Betroffenheit, Pflichten und Haftung der Geschäftsleitung gemäß NIS-2

Vortrag von

Sabine Sobola
Geschäftsführerin der
LiiDU GmbH und Rechtsanwältin

Veranstalterin: IHK Regensburg für Oberpfalz/Kelheim

online
am 24.03.2026

Sabine Sobola

- Rechtsanwältin und
- Geschäftsführerin

  der LiiDU GmbH
- IT- und Datenschutzrecht seit 1998

Agenda

1. Die NIS-2-Richtlinie

2. Das deutsche Umsetzungsgesetz zu NIS-2, v.a. das neue BSIG

3. Speziell: Haftung und Schulungspflicht der Geschäftsleitung

Einleitung:

Gesetzliche Verpflichtung zur IT-Sicherheit – Stand heute

Um was es geht: Gefahren für die IT-Sicherheit

Innentäter

Hacker, Viren,…
(Außentäter)

Systemstörungen

Folgen von Datensicherheitsverlust:

- Wirtschaftliche Schäden
- Reputationsverlust
- Rechtliche Konsequenzen

Was bedeutet IT-Sicherheit/Datensicherheit?

- **Vertraulichkeit:** Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
- **Verfügbarkeit:** Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen haben dem Benutzer zum geforderten Zeitpunkt zur Verfügung zu stehen.
- **Integrität:** Die Daten sind vollständig und unverändert.
- **Belastbarkeit:** Widerstandsfähigkeit der IT im Fehlerfall, bei Störungen und bei hoher Beanspruchung.

Gesetzliche Verpflichtungen der Unternehmen zur IT-Sicherheit

1. NIS-2, hier v.a. aus dem BSIG, v.a. die Risikomanagementmaßnahmen aus § 30 für Unternehmen aus den Sektoren nach Anhang 1 und 2 und Unternehmensgröße

2. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), ein sog. „Artikelgesetz“.

Das war noch bis 2025 eine wichtige gesetzliche Grundlage, die Anwendung auf AGs, GmbHs und im Rahmen des HGB fand. Sie verpflichtete grundsätzlich zum Risikomanagement, wozu auch die Pflicht gehört, ein angemessenes IT-Sicherheitsniveau zu gewährleisten

Bei Verstößen haften persönlich: Vorstand, Aufsichtsrat und Geschäftsführer

2. DSGVO, Art. 25 Abs. 1 und Art. 32 DSGVO

4. TDDDG, v.a. § 18 Abs. 4 TDDDG

5. § 165 Abs. 1 S. 2 TKG

6. DORA

7. KritisVO, als Teil des IT-Sicherheitsgesetzes 2015 und KRITIS-DachG

Definition der KRITIS nach dem alten BSIG

„Kritische Infrastrukturen“:

- Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie der Siedlungsabfallentsorgung und dem Finanz- und Versicherungswesen, vgl. alter § 2 Abs. 10 BSIG.
- „kritisch“, wenn ihr Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe befürchten ließe oder die öffentliche Sicherheit gefährden könnte.
- Was KRITIS sind ergibt sich aus der KRITIS-VO.

In der Regel -> Betreiber versorgt mehr als 500.000 Personen

Verpflichtungen nach dem alten BSIG – wichtigste Punkte:

Besondere Pflichten für Betreiber von **„kritischen Infrastrukturen“:**

- **Mindeststandards an technischer Sicherheit** für Betreiber kritischer Infrastrukturen → „Stand der Technik“ zu berücksichtigen
- **Pflicht zum Einsatz von Systemen zur Angriffserkennung** (neu seit 2021). Hier gibt es eine **Orientierungshilfe des BSI**, die auch am 18.11.2024 aktualisiert wurde.
- Betreiber kritischer Infrastrukturen müssen dem **BSI Störungen an ihren Systemen** wie Schadprogramme und Hackerattacken **melden.**
- Mindestens alle zwei Jahre **nachweisen**, dass Vorgaben des Gesetzes eingehalten werden (möglich: Sicherheitsauditierung, Prüfung, Zertifizierung)
- **Registrierung einer Kritischen Infrastruktur beim BSI und** bereits bestehenden Pflicht eine **jederzeit erreichbare Kontaktstelle** für die von ihnen betriebene Kritische Infrastruktur zu benennen.
- Pflicht zur Vorlage der für eine Bewertung aus Sicht des BSI erforderlichen Unterlagen und zur Erteilung der Auskunft.
- Pflichten im Zusammenhang mit dem Einsatz kritischer Komponenten, z.B. Erklärung des Herstellers der kritischen Komponenten über seine Vertrauenswürdigkeit (sog. **Garantieerklärung**).

Rechtsfolgen

- Rechtsfolgen bei Verstoß gegen das alte BSIG waren geregelt in § 14 BSIG-alt
  - Geldbuße bis zu 2.000.000,- EUR, wenn Betreiber kritischer Infrastrukturen Sicherheitsmängel nicht im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde beseitigen.
  - Mittlerweile sehr umfangreicher Bußgeldkatalog!

Vorteile des alten IT-Sicherheitsgesetzes

- Schaffung eines **Mindestniveaus an IT-Sicherheit** in Deutschland
- Möglichkeit eines **verbesserten Informationsaustausches** zwischen Industrie und Amtsseite:
  - Betreiber kritischer Infrastrukturen informieren BSI über jeweiligen Sicherheitsfall
  - Die beim BSI zusammenlaufenden Informationen werden ausgewertet und den Betreibern kritischer Infrastrukturen zur Verbesserung ihres Schutzes zur Verfügung gestellt
- Erweiterte **Beratungsfunktion des BSI** für Betreiber kritischer Infrastrukturen
- **Aufklärung und Sensibilisierung der Öffentlichkeit** über IT-Angriffe durch **jährlichen Bericht**

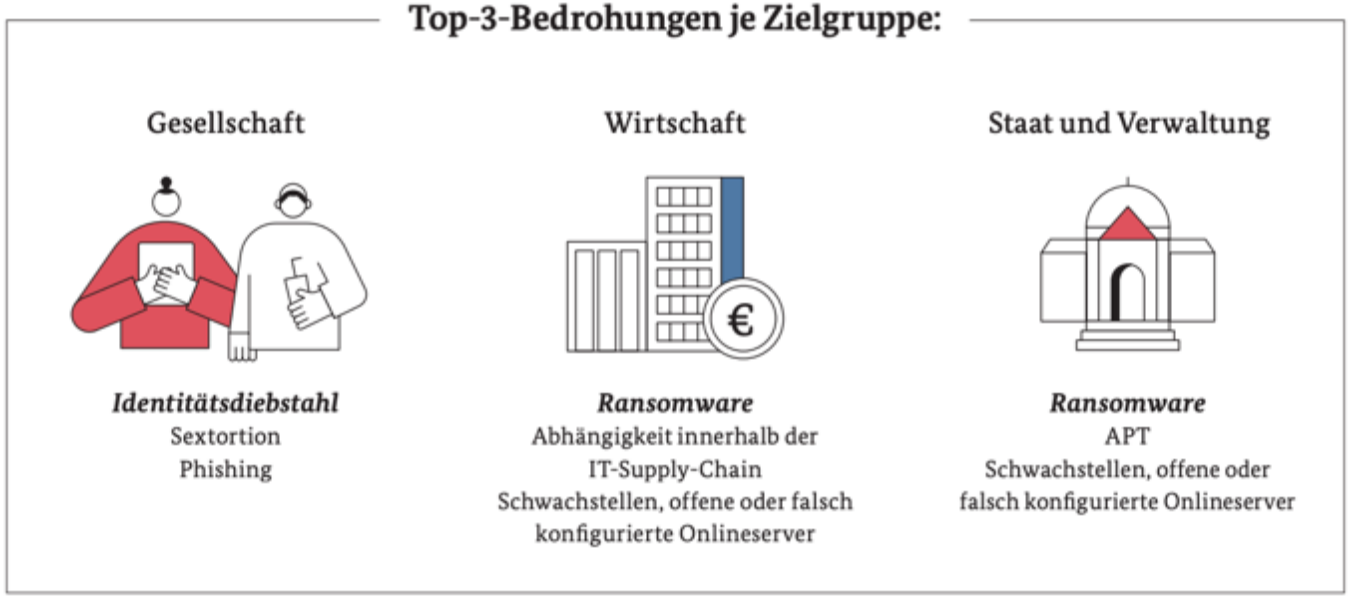
Nachteile des alten IT-Sicherheitsgesetzes

