DENTONS

NIS2 und NIS2UmsuCG im Gesundheitssektor

SIBB – 1. Dezember 2025

Lorenz Wascher (Dentons, ItsBB)
Karolina Vonková (Dentons, ItsBB)

Agenda

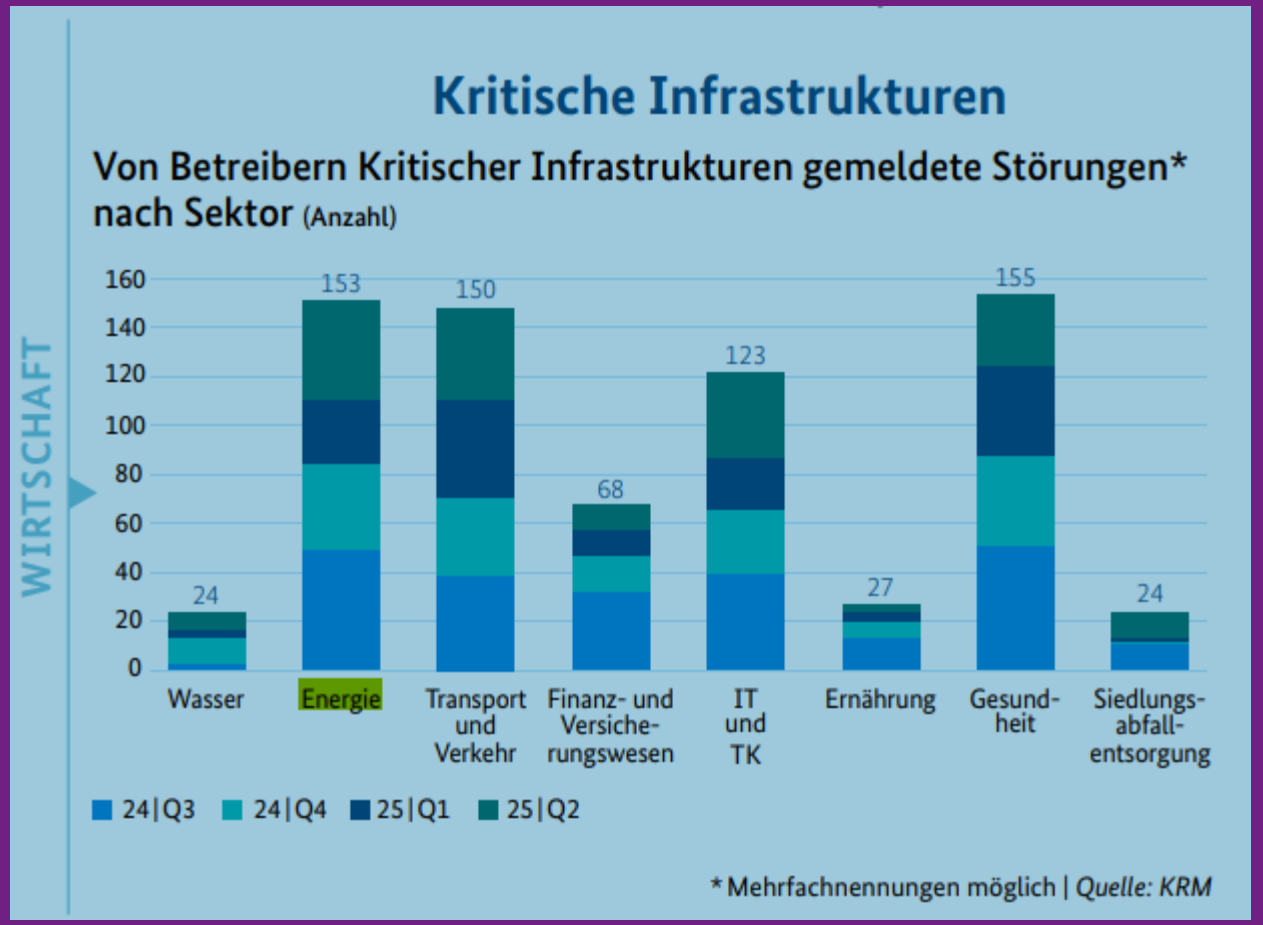
1. Akute Bedrohungslage – BSI Lagebericht 2025
2. Gesetzgebungsverfahren zur Umsetzung von NIS-2
3. Änderungen im Überblick
4. Betroffenheitsprüfung
5. Konzerne und Mehrspartenunternehmen
6. Neue Pflichten
7. Unterstützungsangebote
8. Handlungsempfehlungen

Akute Bedrohungslage – BSI Lagebericht 2025

- IT-Sicherheitslage bleibt angespannt
- Verschärfte geopolitische Spannungen
- Besonders verstärkte Angriffe auf kritische Infrastrukturen
- Empfehlung des BSI: Schutz der Angriffsflächen intensivieren

Den Lagebericht des BSI – mit Zusammenfassung und Grafiken – finden Sie hier.

Die vollständige Fassung des BSI-Lageberichts für den Zeitraum Juli 2024 bis Juni 2025 steht hier zum Abruf bereit.



