € Umsatz/Bilanz.
- In Anlage 1 oder 2 BSIG — kleinteilig festzustellen, oft *Beratung erforderlich*, auch um Nicht-Betroffenheit zu sichern.
- Strengere Aufsicht als NIS1, weniger als bei besonders wichtigen.

Achtzehn *Sektoren.*

NIS2 erfasst 18 Sektoren. Anlage 1 (besonders wichtig) und Anlage 2 (wichtig) des BSIG listen die Einrichtungsarten detailliert auf.

01. Energie — ANLAGE 1	*02.* Finanzwesen — ANLAGE 1	*03.* Gesundheit — ANLAGE 1	*04.* Wasser & Abwasser — ANLAGE 1	*05.* Verkehr — ANLAGE 1	*06.* Digitale Infrastruktur — ANLAGE 1
07. Öffentliche Verwaltung — ANLAGE 1	*08.* Weltraum — ANLAGE 1	*09.* IKT-Dienste — ANLAGE 1	*10.* Telekommunikation — ANLAGE 1	*11.* Vertrauensdienste — ANLAGE 1	*12.* Post & Kurier — ANLAGE 2
13. Abfallbewirtschaftung — ANLAGE 2	*14.* Chemie — ANLAGE 2	*15.* Lebensmittel — ANLAGE 2	*16.* Verarbeitendes Gewerbe — ANLAGE 2	*17.* Forschung — ANLAGE 2	*18.* Digitale Dienste — ANLAGE 2

— ORANGE-HINTERLEGUNG · ANLAGE 1 (BESONDERS WICHTIG) — NEUTRAL · ANLAGE 2 (WICHTIG)

Wer von NIS2 erfasst wird – und es *nicht ahnt.*

BEISPIEL A

Mittelständischer Lebensmittelproduzent

Eine Manufaktur mit 80 Mitarbeitenden und 14 Mio. € Umsatz fällt über *Anlage 2 (Lebensmittel)* in den wichtigen Sektor — obwohl sie sich selbst als „klassischer Mittelstand" sieht.

> *„Wir produzieren doch nur Wurst – was hat das mit IT-Sicherheit zu tun?" – Die Frage stellt sich heute nicht mehr.*

BEISPIEL B

IT-Dienstleister mit 60 MA

MSPs, Systemhäuser und Softwarehersteller fallen über *Anlage 1 (IKT-Dienste)* sogar in die Kategorie besonders wichtig — bereits ab 50 MA oder 10 Mio. € Umsatz.

> *IKT-Dienstleister tragen die strengsten Pflichten – weil sie die Lieferkette anderer sind.*

Wer *nicht* betroffen ist.

GRÖSSE

Kleinstunternehmen & KMU

< 50 Mitarbeitende *und* ≤ 10 Mio. € Umsatz/Bilanz. Grundsätzlich ausgenommen — sofern nicht ein KRITIS-Tatbestand greift.

GRUNDSÄTZLICH AUSGENOMMEN

BUNDESVERWALTUNG

Eigene Regeln nach § 29 BSIG

Bundesbehörden unterliegen eigenen Vorgaben — insbesondere § 44 (BSI-Standards) statt § 30.

SEPARATE REGELUNG

FINANZSEKTOR

DORA geht vor

Wenn DORA (VO (EU) 2022/2554) gilt, greift die Sonderausnahme nach § 28 Abs. 6 BSIG.

DORA ALS LEX SPECIALIS

TK & ENERGIE

Sektorspezifische Regeln

Eigene Regelungen nach § 28 Abs. 5 BSIG — teilweise ausgenommen, teilweise erweitert.

SEKTORRECHT BEACHTEN

§ 02 — KAPITEL II

II.

Direkte Verpflichtung & *indirekter Druck.*

Warum auch nicht-betroffene Unternehmen handeln müssen — und wer den Hebel in der Hand hält.

§ 02.5 — § 30 NR. 4 BSIG ALS HEBEL

Der *Lieferkettendruck* kommt nicht vom Gesetz — sondern vom Kunden.