- BSI ist dem Bundesinnenministerium unterstellt → mögliche Interessenkonflikte
- Nähere Definitionsbestimmung kritischer Infrastrukturen waren nicht im Gesetz (vom Gesetzgeber) vorgesehen, sondern in Rechtsverordnung (Verwaltung) → Verwaltung definiert, welche Unternehmen in den Anwendungsbereich des Gesetzes fallen (sollte Gesetzgeber tun, ist aber auch nichts Ungewöhnliches!)
- Meldepflicht für Unternehmen schaffte neuen Aufwand
- Art. 1 § 8b Abs. 2 Nr. 4 b) BSIG-alt: BSI kann die vorliegenden Daten an die sonst zuständigen Behörden des Bundes zur Erfüllung ihrer Aufgaben weiterreichen. → „Erfüllung ihrer Aufgaben“?
- Datenschutz: wie geht das BSI eigentlich mit personenbezogenen Daten um?

Bericht des BSI 2025:

- IT-Sicherheitslage in Deutschland nach dem BSI:

  „Die IT-Sicherheitslage in Deutschland bleibt auf angespanntem Niveau. Durch die fortschreitende Digitalisierung wachsen Angriffsflächen, die zu schlecht geschützt werden. Im Kontext geopolitis(



Zusammenfassung der alten Rechtslage:

- Über diverse gesetzliche Regelungen waren Unternehmen schon immer zum Risikomanagement (auch der IT-Sicherheit) verpflichtet. Die Regelungen waren allerdings so weit, dass das die Unternehmen nicht zu mehr IT-Sicherheit veranlasste.
- 2015 kam das erste IT-Sicherheitsgesetz. Es war ein guter Schritt in die richtige Richtung zur Verbesserung der IT-Sicherheit. Es waren aber überwiegend nur die KRITIS betroffen (also Unternehmen, die Anlagen betreiben, die über 500.000 Personen versorgen).
- Kritikpunkte bis heute:
  - klare Regelungen fehlen, welche Daten für wie lange vom BSI gespeichert werden,
  - an wen und zu welchen Zwecken Daten vom BSI übermittelt werden können und
  - BSI ist nicht unabhängig genug.

Seit 06.12.2025: Gesetzgeberische Neuausrichtung

- Bisher waren „nur“ ca. 1.600 Unternehmen von den strengen IT-sicherheitsrechtlichen Vorgaben des BSIG umfasst (sog. KRITIS).
- Das alte IT-Sicherheitsgesetz (dort v.a. das alte BSIG) wurde nun durch ein **nationales Umsetzungsgesetz** (oft „NIS-2-Gesetz“ genannt) abgelöst (auf Basis der NIS-2-Richtlinie).
- Seit dem 06.12.2025 sind es **neben den KRITIS** weitere **ca. 30.000 Unternehmen**, die direkt von NIS-2 betroffen sind.
- Ob ein Unternehmen unter NIS2 fällt, muss für jeden Einzelfall gesondert geprüft werden.
- Erste Frist: **bis 06.03.2026** müssen sich die NIS-2-Unternehmen **beim BSI registrieren**: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html

Teil 1:

Die **NIS-2-Richtlinie**

Anwendungsbereich der NIS-2-Richtlinie

NIS2 = Richtlinie der EU über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Hier geht's zum Verordnungstext: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

Sektoren mit hoher Kritikalität	Sonstige kritische Sektoren
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser und Abwasser	Anbieter Digitaler Dienste
Digitale Infrastruktur	Forschung
Verwaltung von IKT-Diensten (B-to-B)	
Öffentliche Verwaltung	
Weltraum	

Anwendungsbereich der NIS-2-Richtlinie

- Unterteilung in **„wesentliche“** und **„wichtige“** Einrichtungen, Art. 3 NIS2-RL

- Dabei ist (meist) der **Sektor** und ein **Schwellenwert** ausschlaggebend dafür, ob ein Unternehmen oder Dienstleister der Richtlinie unterliegt (50 Beschäftigte oder ein Jahresumsatz von 10 Millionen Euro). Mehr Infos

- **Nicht** erfasst sind Bereiche wie Verteidigung, nationale Sicherheit, öffentliche Sicherheit, Strafverfolgung und Justiz. Auch Parlamente und Zentralbanken sind vom Anwendungsbereich ausgenommen.

Aufgabe für die Mitgliedsstaaten

Nationale Cybersicherheitsstrategie für die Mitgliedsstaaten - Art. 7 Abs. 1:

- „Jeder Mitgliedstaat erlässt eine nationale Cybersicherheitsstrategie, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält.“

Schwerpunkte für Konzepte – Art. 7 Abs. 2,. z.B.:

- Aufrechterhaltung des offenen Internets – „erforderlichenfalls einschließlich der Cybersicherheit von Unterseekommunikationskabeln“
- Förderung von neuen Technologien zum Risikomanagement
- Förderung und Entwicklung der allgemeinen und beruflichen Bildung auf dem Gebiet der Cybersicherheit u.a. durch Unterstützung der Hochschul- und Forschungseinrichtungen,
- Stärkung der Cyberresilienz und -hygiene kleiner und mittelgroßer Unternehmen.