NIS-2 Gesetzgebungsverfahren

Unmittelbar bevorstehendes Inkrafttreten

NIS-2

EU-Richtlinie 2022/2555 soll ein hohes gemeinsames Cybersicherheitsniveau in der Union förden

NIS-2 Umsetzungsfrist

Die EU-Mitgliedstaaten mussten NIS-2 bis 17.10.2024 umsetzen, Deutschland hat die Frist verstreichen lassen

Durch Bundesrat am 21. November 2025 beraten – keinen Vermittlungsausschuss einberufen – derzeit beim BPRäs

Inkrafttreten des Gesetzes

Das Gesetz tritt unmittelbar nach Ausfertigung und Verkündung in Kraft, ohne Verzögerung

Ausweitung des Anwendungsbereichs und weitere Neuerungen

Neu: Erweiterter Scope und Pflichten

Erweiterter Anwendungsbereich

Nunmehr ca. 29.000 Einrichtungen statt wie bisherig etwa 4.500

Neue Kategorien: *wichtige* und *besonders wichtige Einrichtung*

- Basierend auf Unternehmensgröße und Umsatz
- KRITIS gehören zu den besonders wichtigen Einrichtungen

Umfassendes Risikomanagement

Erweiterte Pflichten beinhalten ein umfassendes Risikomanagement zur Vermeidung von Verstößen und Sicherstellung der Compliance.

Neu: Meldeverfahren und verschärfte Sanktionen

Dreistufiges Meldeverfahren

Ein dreistufiges Meldeverfahren wurde eingeführt, um Verstöße systematisch zu erfassen und zu bearbeiten.

Höhe der Sanktionen

Für besonders wichtige Einrichtungen drohen Geldbußen bis zu 10 Millionen Euro oder 2% des weltweiten Vorjahresumsatzes. Für wichtige Einrichtungen gelten Bußen bis 7 Millionen Euro oder 1,4% des Umsatzes.

Geschäftsleiterhaftung und Sicherheit

Geschäftsleiter haften persönlich und sind damit unter anderem für die Umsetzung der Risikomanagementmaßnahmen verantwortlich.

Betroffenheitsprüfung für Gesundheitsunternehmen

Sektorielle Erfassung

Über § 28 BSIG & Anlage 1 und 2 BSIG

§ 28 Abs. 1 Nr. 1 BSIG – Betreiber kritischer Anlagen – über Sektoren

- Betreiber von KRITIS („*Betreiber kritischer Anlagen*“) – dortige Schwellenwerte beachten!
  - Krankenhaus (§ 108 SGB 5)
  - Versorgung mit lebenserhaltenden Medizinprodukten
  - Versorgung mit Arznei, Blut, Plasma
  - Laboratoriumsdiagnostik

Anlage 1 – besonders wichtige und wichtige Einrichtungen

- 18 Sektoren, darunter der Gesundheitssektor!
- Einordnung abhängig von Schwellenwerten

Anlage 2 – Sektoren wichtiger Einrichtungen

Anlage 1

4	**Gesundheit**		
4.1.1			Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371
4.1.3			Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
4.1.4			Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
4.1.5			Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