NIS2-betroffene Unternehmen *müssen* ihre Lieferkette absichern (§ 30 Abs. 2 Nr. 4 BSIG). Das schafft unmittelbaren Druck auf alle Lieferanten und Dienstleister — auch auf solche, die selbst nicht unter NIS2 fallen.

REGULATOR
EU / BSI

→

NIS2-PFLICHTIG
Kunde (z. B. KRITIS)

→

SIE ALS LIEFERANT
Ihr Unternehmen

→

WEITERGEGEBEN
Ihre Unterlieferanten

FRAGEBÖGEN
Selbstauskunfts-Fragebögen zu IT-Sicherheitsmaßnahmen.

VERTRAGSKLAUSELN
NIS2-Pflichten werden vertraglich an Lieferanten weitergereicht.

NACHWEISE
ISO 27001, BSI-Grundschutz o. ä. als Voraussetzung.

KONSEQUENZ
Kein Nachweis — kein Vertrag. Ausschluss von Ausschreibungen.

§ 02.6 — WO ES OHNE NACHWEISE SCHWIERIG WIRD

Geschäftsfähigkeit als Funktion Ihres *Sicherheitsniveaus.*

BRANCHE

Gesundheitswesen

Krankenhäuser, Labore und Medizingeräte-Hersteller verlangen Nachweise gemäß NIS2 / DORA.

RISIKO · HOCH

BRANCHE

Energiewirtschaft

KRITIS-Versorger verpflichten Dienstleister vertraglich zu Sicherheitsstandards.

RISIKO · HOCH

BRANCHE

Automotive & Industrie

TISAX und ähnliche Standards werden in NIS2-Lieferketten als Mindestanforderung vorausgesetzt.

RISIKO · MITTEL

BRANCHE

Finanzsektor

Banken und Versicherer (DORA + NIS2) führen strenge Lieferantenaudits durch.

RISIKO · HOCH

BRANCHE

Öffentliche Aufträge

Vergabeverfahren verlangen zunehmend ISO 27001 oder BSI-Grundschutz als Eignung.

RISIKO · MITTEL

BRANCHE

Cloud & IT-Dienstleistungen

MSPs und Cloud-Anbieter unterliegen selbst NIS2 und reichen Anforderungen weiter.

RISIKO · SEHR HOCH

§ 03 — KAPITEL III

III.

Was müssen NIS2-betroffene Unternehmen *umsetzen?*

Registrierung · Meldepflichten · Risikomanagement · Geschäftsleitungspflichten.

Fünf Punkte zur *Registrierung.*

Besonders wichtige und wichtige Einrichtungen sind verpflichtet, sich beim BSI zu registrieren.

i. Frist

Grundsätzlich ab 06.03.2026, spätestens jedoch *3 Monate*, nachdem die Einrichtung erstmals als besonders wichtig oder wichtig gilt (§ 33 Abs. 1 BSIG). Das BSI beginnt voraussichtlich noch 2026 mit Prüfungen.

ii. Angaben

Name, Rechtsform, Anschrift, E-Mail, IP-Bereiche, Telefon, Handelsregisternummer, zuständige Aufsichtsbehörde, relevanter Sektor.

iii. Meldeplattform

Gemeinsame Plattform von BSI und BBK. *Achtung:* ein „Mein Unternehmen"-Zugang zu ELSTER ist Voraussetzung — Zeitachse beachten.

iv. Änderungen

Unverzüglich, spätestens innerhalb von *2 Wochen* nach Kenntnisnahme zu melden (§ 33 Abs. 5 BSIG).

v. BSI kann von Amts wegen registrieren

Erfüllt die Einrichtung ihre Registrierpflicht nicht, registriert das BSI selbst (§ 33 Abs. 3 BSIG) — und kann zugleich Bußgelder verhängen.

Vom Vorfall zur *Abschlussmeldung* – gestuft.