Wesentliche Pflichten für Einrichtungen aus der NIS-2-Richtlinie:

Sicherheitsmaßnahmen für Unternehmen und Behörden im Detail - 1

Sicherheitsmaßnahmen, nun „**Risikomanagementmaßnahmen**“ nach **Art. 21** der Richtlinie:

- Die von der RL betroffenen Einrichtungen müssen geeignete **technische**, **operative** und **organisatorische Maßnahmen** zur Risikobeherrschung und Minimierung der Auswirkungen von Sicherheitsvorfällen treffen.
- **Kriterien:** Stand der Technik, europäische und internationale Normen, Kosten, Ausmaß der Risikoexposition, Größe der Einrichtung, Eintrittswahrscheinlichkeit von Vorfällen und deren Schwere, einschließlich gesellschaftlicher und wirtschaftlicher Auswirkungen
- **Mindestmaßnahmen** sind in Abs. 2 festgelegt, z.B.:
  - Backup-Management und Wiederherstellung nach einem Notfall;
  - Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
  - Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

Wesentliche Pflichten für Einrichtungen aus der NIS-2-Richtlinie:

Sicherheitsmaßnahmen für Unternehmen und Behörden im Detail - 2

- Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung;
- gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung;
- Eine der Mindestmaßnahmen umfasst **auch die Lieferkette:** Hierbei soll das Unternehmen die spezifischen Schwachstellen seiner unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.

Wesentliche Pflichten für Einrichtungen aus der NIS-2-Richtlinie: Meldepflichten im Detail

Meldepflichten nach Art. 23 der Richtlinie

- Dreistufiges Meldepflichtmodell bei erheblichem Sicherheitsvorfall:
  - Frühwarnung unverzüglich, maximal innerhalb von **24h**, ggf. Angabe ob krimineller Hintergrund oder grenzüberschreitende Auswirkung haben könnte
  - Meldung des Sicherheitsvorfalls unverzüglich, maximal innerhalb von **72h** mit erster Bewertung des Sicherheitsvorfalls
  - Zwischenbericht auf Ersuchen der Behörden
  - Spätestens nach **einem Monat** detaillierter Abschlussbericht
- Ggf. **Mitteilungspflicht an Empfänger** der Dienste über Gegenmaßnahmen, wenn auch diese potenziell bedroht sind. Ggf. auch Mitteilung über die erhebliche Cyberbedrohung selbst an die Empfänger.
- Ggf. **Information der Öffentlichkeit**, wenn Sensibilisierung der Öffentlichkeit notwendig oder sonst im öffentlichen Interesse nach Aufforderung durch Behörde.

Haftung, Sanktion und Verantwortlichkeit:
Persönliche Haftung der Führungskräfte

Persönliche Haftung der natürlichen Person, die für eine wesentliche Einrichtung verantwortlich ist

„Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können.“ (Art. 32 Abs. 6)

→ Das bedeutet eine persönliche Haftung für Führungskräfte juristischer Personen für erweiterte Cybersecuritypflichten, inklusive der bereits dargelegten Geldbuße!

Zeitlicher Fahrplan zur Umsetzung der NIS2-Richtlinie

Artikel 41 - Umsetzung

(1) Bis zum 17. Oktober 2024 erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Vorschriften ***ab dem 18. Oktober 2024*** *an.*

(2) Bei Erlass der in Absatz 1 genannten Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

- Das deutsche Umsetzungsgesetz kam erst am 06.12.2025.

Fazit:

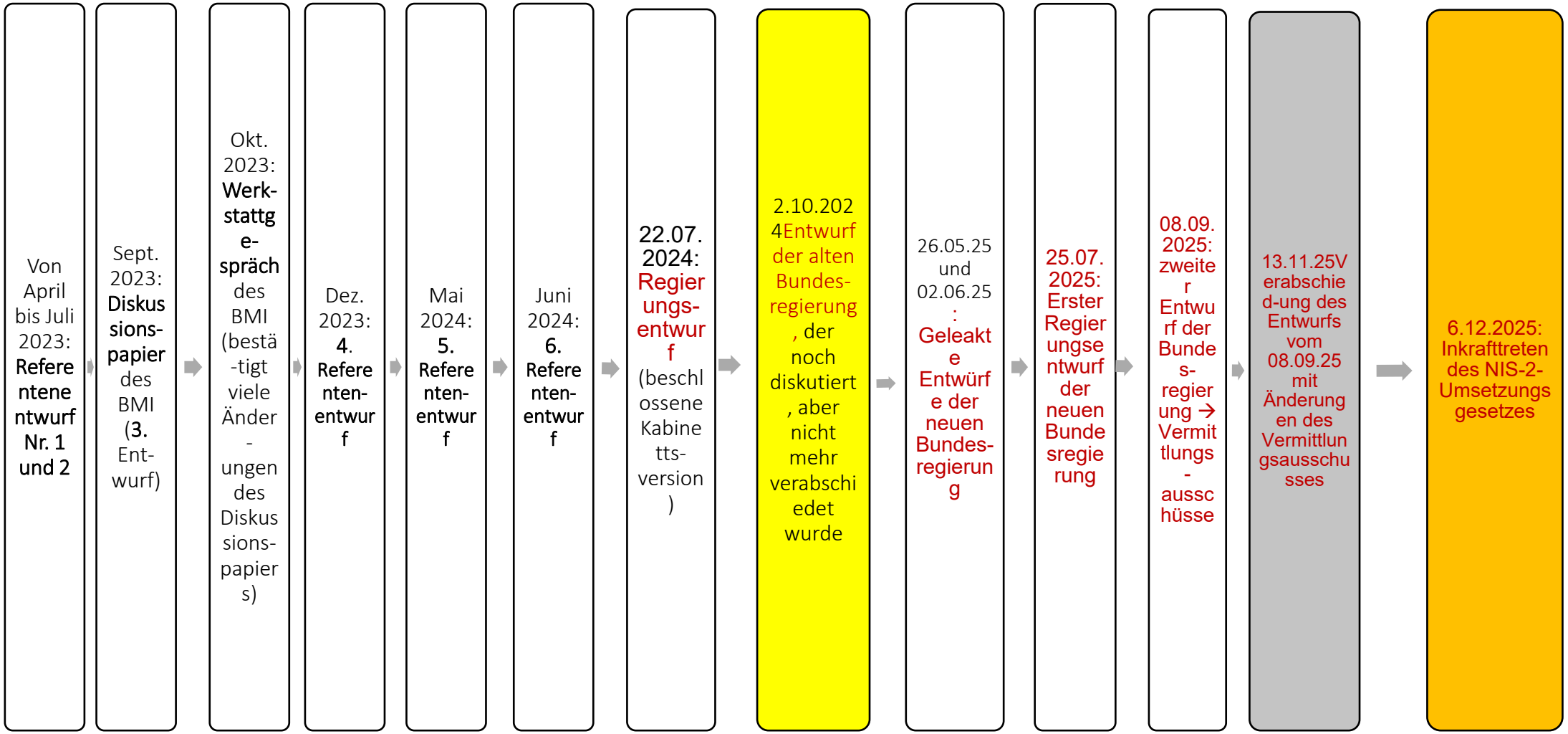
Die NIS-2-Richtlinie gibt bereits die wesentlichen Pflichten zur Cybersicherheit, den Meldepflichten und der Haftung für die Geschäftsleitung vor.

Der deutsche Gesetzgeber hat diese Inhalte dann entsprechend in deutsches Recht umgesetzt (v.a. im BSIG).