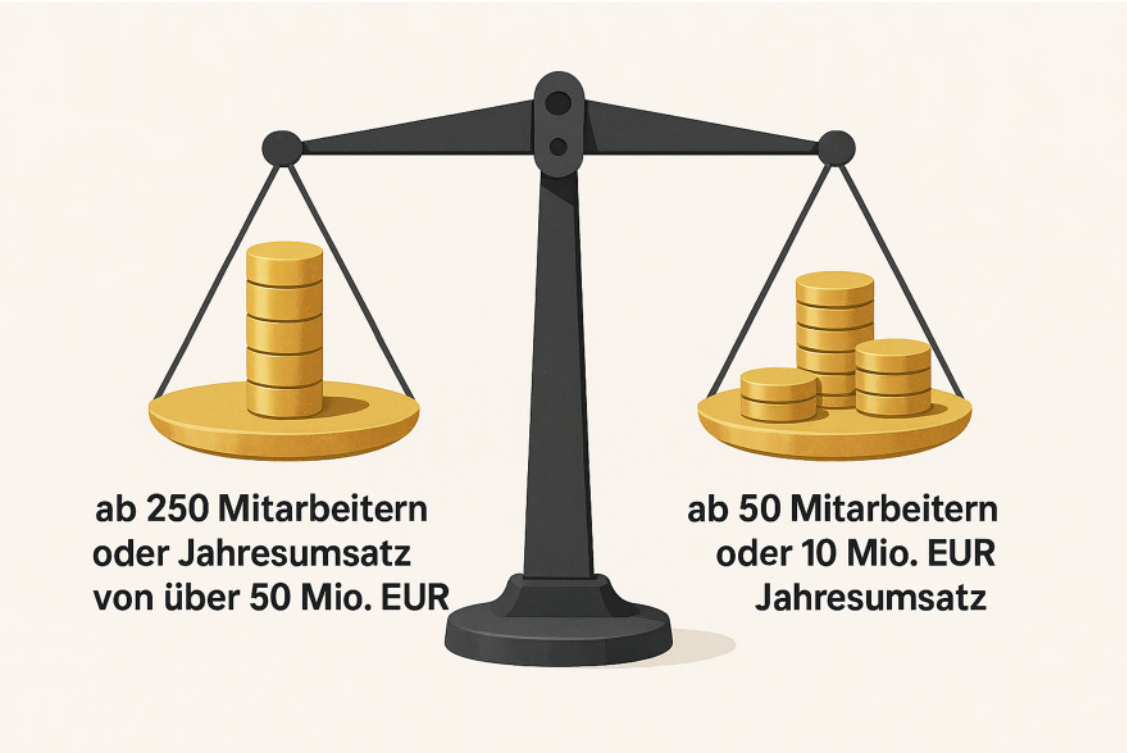
Anlage 2

5	**Verarbeitendes Gewerbe/Herstellung von Waren**		
5.1		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
5.1.1			Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 herstellen, mit Ausnahme von Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 („Liste kritischer Medizinprodukte für Notlagen im Bereich

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
			der öffentlichen Gesundheit“) eingestuft werden