Bei einem erheblichen Sicherheitsvorfall gilt ein vierstufiges Meldeverfahren.

0–24 Std.

Frühe Erstmeldung

Verdacht auf rechtswidrige oder böswillige Handlung sowie grenzüberschreitende Auswirkungen angeben.

≤ 72 Std.

Folgemeldung

Bestätigung und Aktualisierung; erste Bewertung des Schweregrads, Kompromittierungsindikatoren benennen.

Auf Ersuchen

Zwischenmeldung

Auf Anfrage des BSI: relevante Status-aktualisierungen zum laufenden Vorfall.

≤ 1 Monat

Abschlussmeldung

Ausführliche Beschreibung; Art der Bedrohung und Ursache; getroffene und laufende Maßnahmen; grenz-überschreitende Auswirkungen.

Persönliche Pflichten — *persönliche Haftung.*

§ 38 BSIG

Pflichten der Geschäftsleitung

01. **Schulungspflicht.** Regelmäßige Teilnahme an Schulungen zu IT-Sicherheit und Risikomanagement (§ 38 Abs. 3).

02. **Überwachungspflicht.** Risikomanagementmaßnahmen nach § 30 umsetzen *und* überwachen (§ 38 Abs. 1).

03. **Persönliche Haftung.** Bei schuldhafter Pflichtverletzung haftet die Geschäftsleitung gegenüber der Einrichtung (§ 38 Abs. 2).

04. **Haftung für Schäden & Bußgelder.** Bei Verstößen gegen NIS2 / das BSI-Gesetz haften Geschäftsführer *persönlich* — für Schäden *und* für verhängte Bußgelder.

§ 65 BSIG

Bußgelder

BESONDERS WICHTIG

bis 10 Mio. €

oder 2 % Konzernumsatz

WICHTIG

bis 7 Mio. €

oder 1,4 % Konzern-umsatz

ZUSÄTZLICH

Offenlegung von Informationen – Tätigkeitsverbote für Leitungsorgane möglich.

§ 04 — KAPITEL IV

iv.

Erwartungen an nicht direkt *betroffene* Unternehmen.

Warum Kunden Informationen, Nachweise oder Sicherheitszusagen verlangen — und wie konkret das wird.

Sechs Dinge, auf die Sie sich jetzt schon *vorbereiten* sollten.

I. — FRAGEBÖGEN

Sicherheitsfragebögen

Selbstauskunft zu technischen und organisatorischen Maßnahmen (TOMs) — oft umfangreich und verbindlich.

STANDARD HEUTE

II. — VERTRAG

Klauseln zu § 30 BSIG

Direkter Verweis auf die Anforderungen — Sie verpflichten sich zur Einhaltung der zehn Maßnahmen.

VERBINDLICH

III. — AUDIT

Auditrechte

Recht zur Prüfung Ihrer IT-Sicherheitsmaßnahmen — Audits, Vor-Ort-Besuche, Penetrationstests.

VORBEREITUNG NÖTIG

IV. — MELDEKETTE

Weitergabe der Meldepflicht

Vertragliche Pflicht, sicherheitsrelevante Vorfälle unverzüglich an den NIS2-pflichtigen Kunden zu melden.

24 / 72-H-LOGIK

V. — ZERTIFIKATE

Nachweise

ISO 27001, SOC 2, BSI-Grundschutz oder branchenspezifische Standards als Zugangsvoraussetzung.

MARKTSTANDARD

VI. — WIEDERHOLUNG

Regelmäßige Nachweise

Einmalig genügt nicht — jährliche Updates, Re-Zertifizierungen, Sicherheitsberichte werden erwartet.

DAUERAUFGABE

§ 05 — KAPITEL V · DAS KERNSTÜCK

V.

Die zehn Mindestmaßnahmen aus *§ 30 BSIG.*

Was NIS2 zwingend vorschreibt — und warum es auch für Sie gilt.