Teil 2:

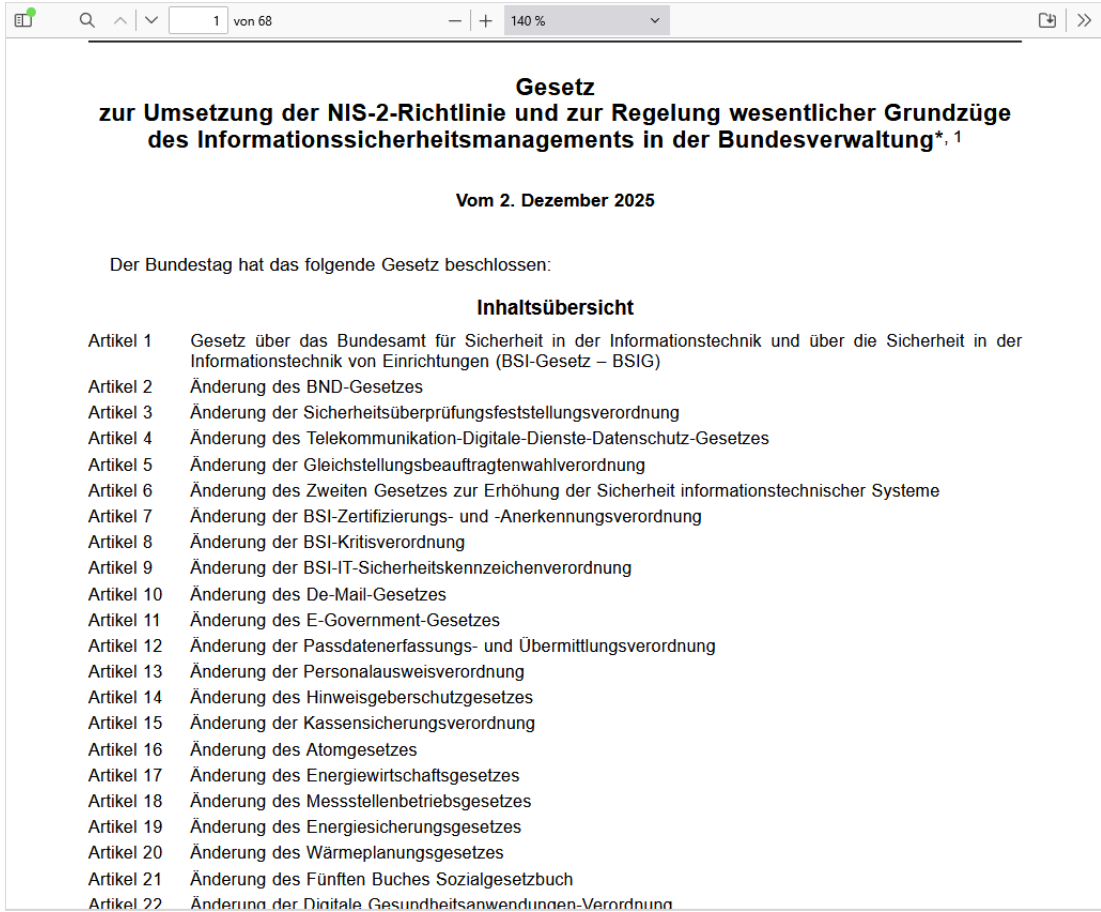
Das deutsche Umsetzungsgesetz zu NIS-2, v.a. das **neue BSIG**

Entwürfe des NIS2UmsuCG bzw. NIS-2-Gesetzes



Umsetzung von NIS-2

- Das deutsche NIS-2-Umsetzungsgesetz ist ein Artikelgesetz. Das heißt: es gibt verschiedene Artikel in dem Gesetz, von denen jeder ein anderes Gesetz verändert oder sogar neu fasst.
- In Artikel 1 des NIS-2 Umsetzungsgesetzes ist eine Neufassung des **BSI-Gesetzes** enthalten:
  - https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html
- Das BSI-Gesetz (BSIG) ist das Herzstück der deutschen Umsetzung der NIS-2-Richtlinie



1 von 68 140 %

Gesetz
zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*, [1]

Vom 2. Dezember 2025

Der Bundestag hat das folgende Gesetz beschlossen:

Inhaltsübersicht

Umsetzung von NIS-2

- Das Umsetzungsgesetz zu NIS-2 verändert die deutsche KRITIS-Regulierung deutlich.
- Neben den Betreibern kritischer Anlagen gibt es nun auch noch die besonders wichtigen und wichtigen Einrichtungen (nach NIS-2-Richtlinie: „wesentliche“ und „wichtige“ Einrichtungen).
- Die verschiedenen Gruppen am Betreibern führen zu einem Mehrklassen-System an Betreibern mit jeweils unterschiedlichen Stufen von Pflichten.

Hier findet sich das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 02.12.2025:

https://www.recht.bund.de/bgbl/1/2025/301/VO

Aus Seite 1 des BSIG zitiert:

2024 bestätigte sich die Erfahrung der Vorjahre, dass geopolitische und zwischenstaatliche Konflikte oftmals mit einer ganzen Bandbreite an Phänomenen im Cyberraum einhergehen:

*Desinformation, Hacktivismus, Spionage und Sabotage waren sowohl im russischen Angriffskrieg gegen die Ukraine als auch in der Folge des Terrorangriffs der Hamas auf Israel zu beobachten. Im Bereich der Wirtschaft zählen hierbei Ransomware-Angriffe, Ausnutzung von Schwachstellen, offene oder falsch konfigurierte Online-Server sowie Abhängigkeiten von der IT-Lieferkette und in diesem Zusammenhang auch insbesondere Cyberangriffe über die Lieferkette (sogenannte Supply-Chain-Angriffe) zu den größten Bedrohungen. Zusätzlich zu den bereits bekannten Bedrohungen entstanden in Folge des russischen Angriffskriegs auf die Ukraine und der damit einhergehenden **„Zeitenwende“** auch neue Bedrohungen oder die Einschätzungen zu bereits bekannten Bedrohungen mussten aufgrund veränderter Rahmenbedingungen geändert werden. Beispiele hierfür bestehen im Bereich Hacktivismus, insbesondere mittels Distributed-Denial-of-Service (DDoS)-Angriffen oder auch durch in Deutschland erfolgte Kollateralschäden in Folge von Cyber-Sabotage-Angriffen im Rahmen des Krieges. Zudem haben Störungen und Angriffe im Bereich der Lieferketten sowohl aus den Bereichen Cybercrime als auch in Folge der Zeitenwende zugenommen. Diese Phänomene treten nicht mehr nur vereinzelt auf,* ***sondern sind Teil des unternehmerischen Alltags geworden…***

Präzisierung der betroffenen Unternehmen – wer fällt unter NIS-2?

Als **besonders wichtige Einrichtungen** gelten gemäß **§ 28 Abs. 1 BSIG**

1. **Betreiber kritischer Anlagen**
2. **qualifizierte Vertrauensdiensteanbieter**, **Top Level Domain Name Registries** oder **DNS Diensteanbieter**
3. **Anbieter** öffentlich zugänglicher **Telekommunikationsdienste** oder öffentliche **Telekommunikationsnetze**, die

   a) mindestens 50 Mitarbeiter beschäftigen oder

   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen;

Präzisierung der betroffenen Unternehmen – wer fällt unter NIS-2?