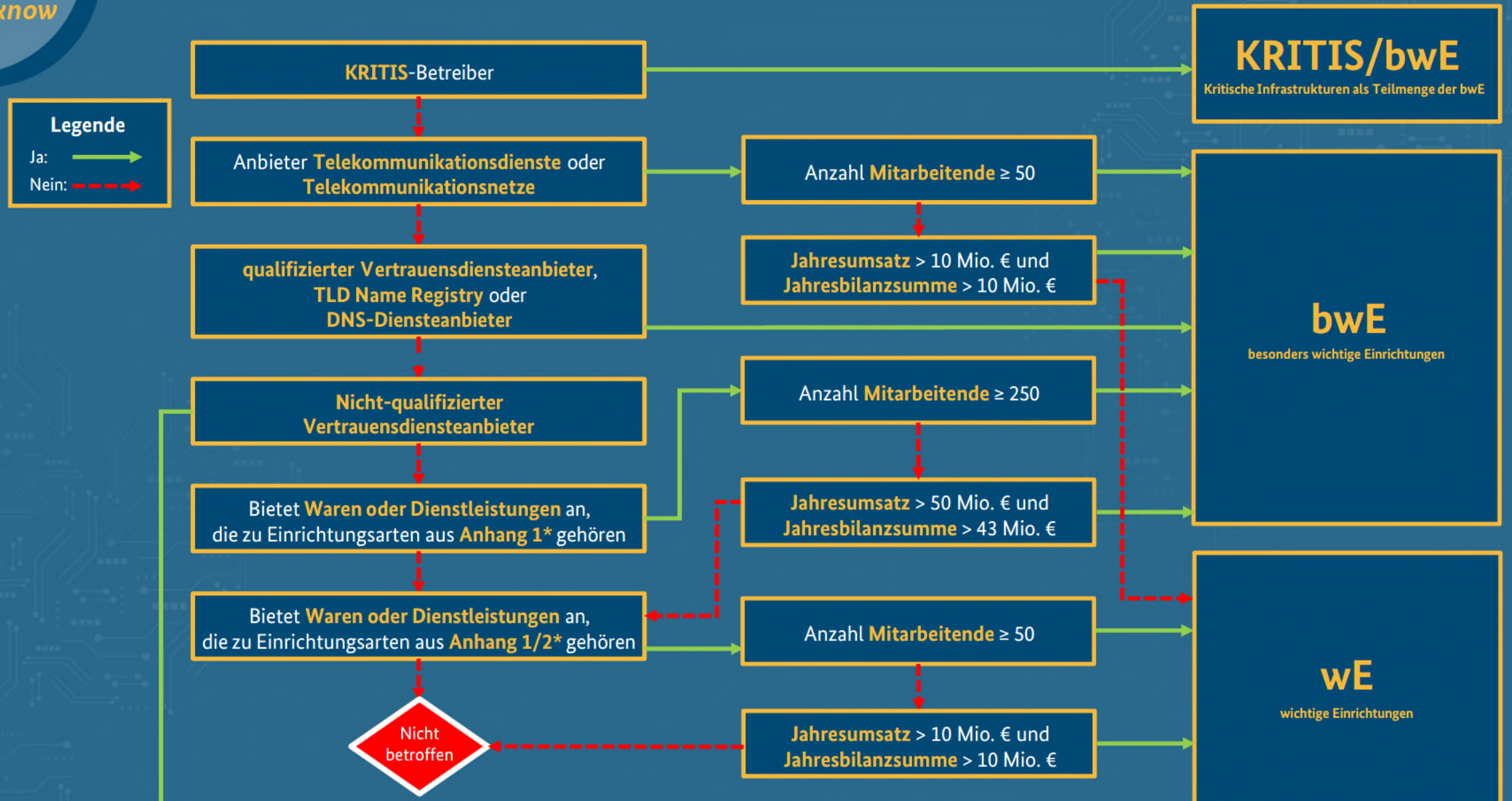
Schwellenwertprüfung

Zwei Kategorien



1. **Besonders wichtige Einrichtungen (Großunternehmen)**
   - KRITIS-Betreiber nach BSI-KritisV bleiben erfasst
   - ab 250 Mitarbeitern oder Jahresumsatz von über 50 Mio. EUR und Jahresbilanzsumme von über 43 Mio. EUR
   - Geldbußen bis zu EUR 10 Mio. oder 2% des weltweiten Jahresumsatzes
2. **Wichtige Einrichtungen (mittlere Unternehmen)**
   - Ab 50 Mitarbeitern oder 10 Mio. EUR Jahresumsatz
   - Mindestens 50 und höchstens 249 Mitarbeitende und Jahresumsatz von weniger als 50 Mio. EUR oder Jahresbilanzsumme von weniger als 43 Mio. EUR
   - ODER weniger als 50 Mitarbeiter und Jahresumsatz und Jahresbilanzsumme von jeweils mindestens 10 Mio. EUR
   - Geldbußen bis zu EUR 7 Mio. oder 1,4% des weltweiten Jahresumsatzes

#nis2know



*Anlage 1: www.bsi.bund.de/dok/nis-2-anlage-1 | Anlage 2: www.bsi.bund.de/dok/nis-2-anlage-2

Konzern- und Mehrspartenregelungen

Berechnung der Schwellenwerte

Vorsicht: Bei Schwellenwertbetrachtung gelten die Kennzahlen des Konzerns
Verbundene Unternehmen und Partnerunternehmen können mitgerechnet werden

- Partnerunternehmen – Beteiligung ab 25 % und bis 50 %
- Verbundene Unternehmen – Beteiligung von mehr als 50 %

Aber: Keine Auswirkung auf die Geltung der NIS-2-Anforderungen
Es gibt keine **Infektionswirkung** – die Anwendbarkeit der NIS-2 auf Tochtergesellschaften überträgt sich nicht auf den gesamten Konzern

§ 28 Abs. 3 BSIG – keine Berücksichtigung *„der Einrichtungsart nicht zuzuordnender Geschäftstätigkeit“*
Bei der Ermittlung von Beschäftigtenzahl, Umsatz und Bilanz sind nur solche Geschäftsbereiche zu berücksichtigen, die in den regulierten Bereich fallen (dürfen „vernachlässigbare“ Tätigkeiten außer Betracht bleiben

➢ Keine Benachteiligung breit aufgestellter Unternehmen

Rechtsunsicherheit
Sobald regulierte Tätigkeiten nicht eindeutig einer juristischen Person zugeordnet werden kann, sollten alle Beteiligten den sichersten Weg wählen und die Anforderungen umsetzen

Besonderheiten bei Mehrspartenunternehmen

Sektorabgrenzungsproblematik

Mehrspartenunternehmen wie städtische Kliniken werden nach NIS-2 durch eine relevante Tätigkeit in einem Sektor reguliert

Unklare Rechtsfrage: Ausnahme bei einer Nebentätigkeiten - § 28 Abs. 5 S. 4 BSIG

Der Begriff „vernachlässigbar" wurde durch „Nebentätigkeit" ersetzt, doch die genaue Schwelle bleibt unklar

Damit geklärt: ursprüngliche Problemfälle zur Sektorzuordnung

Lokales WLAN oder Photovoltaikanlagen auf dem Hallendach

Empfehlung für Mehrspartenunternehmen

Proaktiv auf neue Pflichten einstellen, ohne auf endgültige rechtliche Klärung zu warten

Neue Pflichten für Unternehmen

Registrierung beim BSI und Fristen

§§ 33, 34 BSIG

EINRICHTUNGSTYP	FRIST	VORAUSSICHTLICHE DEADLINE
Besonders wichtige Einrichtungen (§ 33 BSIG)	3 Monate nach Inkrafttreten	ca. April 2026
Besondere Einrichtungsarten (§ 34 iVm § 60 BSIG)	6 Monate nach Inkrafttreten	ca. Juli 2026

Im Konzern: Angabe nur einer Kontaktstelle erforderlich

Umfassendes Risikomanagement/ISMS

§ 30 BSIG

geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen

Schutzziele: Verfügbarkeit, Integrität und Vertraulichkeit

Mindestmaßnahmen nach § 30 Abs. 2 BSIG

- Konzepte zur Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs (Back-up-Management, Wiederherstellung, Krisenmanagement)
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen
- Konzepte zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Grundlegende Verfahren im Bereich Cyberhygiene und Schulungen
- Konzepte für den Einsatz von Kryptografie und Verschlüsselung
- Sicherheit des Personals, Zugriffskontrolle und Management von Anlagen
- Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikationssysteme

Maßnahmen werden für Unternehmen im digitalen Bereich verbindlich in EU-DurchführungsVO 2024/2690 konkretisiert!