§ 05.0 — § 30 ABS. 1 BSIG · GENERALKLAUSEL

> *„Betroffene Unternehmen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu treffen […].*

> *Bei der Bewertung der Verhältnismäßigkeit sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten sowie Eintrittswahrscheinlichkeit und Schwere von Vorfällen samt ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen."*

— WORTLAUT, GEKÜRZT

Zehn Maßnahmen. *Mindestens.*

§ 30 Abs. 2 BSIG verpflichtet besonders wichtige und wichtige Einrichtungen, mindestens diese zehn Maßnahmen zu ergreifen.

01. Risikoanalyse & *IT-Sicherheitskonzept*

02. Bewältigung von Sicherheitsvorfällen

03. Business Continuity & Backup

04. *Lieferkettensicherheit*

05. Sichere Entwicklung & Schwachstellen

06. *Effektivitätsbewertung* der Maßnahmen

07. Schulungen & Sensibilisierung

08. Kryptographie & Verschlüsselung

09. Personalsicherheit & Zugriffe

10. Multi-Faktor-Authentifizierung

Maßnahme *01.* — Risikoanalyse & IT-Sicherheitskonzept

WORTLAUT · § 30 ABS. 2 NR. 1 BSIG

> *Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik.*

WARUM

Hintergrund

Ohne Kenntnis der eigenen Risiken können keine wirksamen Schutzmaßnahmen ergriffen werden. Eine strukturierte Risikoanalyse ist die Basis jeder Sicherheitsstrategie.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Kunden fragen gezielt: „Haben Sie eine aktuelle Risikoanalyse?" Ohne dokumentiertes IT-Sicherheitskonzept sind Sie bei Ausschreibungen im Nachteil. Viele Verträge verlangen ein ISMS — z. B. nach ISO 27001.

PRAXISTIPP

→ Starten Sie mit einer einfachen Asset-Inventur und Risikobeurteilung. Dokumentieren Sie IT-Systeme, Daten und Bedrohungen. Ein einseitiges Konzept ist besser als keines.

Maßnahme *02.* – Bewältigung von Sicherheitsvorfällen

WORTLAUT · § 30 ABS. 2 NR. 2 BSIG

> *Bewältigung von Sicherheitsvorfällen.*

WARUM

Hintergrund

Die Frage ist nicht *ob*, sondern *wann* ein Vorfall eintritt. Ohne Incident-Response-Plan verliert man Zeit und Daten — der Plan muss vorab erarbeitet und geübt werden. Das BSI muss zudem unterscheiden können: Einzelfall oder genereller Angriff.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Lieferketten-Kunden verlangen Notfallpläne: „Was tun Sie, wenn Sie gehackt werden? Informieren Sie uns rechtzeitig?" Ohne Plan riskieren Sie Vertragsverletzungen und Haftung bei Datenweitergabe.

PRAXISTIPP

→ Einfacher IR-Plan: Wer wird wann informiert? Welche Systeme werden offline genommen? Wer ist immer erreichbar? Üben Sie jährlich in einem Tabletop-Exercise.

Maßnahme *03.* – Business Continuity, Backup & Krisenmanagement

WORTLAUT · § 30 ABS. 2 NR. 3 BSIG

> *Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement.*

WARUM

Hintergrund

Ransomware ist die größte Bedrohung für KMU. Ohne funktionsfähige Backups und Wiederherstellungsplan können Angriffe existenzbedrohend werden. BCM schützt Geschäftsbeziehungen.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

NIS2-Kunden prüfen: „Können Sie uns im Notfall weiterhin beliefern?" Ausfälle bei Lieferanten gefährden die gesamte Kette — Business-Continuity-Konzepte werden Vertragsbestandteil.

PRAXISTIPP

→ Testen Sie Backups regelmäßig. *3-2-1-Regel:* 3 Kopien, 2 Medien, 1 extern. Notfallplan mit Kontaktlisten und Priorisierung kritischer Systeme.