4. Sonstige **natürliche oder juristische Personen** oder rechtlich unselbstständige **Organisationseinheiten** einer **Gebietskörperschaft**, die anderen natürlichen oder juristischen Personen **entgeltlich Waren oder Dienstleistungen anbieten**, die **einer der in Anlage 1 bestimmten Einrichtungsarten** zuzuordnen ist **und** die

a) mindestens 250 Mitarbeiter beschäftigt oder

b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

Davon ausgenommen sind Einrichtungen der Bundesverwaltung, insofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

Präzisierung der betroffenen Unternehmen – wer fällt unter NIS-2?

Als **wichtige Einrichtungen** gelten gem. **§ 28 Abs. 2:**

1. **Vertrauensdiensteanbieter**

2. **Anbieter** öffentlich zugänglicher **Telekommunikationsdienste** oder **Betreiber** öffentlicher **Telekommunikationsnetze**, die

   a) weniger als 50 Beschäftigte haben und

   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen

Präzisierung der betroffenen Unternehmen – wer fällt unter NIS-2?

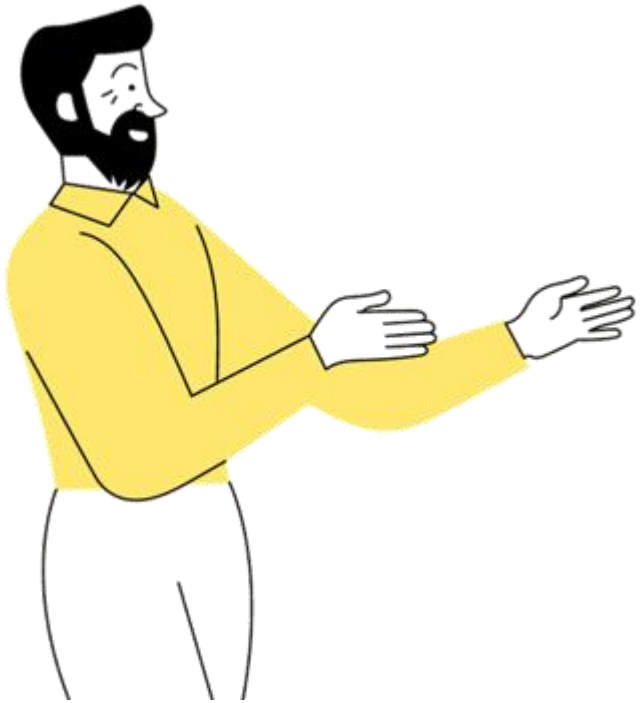
3. **natürliche** oder **juristische Person** oder eine **rechtlich unselbstständige Organisationseinheit** einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen **entgeltlich Waren oder Dienstleistungen anbietet**, die **einer der in Anlagen 1 und 2 bestimmten Einrichtungsarten** zuzuordnen ist **und** die

a) mindestens 50 Mitarbeiter beschäftigt oder

b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

Wer ist also betroffen?



- **KRITIS-Unternehmen** und
- **Besonders wichtige Einrichtungen** (Sektor aus Anlage 1 **und** entsprechende Größe/Umsatz) und
- **Wichtige Einrichtungen** (Sektor aus Anlage 1 oder 2 **und** entsprechende Größe/Umsatz)

- Die einzelnen Sektoren finden Sie hier in Anlage 1 und 2, ganz am Ende des BSIG:

https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

Ausnahme nach § 28 Abs. 3 BSIG

„(3) Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind.“

→ Es soll verhindert werden, dass eine nur geringfügige Nebentätigkeit zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt.

Zusammenrechnen der Zahlen nach § 28 Abs. 4 BSIG

„(4) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission (2003/361/EG) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden. Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission (2003/361/EG) sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.“

→ Die Zahlen zu Mitarbeitern, Jahresumsätze Jahresbilanzsumme werden zusammengezählt, wenn es sich um verbundene Unternehmen (mehr als 50% der Anteile/Stimmanteile) oder um Partnerunternehmen (mehr als 25% der Anteile/Stimmanteile) handelt.

→ Zur genaueren Bestimmung: Benutzerleitfaden der EU: https://op.europa.eu/de/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1/language-de

Betreiber kritischer Anlagen (KRITIS)

- Bisherige KRITIS-Betreiber heißen nun **„Betreiber kritischer Anlagen“.**
- Die Grundsätze zur Identifikation von KRITIS-Anlagen bleiben bestehen.

Kategorie	Sektoren
Kritische Anlagen	KRITIS: Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, Siedlungsabfallentsorgung

Betreiber kritischer Anlagen (KRITIS)

- Die Betreiber kritischer Anlagen werden automatisch zu Unternehmen der neuen NIS2-Gruppe **„besonders wichtige Einrichtungen“** und erben damit auch deren Pflichten.

  → Die bisherigen KRITIS-Pflichten für Betreiber (Identifikation, Registrierung, Meldung bis hin zu Nachweisen) bleiben im Grunde bestehen, werden durch NIS2 jedoch leicht geändert.

Pflichten von NIS-2-Unternehmen im Überblick

Die bisherigen KRITIS-Pflichten bleiben **zwar in Grundzügen erhalten,** werden teilweise aber **präzisiert, verschärft und neu strukturiert.** Die Pflichten umfassen **mindestens:**

- Cybersecurity: Umsetzung von Maßnahmen zum Risikomanagement
- Meldepflichten: Vorfallsmeldungen an das BSI
- Registrierung: Identifikation und Meldung beim BSI
- Nachweise: Prüfung zur Umsetzung und Nachweis an das BSI
- Informationspflichten: Kommunikation mit Behörden und evtl. Betroffenen
- Governance: Schulungspflicht für Leitungsorgane
- Zusätzliche KRITIS-Anforderungen: Für kritische Anlagen

Risikomanagementmaßnahmen
Allgemein – für alle NIS-2-Unternehmen

- **§ 30 Abs. 1 BSIG:** Besonders wichtige und wichtige Einrichtungen müssen **verhältnismäßige technische und wirksame technische und organisatorische Maßnahmen** ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität der informationstechnischen Systeme zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.
- **§ 30 Abs. 2 S.1 BSIG:** Die von den Betreibern und Einrichtungen umzusetzende Maßnahmen müssen auf einem **„gefahrenübergreifenden Ansatz“** beruhen.
- Zudem sollen die Maßnahmen den **Stand der Technik** einhalten.