#nis2know

NIS-2-Risikoanalyse

Die Risikoanalyse spielt bei der Umsetzung der Risikomanagementmaßnahmen eine zentrale Rolle. Sie ist den Risikomanagementmaßnahmen insofern vorgeschaltet, als dass eine Risikoexposition als Ergebnis der Analyse die Verhältnismäßigkeit der Risikomanagementmaßnahmen begründet.

- **Risikomanagementmaßnahmen** müssen **verhältnismäßig** und dem bestehenden Risiko einer „besonders wichtigen“ oder „wichtigen“ Einrichtung **angemessen** sein.
- Bei der **Bemessung der Verhältnismäßigkeit** sind Ausmaß der Risikoexposition, Größe der Einrichtung, Eintrittswahrscheinlichkeit und Schwere sowie Auswirkungen von Sicherheitsvorfällen zu berücksichtigen.
- **Bestandteile einer Risikoanalyse** sind: Identifikation von Bedrohungen und Schwachstellen, Risikobewertung, Bewertung von Maßnahmen, Dokumentation und Compliance, Integration in das Sicherheitsmanagement
- Bei der Wahl der Risikoanalysemethodik sind die Einrichtungen frei. Eine **Orientierung an bestehenden Standards** (z. B. BSI-Standard 200-3) wird jedoch empfohlen.

Mehr Infos: www.bsi.bund.de/dok/nis-2-risikoanalyse

Version 1.0 – 30.06.2025

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Dreistufiges Meldeverfahren

§ 32 BSIG – bei *erheblichen Sicherheitsvorfällen*

STUFE	FRIST	INHALT
Stufe 1 - Frühe Erstmeldung	Unverzüglich, spätestens binnen 24 Stunden nach Kenntnis	Frühwarnung (early warning) an das nationale Computer-Sicherheitsreaktionsteam (CSIRT) oder die Aufsichtsbehörde
Stufe 2 - Bestätigende Erstmeldung	Innerhalb weiterer 48 Stunden (d.h. spätestens 72 Stunden nach Erstkenntnis)	Ausführlichere Erstmeldung, die u.a. erste Erkenntnisse zu Schweregrad und Auswirkungen des Vorfalls enthält
Stufe 3 - Abschlussmeldung	Spätestens einen Monat nach der ersten Meldung	Detaillierte Analyse der Ursache, des Ablaufs und der ergriffenen Gegenmaßnahmen
Laufend - Zwischenmeldungen	Auf Ersuchen des BSI	Relevante Statusaktualisierungen

Unsicherheit verbleibt: was ist ein *erheblicher Sicherheitsvorfall*?

Erleichterung im Konzern: Abgabe nur einer Meldung erforderlich

#nis2know

NIS-2-Meldepflicht

Wer muss wann was ans BSI melden?

- **„Besonders wichtige“** und **„wichtige Einrichtungen“** müssen dem BSI erhebliche Sicherheitsvorfälle **melden**
- Erhebliche Sicherheitsvorfälle sind z. B. schwerwiegende **Betriebsstörungen der Dienste**, führen zu finanziellen **Verlusten** oder **Schäden** für Dritte (Konkretisierung wird beizeiten veröffentlicht)
- **Meldefristen**: Nach Kenntniserlangung 24 h für die frühe Erstmeldung, 72 h für eine Meldung und 30 Tage für Abschlussmeldung/Folgemeldung
- Die Meldung beinhaltet eine **Bewertung** des Vorfalls inkl. Schweregrad, **Auswirkungen**, Kompromittierungsindikatoren sowie **Kontaktinformationen**
- Das **BSI** quittiert Meldungen, nimmt ggf. **Kontakt** auf und verarbeitet Meldungen sanitarisiert in **Lageprodukten**