Maßnahme *04.* – Lieferkettensicherheit

WORTLAUT · § 30 ABS. 2 NR. 4 BSIG

> *Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Dienstleistern.*

WARUM

Hintergrund

Supply-Chain-Angriffe (SolarWinds, ASUS Live Update) zeigen: Angreifer nutzen schwächere Glieder der Lieferkette, um in sichere Systeme einzudringen. § 30 Nr. 4 ist daher der zentrale Hebel.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Diese Maßnahme ist der direkte Grund, warum Sie als Lieferant unter Druck geraten. Ihr Kunde muss seine Lieferkette absichern — und dazu gehören Sie. Sicherheitsfragebögen sind die direkte Folge. Schon eine schlecht gesicherte Klimaanlagensteuerung kann zum Einfallstor werden.

PRAXISTIPP

→ Liste Ihrer eigenen Lieferanten und Dienstleister erstellen, deren IT-Sicherheit bewerten und sicherstellen, dass IT-Dienstleister grundlegende Standards erfüllen.

Maßnahme *05.* – Sichere Entwicklung & Schwachstellenmanagement

WORTLAUT · § 30 ABS. 2 NR. 5 BSIG

> *Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen.*

WARUM

Hintergrund

Ungepatchte Systeme sind das *Einfallstor Nr. 1*. Ein formales Schwachstellenmanagement stellt sicher, dass bekannte Lücken zeitnah geschlossen werden — bevor sie ausgenutzt werden.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Software-Lieferanten werden gezielt nach Patch-Zyklen und Vulnerability-Disclosure-Prozessen gefragt. Wer keine nachweisbare Patch-Policy hat, scheidet aus Ausschreibungen aus.

PRAXISTIPP

→ Einfaches Patch-Management: alle Systeme wöchentlich auf Updates prüfen, kritische Patches binnen 72h einspielen. Prozess schriftlich dokumentieren.

Maßnahme *06.* — Effektivitätsbewertung der Maßnahmen

WORTLAUT · § 30 ABS. 2 NR. 6 BSIG

> *Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik.*

WARUM

Hintergrund

Sicherheitsmaßnahmen helfen nur, wenn sie tatsächlich wirken. Regelmäßige Reviews, interne Audits und Penetrationstests zeigen Lücken auf, bevor Angreifer sie finden.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Kunden und Auditoren fragen: „Wie wissen Sie, dass Ihre Maßnahmen wirken?" Ohne Nachweis (Audit-Reports, Pentest-Ergebnisse) wirken Sicherheitsbehauptungen unglaubwürdig.

PRAXISTIPP

→ Jährlich interne Sicherheitsrevision durchführen, alle zwei Jahre externer Pentest. Ergebnisse und Maßnahmen dokumentieren.

Maßnahme *07.* – Schulungen & Sensibilisierung

WORTLAUT · § 30 ABS. 2 NR. 7 BSIG

> *Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik.*

WARUM

Hintergrund

Über *80 % aller Cyberangriffe* beginnen mit Phishing oder menschlichem Fehlverhalten. Regelmäßige Schulungen sind der effektivste ROI in der IT-Sicherheit — und für Geschäftsleitungen nach § 38 BSIG verpflichtend.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Viele Kunden-Fragebögen fragen explizit: „Führen Sie regelmäßige Security-Awareness-Schulungen durch?" Ohne Schulungsnachweis fehlt ein zentrales Kriterium.

PRAXISTIPP

→ Mindestens jährlich Phishing-Simulationen und Awareness-Trainings durchführen. Dokumentierte Schulungen über etablierte Anbieter sind ausreichend.

Maßnahme *08.* — Kryptographie & Verschlüsselung

WORTLAUT · § 30 ABS. 2 NR. 8 BSIG

> *Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren.*

WARUM

Hintergrund

Verschlüsselung schützt sensible Daten bei Übertragung und Speicherung. Ein fehlendes Kryptographiekonzept ist häufig der Grund für erfolgreiche Datenpannen — mit anschließender DSGVO-Meldepflicht.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Kunden, die mit sensiblen Daten arbeiten (Gesundheit, Finanzen), verlangen Nachweise: TLS, AES-256 und sichere Schlüsselverwaltung sind Standard.