→ Siehe § 30 des BSIG vom 02.12.2025

Risikomanagementmaßnahmen – konkret (für alle NIS-2-Unternehmen)

Die Maßnahmen müssen **mindestens** folgende Themen umfassen, **§ 30 Abs. 2, S. 2:**

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, für die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Besonderheiten für Betreiber kritischer Anlagen - Speziell für KRITIS

§ 31 BSIG: Betreiber kritischer Anlagen müssen darüber hinaus weitere Anforderungen umsetzen:

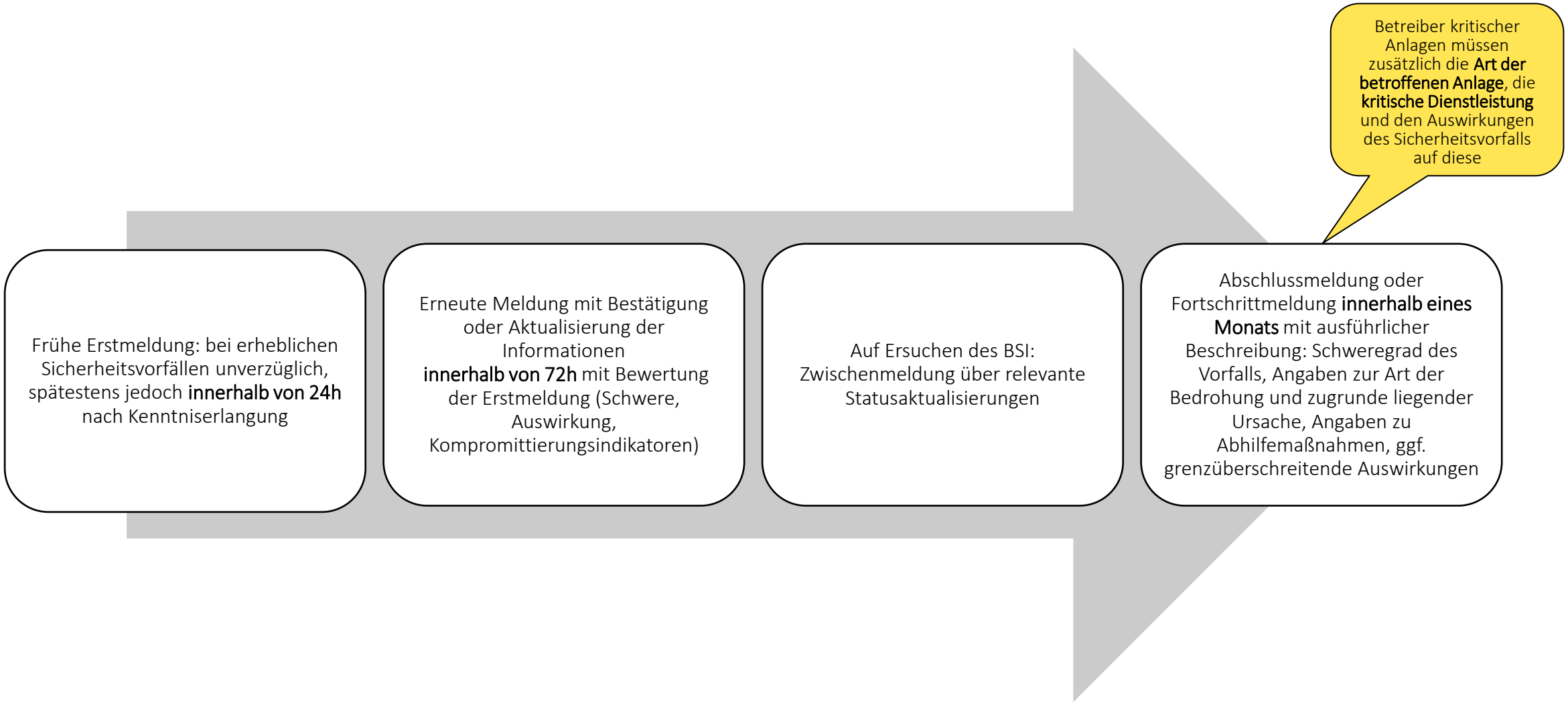
- Einsetzen von Systemen zur Angriffserkennung (fortwährendes Identifizieren von Bedrohungen sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen)

Und auch nach **§ 41 BSIG:** Untersagung des Einsatzes von Kritischen Komponenten durch das BSI ist möglich;

Informationen und Meldewesen-Pflichten für alle NIS-2-Unternehmen

- **§ 32 BSIG:** Besonders wichtige und wichtige Einrichtungen müssen dem BSI-Sicherheitsvorfälle melden.
- Dies erfolgt über eine vom BSI selbst eingerichtete Meldemöglichkeit.
- **Erheblicher Sicherheitsvorfall**: Ein Sicherheitsvorfall, der
  - schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, oder
  - andere natürliche oder juristische Personen durch erheblich materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Meldung von Sicherheitsvorfällen



Unterrichtungspflichten - Pflichten für alle NIS-2-Unternehmen

- § 35 BSIG: Bei erheblichen Sicherheitsvorfällen kann das BSI besonders wichtige und wichtige Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über die Sicherheitsvorfälle zu unterrichten.
- Einrichtungen aus dem Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und Digitale Dienste müssen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle **Maßnahmen oder Abhilfemaßnahmen** mitteilen, die die Empfänger als Reaktion auf die Bedrohung ergreifen können.
- § 36 BSIG: Falls eine Sensibilisierung der Öffentlichkeit notwendig ist, kann das BSI das Unternehmen auffordern dies zu tun.

Weitere Pflichten für betroffene Unternehmen

- **§ 33 BSIG: Registrierung beim BSI**: **spätestens 3 Monate** nachdem das Unternehmen erstmals oder erneut als Einrichtung im Sinne des NIS2UmsucG gilt oder Domain-Name-Registry-Dienste anbietet, muss es über die gemeinsam eingerichtete Meldestelle folgende Angaben übermitteln:

  1. Name der Einrichtung, einschließlich der Rechtsform und ggf. Handelsregisternummer
  2. Anschrift und aktuelle Kontaktdaten (E-Mail-Adresse, öffentliche IP-Adressbereiche, Telefon)
  3. Relevanter in Anlage 1 oder 2 genannter Sektor oder einschlägige Branche
  4. Auflistung der EU-Mitgliedsstaaten, in denen Einrichtung ihre Dienste erbringt
  5. Zuständigen Aufsichtsbehörden des Bundes und der Länder

→ Es ist mittlerweile ein Online-Meldeportal seitens des BSI freigeschaltet:

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html

Bußgeldvorschriften des § 65

(1) Ordnungswidrig handelt, wer **entgegen § 39 Abs. 1 S. 1** (in Verbindung mit einer Rechtsverordnung nach § 56 Abs. 4 S. 1) einen Nachweis nicht richtig oder nicht vollständig erbringt (gilt nur für Betreiber kritischer Anlagen).

(2) Ordnungswidrig handelt, wer **vorsätzlich oder fahrlässig... (gilt für alle!)**

- einer vollziehbaren Anordnung … zuwiderhandelt,
- Risikomanagementmaßnahmen nach § 30 Abs. 1 nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift,
- Die Einhaltung der Risikomanagementmaßnahmen nicht, nicht richtig oder nicht vollständig dokumentiert,
- einer Meldepflicht nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt,
- eine für die Registrierungspflicht erforderliche Angabe nicht, nicht richtig oder nicht vollständig übermittelt,
- über die angegebene Kontaktstelle nicht erreichbar sind,
- das Bundesamt nicht, nicht richtig oder nicht rechtzeitig über geänderte Daten im Rahmen der Registrierungspflicht informiert,
- Mitteilungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
- Nachweise nicht rechtzeitig erbringt (KRITIS),
- Zugänge nicht oder nicht rechtzeitig gewährt,
- wer vorgibt, Inhaber einer Zertifizierung zu sein, ohne dass diese besteht, …