Mehr Infos: www.bsi.bund.de/dok/nis-2-meldepflicht

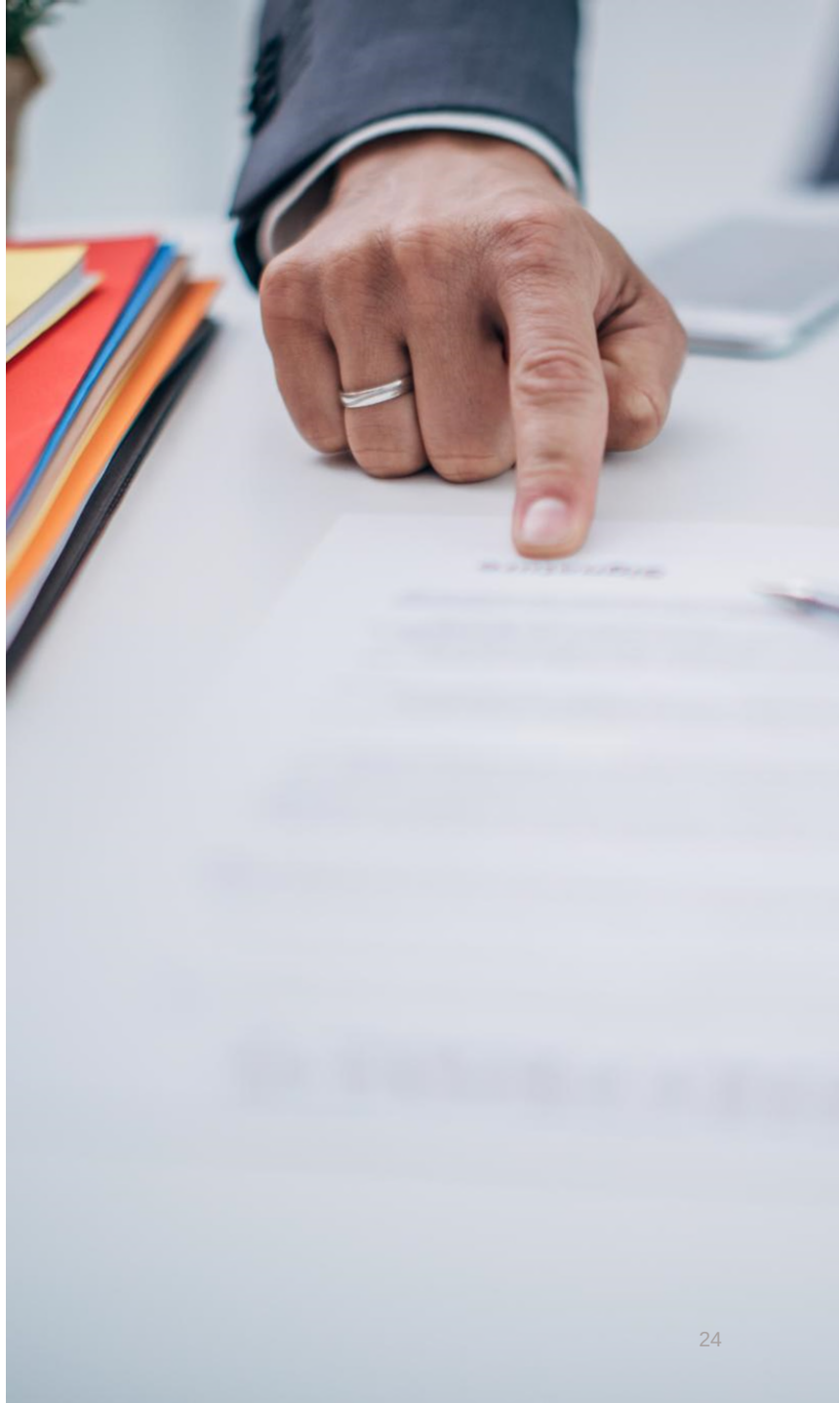
Version 1.0 – 30.06.2025

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Geschäftsleiterhaftung

1. **Billigungs- und Überwachungspflichten (§ 38 Abs. 1 BSIG)**
   - Vorstände und Geschäftsführer müssen alle wesentlichen Cybersicherheitsmaßnahmen ihres Unternehmens formal billigen und deren Umsetzung dauerhaft beaufsichtigen
   - Eine Delegation auf Dritte - etwa allein an die IT-Abteilung oder einen ISB - wäre unzulässig
2. **Persönliche Haftung (§ 38 Abs. 2 BSIG)**
   - Kommen die Leitungsorgane diesen Pflichten nicht nach, haften sie persönlich gegenüber der eigenen Gesellschaft auf Schadensersatz
   - Die Haftung greift bei schuldhafter Verletzung der Cybersicherheitspflichten und umfasst sämtliche resultierenden Schäden für die Einrichtung
   - **Besonders brisant: auch Behördenbußgelder erfasst, die aufgrund von Pflichtverletzungen verhängt werden**