PRAXISTIPP

→ E-Mails mit sensiblen Daten via S/MIME oder PGP. Laptops und mobile Geräte verschlüsseln (Bitlocker / FileVault). Alle Verbindungen über HTTPS / TLS.

Maßnahme *09.* – Personalsicherheit & Zugriffsmanagement

WORTLAUT · § 30 ABS. 2 NR. 9 BSIG

> *Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen.*

WARUM

Hintergrund

Insider-Bedrohungen und kompromittierte Konten sind — neben Ransomware — die häufigsten Sicherheitsvorfälle. *Least Privilege* reduziert den Schaden erheblich.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

Kunden prüfen: „Wer in Ihrem Unternehmen hat Zugriff auf unsere Daten?" Rollenbasierte Zugriffskonzepte, Hintergrundprüfungen und Offboarding werden standardmäßig hinterfragt.

PRAXISTIPP

→ Rechtemanagement: jeder bekommt nur die Rechte, die er braucht. Vierteljährlich prüfen. Sofortiges Deaktivieren bei Austritt.

Maßnahme *10.* – Multi-Faktor-Authentifizierung

WORTLAUT · § 30 ABS. 2 NR. 10 BSIG

> *Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme.*

WARUM

Hintergrund

MFA ist die einzeln wirksamste Maßnahme gegen Kontoübernahmen. Laut Microsoft verhindert MFA über *99 %* der automatisierten Angriffe. Ohne MFA ist kein modernes Sicherheitskonzept vollständig.

AUCH OHNE DIREKTE BETROFFENHEIT RELEVANT

Kunden- & Lieferkettendruck

MFA ist Standardanforderung in fast jedem IT-Sicherheitsfragebogen. Viele Cyber-Versicherungen setzen MFA als Grundvoraussetzung — ohne MFA oft keine Police.

PRAXISTIPP

→ MFA für alle Accounts aktivieren: E-Mail (M365 / Google), VPN, Cloud-Dienste, kritische Anwendungen. Einstieg: Microsoft / Google Authenticator. Zeitaufwand: ein Nachmittag.

§ 06 — FAZIT & NÄCHSTE SCHRITTE

Vier Schritte für *Morgen vormittag.*

01.

Betroffenheit prüfen

Sind Sie direkt betroffen? Check: ≥ 50 MA / ≥ 10 Mio. € + NIS2-Sektor. Wenn ja: Registrierung binnen 3 Monaten beim BSI.

02.

Lieferkettendruck antizipieren

Auch wenn nicht direkt betroffen — Ihre Kunden werden fragen. Bereiten Sie sich auf Sicherheitsfragebögen und Vertragsklauseln vor.

03.

Zehn Maßnahmen als Checkliste

Prüfen Sie jede der zehn Maßnahmen aus § 30 BSIG: Was haben Sie bereits? Was fehlt? Realistischer Umsetzungsplan.

04.

Dokumentation aufbauen

NIS2 verlangt Nachweise. Dokumentieren Sie Ihre Maßnahmen — das zahlt sich für Kunden-Audits *und* Versicherungen aus.

Vielen *Dank.*

Fragen & Diskussion — wir freuen uns auf Ihre Themen.

QUELLEN & GRUNDLAGEN

§ BSIG — Gesetz zur Umsetzung der NIS-2-Richtlinie (BGBl. I 2025 Nr. 301, 5. Dezember 2025).

§ EU-Richtlinie (EU) 2022/2555 (NIS2) vom 14. Dezember 2022.

§ BSI — Bundesamt für Sicherheit in der Informationstechnik · bsi.bund.de

§ ENISA — European Union Agency for Cybersecurity.

KONTAKT

§ *RAK|LAW Rechtsanwaltsgesellschaft Appelt Krause mbH*

§ Tal 16, 80331 München

§ kontakt@rak-law.com, www.rak-law.com

§ ERSTGESPRÄCH VEREINBAREN →