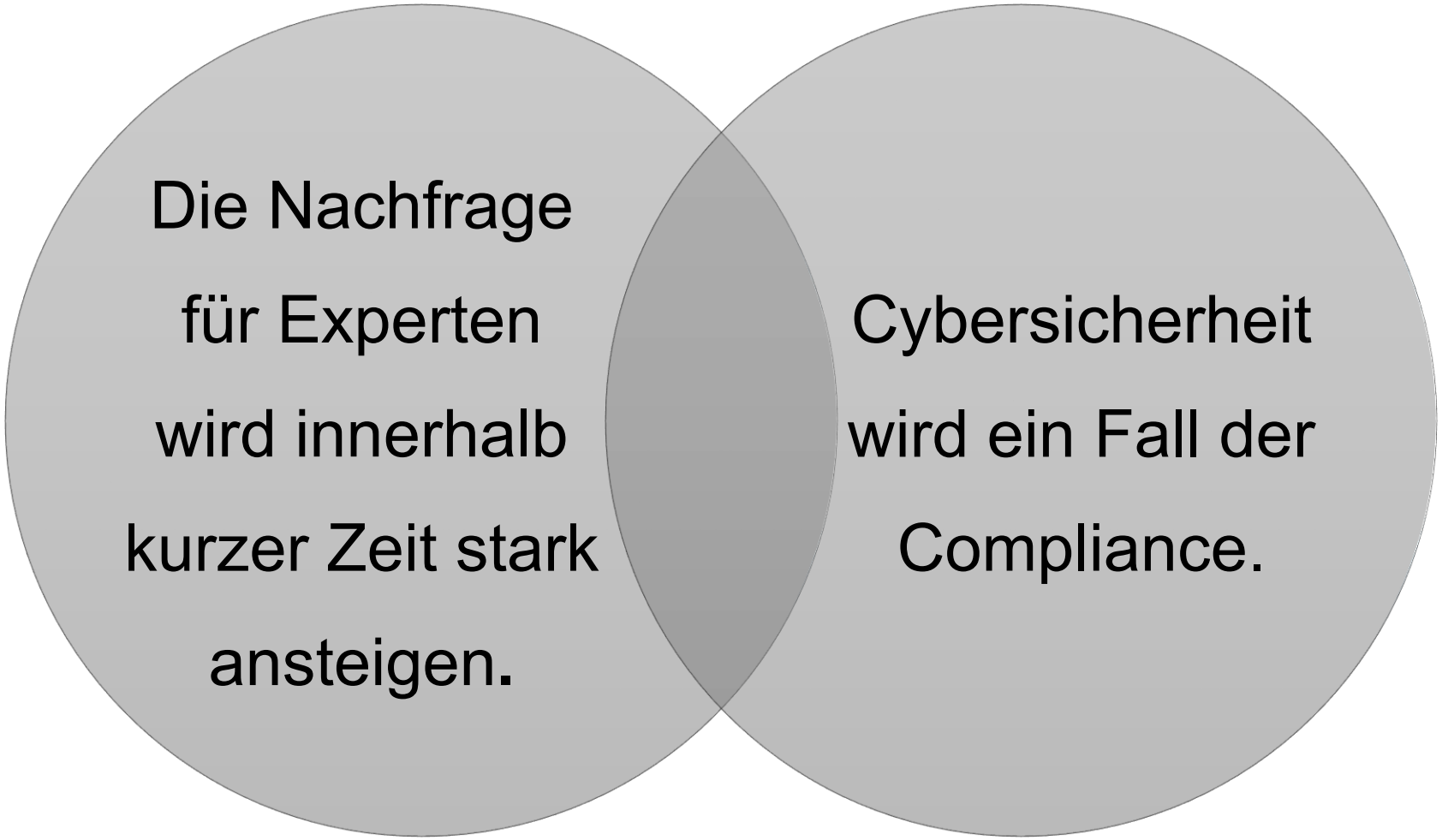
→ nahezu jede Nichterfüllung einer Pflicht ist mit einem Bußgeld versehen

Bußgeldvorschriften des § 65

- Diese Ordnungswidrigkeiten können gemäß **§ 65 Abs. 5** bis **7 mit hohen Bußgeldern** geahndet werden!
- Die Höhe ist gestaffelt. Bei manchen Verstößen kann bis zu 2% des Jahresumsatzes als Strafe angesetzt werden.

Zusammenfassung: Pflichten der Unternehmen

Bedeutung für die Praxis:



Risikomanagement - was ist das?

- Unter einem **Risiko** (im engeren Sinne) ist ein eventuelles, hinsichtlich seiner Eintrittswahrscheinlichkeit und Auswirkung bewertetes, zukünftiges Ereignis zu verstehen, das einen negativen Einfluss auf eine Organisation und ihre Handlungen hat. Nach **Eintritt eines Risikos** erfolgt somit eine **negative Abweichung vom Soll-Zustand**.
- Das Risikomanagement beinhaltet die Gesamtheit der **organisationsweiten Maßnahmen** und **Prozesse**, die das Ziel der **Identifikation, Beurteilung, Steuerung und Überwachung** von Risiken haben. Hierzu gehört auch das Informationssicherheitsmanagement.
- Das BSI hat Empfehlungen ausgesprochen, wie mit dem **Thema Risikomanagement** begonnen werden kann
  https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Risikoanalyse/NIS-2-Risikoanalyse_node.html
- … und wo die **Betroffenheitsprüfung** vorgenommen werden kann:

  https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

Fristen

- Das deutsche NIS-2-Umsetzungsgesetz gilt seit dem 06.12.2025.
- Die **Registrierung** als wichtige oder besonders wichtige Einrichtung hatte **bis 06.03.2026** über das BSI-Portal zu erfolgen. Wer noch nicht registriert ist: so schnell wie möglich **nachholen**.
- Änderungen hinsichtlich der Registrierungsangaben dann regelmäßig (innerhalb von 2 Wochen nach tatsächlicher Änderung) mitteilen
- Die ersten Nachweisprüfungen werden wohl **frühestens ab Winter 2028/2029** stattfinden.

Achtung, für digitale Dienste gilt was Spezielles:

Wer von der Durchführung-VO für **digitale Dienste/Infrastrukturen** betroffen ist: ganz bestimmte Risikomanagementmaßnahmen müssen eigentlich bereits seit Oktober 2024 umgesetzt sein.

- Link zum ersten „Implementing Act“ (Durchführungs-VO): https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

Teil 3:

Haftung und Schulungspflichten der Geschäftsleitung bezüglich NIS-2

Sinn und Zweck der Geschäftsleitungshaftung

- Mit der Umsetzung der NIS-2-Richtlinie steigen die Anforderungen an Unternehmen, die Cybersicherheits-maßnahmen systematisch zu planen, umzusetzen und zu überwachen.
- Besonders im Fokus steht dabei die **Verantwortung der Geschäftsleitung**: Sie muss gewährleisten, dass Cybersicherheit integraler Bestandteil der Geschäfte des Unternehmens und des Risikomanagements ist bzw. wird.
- Diese **besondere Verantwortung** der Geschäftsleitungen ist gesetzlich vorgeschrieben, ebenso wie eine **Schulungspflicht für die Geschäftsleitungen**.