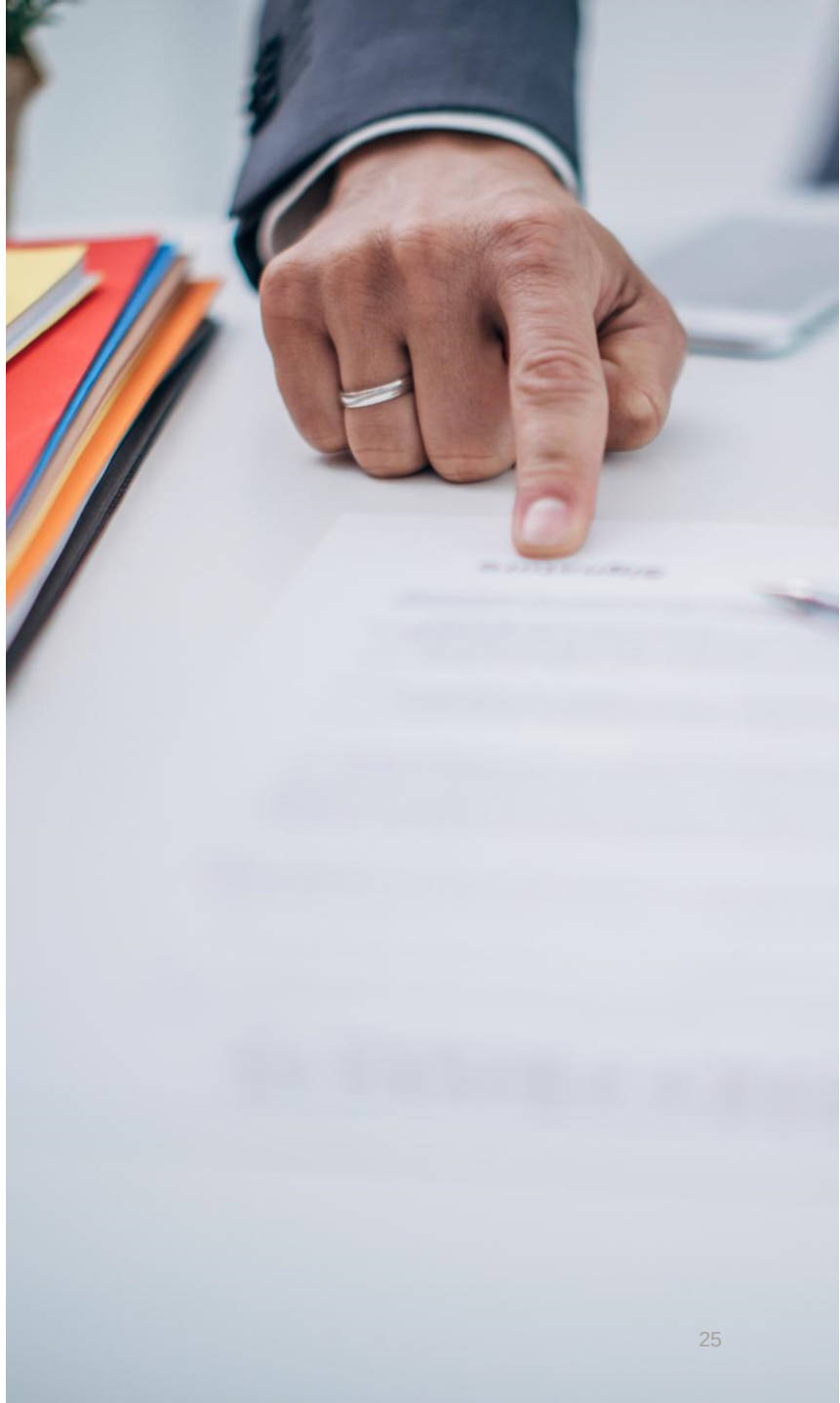


Geschäftsleiterhaftung

3. **Unverzichtbarkeit der Haftung**
    - Ein Verzicht auf solche Ersatzansprüche oder ein interner Haftungserlass ist gesetzlich ausgeschlossen - anders als in vielen anderen Compliance-Bereichen können Aufsichtsräte den Geschäftsleitern keine Absolution erteilen
4. **Schulungspflichten (§ 38 Abs. 4 BSIG)**
    - Geschäftsleiter müssen regelmäßig an Schulungen zu Cybersicherheit teilnehmen, damit sie ausreichende Kenntnisse und Fähigkeiten erwerben, um Risiken einschätzen und angemessene Sicherheitsmaßnahmen steuern zu können

Ultima Ratio: Bei gravierenden Mängeln können durch das BSI Anordnungen ergehen, welche bis zur Untersagung des Betriebs oder zur Abberufung von Geschäftsleitern auf Zeit reichen können

Praktische Konsequenz: Die persönliche Haftung der Geschäftsleitung macht Cybersicherheit zum Board-Level-Thema. Vorstände und Geschäftsführer müssen sich aktiv mit IT-Sicherheitsrisiken auseinandersetzen und können sich nicht mehr darauf berufen, dies sei Aufgabe der IT-Abteilung



Lieferkettensicherheit

§ 30 Abs. 2 Nr. 4 BSIG

Sicherheit der Supply Chain als neue zentrale Pflicht

Gesundheitsunternehmen müssen neben eigenen Systemen auch Cyberrisiken in der Lieferkette berücksichtigen und bewerten

1. **Herausforderung: Wann gehört ein Drittes Unternehmen zur *Lieferkette?***
   - Auslegung ergibt: funktionale und risikobasierte Bewertung
   - Prüffrage: Sind die Systeme dergestalt verbunden, dass Risiken für Netz- und Informationssysteme der regulierten Einrichtung entstehen können?
2. **Erfodert umfassende Risikoanalyse im Einzelfall**
   - spezifischen Schwachstellen jedes wichtigen Dienstleisters sind zu analysieren und die gesamte Cybersecurity-Praxis ihrer Anbieter, einschließlich sicherer Entwicklungsprozesse, zu berücksichtigen

Lieferkettensicherheit

3. Vertragliche Cyber-Due-Diligence

- Beim Einkauf von Hard- und Software, beim Outsourcing von IT-Diensten (z.B. Cloud) oder beim Bezug von OT-Leistungen (z.B. Leit- und Messsysteme) ist vertraglich zuzusichern, dass ihre Partner Mindeststandards der Informationssicherheit einhalten
- Tiefer Eingriff auch in bestehende Lieferbeziehungen

Praktische Umsetzung

➢ Neuverträge: Sicherheitsanforderungen vertraglich festlegen

- Mindeststandards
- Patch-Management
- Meldung von eigenen Sicherheitsvorfällen
- Recht zur Sicherheitsüberprüfung durch den Auftraggeber

➢ Altverträge: Anpassung bestehender Lieferantenverträge

- Regelmäßige Audits von Zulieferern
- Incident-Response-Koordination mit Lieferanten
- Due Diligence bei Neuverträgen

Dentons-Unterstützungsleistungen und Handlungsempfehlungen

Anwendbarkeitsprüfung und Registrierung

Strukturierte Anwendbarkeitsprüfung

Analyse der Unternehmenszugehörigkeit zu erfassten Sektoren und Prüfung relevanter Schwellenwerte.