Umsetzungs- , Überwachungs- und Schulungspflicht für Geschäftsleitungen, § 38 BSIG-E

- Abs.1: Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.
- Abs. 2: Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.
- Abs. 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 Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Bedeutung der Geschäftsleiterhaftung

- Verantwortungsübernahme: Die Geschäftsleitung soll für die ausreichende Umsetzung angemessener Cybersicherheitsstrategien verantwortlich sein.
- Rechenschaftspflicht: Führungskräfte sollen haftbar gemacht werden können, wenn sie die Anforderungen nicht angemessen umsetzten.
- Förderung der Unternehmenskultur: Die Geschäftsleitung soll eine Kultur der Cybersicherheit fördern, in der angemessene Sicherheitspraktiken auf höchster Ebene unterstützt und durchgesetzt werden.

Stellungnahme des Gesetzgebers

- § 38 dient der Umsetzung des Art. 20 der NIS2 Richtlinie und der dort vorgesehenen Pflichten der organschaftlichen Geschäftsleitungen.
- Zu Abs. 1: Die Geschäftsleitungen müssen dafür sorgen, dass die konkret zu ergreifenden Maßnahmen zunächst auch tatsächlich umgesetzt werden und deren Umsetzung kontinuierlich überwachen.

→ Es können Hilfspersonen eingeschaltet werden, das Leitungsorgan bleibt aber letztverantwortlich.

- Zu Abs. 2: Die Binnenhaftung des Geschäftsleitungsorgans bei Verletzung von Pflichten nach dem BSI-Gesetz ergibt sich grundsätzlich aus den allgemeinen Grundsätzen.

Beispiele hierfür: § 93 AktG, § 43 Abs. 2 GmbHG

Fehler, die auf die Führungsebene zurückfallen können

- Erfolgt ein Cyberangriff auf das Unternehmen, weil keine ausreichenden Sicherheitsmaßnahmen implementiert wurden, kann die Führungsebene dafür haftbar gemacht werden.
- Das gilt auch wenn ein Verstoß auf Unachtsamkeit oder Nachlässigkeit der IT-Abteilung zurückzuführen ist.

Typische Fehler:

- In der IT-Infrastruktur bestehen Schwachstellen, die über längere Zeit nicht behoben wurden.
- Das Unternehmen hat keine angemessenen Mitarbeiterschulungen zur Cybersicherheit durchgeführt, weshalb Angreifer mit einer Phishing-Attacke Erfolg hatten.
- Es erfolgte keine angemessene Risikobewertung oder Sicherheitsüberprüfung der eingesetzten Systeme, wodurch Datenlecks entstanden und Informationen in die falschen Hände geraten sind.

Fehler, die auf die Führungsebene zurückfallen können, wenn z.B. kein Back-Up eingespielt werden kann (oder keines da ist)

Beispiel: Fasana

https://www1.wdr.de/nachrichten/rheinland/insolvenz-nach-cyberangriff-bonn-100.html

- Der IT-Sicherheitsvorfall beim Euskirchener Serviettenhersteller **Fasana GmbH** im Mai 2025 gilt als drastisches Beispiel dafür, wie ein Cyberangriff ein Unternehmen in die Insolvenz treiben kann.
- Der Sachverhalt: Es handelte sich um eine professionelle **Ransomware-Attacke**. Kriminelle verschlüsselten zentrale Server und Systeme des Unternehmens. Der Vorfall wurde offensichtlich, als sämtliche Firmendrucker begannen, **Erpresserschreiben** auszugeben. Darin forderten die Täter eine Kontaktaufnahme über das Darknet.
- Alle Rechner mussten vom Netz genommen werden, Aufträge konnten nicht mehr abgewickelt werden, Lieferscheine, Rechnungen etc. konnten nicht mehr erstellt, versandt oder eingesehen werden. Die Produktion kam komplett zum Erliegen.
- Innerhalb von 2 Wochen summierte sich der Umsatzverlust auf 2 Millionen Euro. Das Unternehmen musste Insolvenz anmelden. 240 Arbeitsplätze stehen auf dem Spiel. Bisher konnte kein Investor gefunden werden.

Delegation von Aufgaben und der Nachweis

- Bei NIS-2 haftet die Geschäftsführung (auch) persönlich.
- Eine vollständige Delegation **der Haftung** ist **nicht möglich,** aber eine wirksame Delegation von **Aufgaben** (z. B. an CISO, IT-Leitung) mit klaren Verantwortlichkeiten, Prozessen und Reporting (über den dann auch der Nachweis möglich ist) ist möglich, um die Risikomanagement- und Meldepflichten zu erfüllen.
- Das BSI unterstützt als zentrale Stelle bei der Umsetzung, bietet Tools wie die Betroffenheitsprüfung und das Starterpaket und erwartet eine enge Kooperation zwischen Staat und Wirtschaft für die Cyberresilienz.

Mehr dazu unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun.html

Schulungspflicht der Geschäftsleiter

- Zudem **schreibt das Gesetz vor,** dass Geschäftsleiter besonders wichtiger und wichtiger Einrichtungen **regelmäßig an Schulungen teilnehmen** müssen.
- Leiter von Einrichtungen der Bundesverwaltung gelten nicht als Geschäftsleitung.
- Zweck: Erwerb von Kenntnissen und Fähigkeiten zur **Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken** im Bereich der Cybersicherheit und auf die von der Einrichtung erbrachten Dienste.

Zur Schulungspflicht gibt es bereits ein **Merkblatt des BSI:**

- https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Geschaeftsleitungsschulung/NIS-2-Geschaeftsleitungsschulung_node.html

Schulungspflicht der Geschäftsleiter

- Es gibt auch eine Schulung des BSI zum Thema „Schulungspflicht der Geschäftsleitung“.
- Wer die Unterlagen haben möchte, kann diese unter info@liidu.de anfragen.

Herzlichen Dank für Ihre Aufmerksamkeit!

NIS-2 Schulung für Geschäftsleiter und das Top-Management nach §38 BSIG

Pflichten für die Geschäftsleitung,
Risikomanagementmaßnahmen und
Risikoanalyse nach § 38 BSIG
im Kontext des NIS-2-Regulierung

Early-Bird-Angebot

799,- € zzgl. USt.

02. 07. 2026

ONLINE - SEMINAR

RECHTSANWÄLTIN
SABINE SOBOLA

Jetzt anmelden!

LiiDU

LinkedIn

LiiDU

Sabine Sobola · 1.

Geschäftsführerin der LiiDU GmbH und selbständige Rechtsanwältin

Regensburg, Bayern, Deutschland · **Kontaktinfo**

Zum kostenlosen Newsletter anmelden

www.liidu.de/newsletter

info@liidu.de

0941 46392460

www.liidu.de

Let`s connect - **LinkedIn**

Sie brauchen Unterstützung? Wir sind für Sie da!

- **Externer Datenschutzbeauftragter** (Ext. DSB)
- **Externer KI-Beauftragter** (AI-Officer)
- **Seminare und Fortbildungen**
  im Bereich Recht und Datenschutz
- **Individuelle Beratung**
  im Bereich Datenschutz, IT und IT-Security
- Immer Up-to-date mit dem
  LiiDU-Weekly