Kategorisierung und Tätigkeitsanalyse

Einstufung als kritische oder wichtige Einrichtung und Bewertung von Mehrsparten- und Nebentätigkeiten.

Registrierungsbegleitung beim BSI

Unterstützung bei elektronischer Registrierung inklusive Datenübermittlung und Fristwahrung.

ISMS-Implementierung und Incident-Response-Readiness

ISMS-Implementierung

Bewertung der Sicherheitsmaßnahmen und Entwicklung detaillierter Informationssicherheitsrichtlinien für alle relevanten Bereiche.

Risikoanalyse und Dokumentation

Regelmäßige Bewertung von Cyberrisiken und Erstellung der erforderlichen Policies, Prozesse und Unterstützung bei der Erlangung von Nachweisen zur Vorbereitung auf Zertifizierungen.

Incident-Response-Readiness

Aufbau eines CSIRT oder Incident-Response-Prozesses mit Notfallplänen und Meldeverfahren zur Einhaltung der NIS-2-Anforderungen.

Konzernweite Lösungen

Harmonisierte Umsetzung in komplexen Unternehmensstrukturen

Handlungsempfehlungen

Unmittelbare Sofortmaßnahmen

Betroffenheitsprüfung und Sektorzuordnung klären, Schwellenwerte und Kategorisierung ermitteln. Fristen beachten und Registrierung vorbereiten.

IT-Sicherheitsanalyse

Bestandsaufnahme der IT-Sicherheit und Gap-Analyse zu NIS-2-Anforderungen durchführen. Kritische Lücken identifizieren und bewerten.

Mittelfristige Maßnahmen

ISMS ausbauen, Risikomanagement etablieren, technische Schutzmaßnahmen umsetzen und Lieferkettensicherheit priorisieren.

Governance und Compliance

Cybersecurity als Teil der Corporate Governance integrieren, Geschäftsleitung schulen, Verantwortlichkeiten definieren und Compliance überwachen.

Fazit und Ausblick

Umfassende Veränderungen durch NIS2

Die NIS2-Richtlinie fordert Unternehmen in der Gesundheitsbranche zu umfassenden Anpassungen auf, um den neuen Sicherheitsanforderungen gerecht zu werden.

Frühzeitige Anpassung notwendig

Eine rechtzeitige Umsetzung von Sicherheitsmaßnahmen hilft, Risiken zu minimieren und Compliance sicherzustellen.

Herausforderungen für Gesundheitsunternehmen

Unternehmen in der Gesundheitsbranche stehen vor neuen Herausforderungen durch die NIS2, die strategisches Handeln erfordern.

IT-Sicherheitsnetzwerk Berlin-Brandenburg

„Ihr kompetenter Ansprechpartner für IT-Sicherheit“

Alina Bungarten

Netzwerkmanagerin
alina.bungarten@itsbb.net

Webpage:

www.itsbb.net

- Das IT-Sicherheitsnetzwerk für Berlin und Brandenburg „it’s.BB e.V.“ steht als kompetenter Ansprechpartner für alle Fragen der IT-Sicherheit zur Verfügung und bietet ein sehr breites Spektrum an Kompetenzen:
  - IT-Sicherheitslösungen,
  - IT-Sicherheitsdienstleistungen,
  - IT-Infrastrukturen,
  - IT-Forensik,
  - Beratung,
  - Audits,
  - IT-Rechtsfragen und vieles mehr.
- Unsere Aktivitäten:
  - Regelmäßige Awareness-Veranstaltungen
  - NIS-2 Angebot - Kostenlose Informationen zur NIS-2-Richtlinie - Digitalagentur Berlin
  - Laufende Bearbeitung unserer Arbeitspakete (AP)
  - Akquisition und Bearbeitung gemeinsamer Projekte

it’s.BB wird durch Bundes- und Landesmittel der Gemeinschaftsaufgabe Verbesserung der regionalen Wirtschaftsstruktur“ (GRW) finanziert

Herzlichen Dank für die Aufmerksamkeit

Fragen?

Sprechen Sie uns gerne an!

Lorenz Wascher

Counsel
Berlin
D +49 30 2 64 73 437
E lorenz.wascher@dentons.com

Karolina Vonková, LL.M. (Medizinrecht)

Senior Associate
Berlin
D +49 30 2 64 73 304
E karolina.vonkova@dentons.com