IDW KNOWLEDGE PAPER

DAS **NIS-2-UMSETZUNGSGESETZ**

VORGABEN UND HANDLUNGSEMPFEHLUNGEN IM ÜBERBLICK

STAND 22.02.2026

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

EINLEITUNG

Das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungsgesetz)[1] ist am 6. Dezember 2025 in Kraft getreten und setzt die in der NIS-2-Richtlinie[2] der EU geregelten einheitlichen europäischen Sicherheitsstandards in deutsches Recht um.

Umgesetzt wird die Richtlinie vor allem mittels einer Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG). Das BSIG ist Bestandteil des NIS-2-Umsetzungsgesetzes. Mit dem Inkrafttreten des neuen BSIG wird dessen Anwendungsbereich erheblich erweitert. Insbesondere Organisationen, die für die Grundversorgung der Bevölkerung wichtig sind, müssen künftig strengere Regeln zur IT-Sicherheit einhalten. Dazu zählen u.a. entsprechende Meldefristen bei Sicherheitsvorfällen und Maßnahmen zum Schutz der Systeme. Schätzungen gehen davon aus, dass sich die Anzahl der neuregulierten Organisationen von ca. 4.500 auf ca. 29.500 Organisationen erhöht.

1. BETROFFENE SEKTOREN UND ORGANISATIONEN

Organisationen müssen selbstständig prüfen, ob sie unter das neue BSIG fallen. Eine Information von Seiten einer staatlichen Stelle erfolgt nicht. Die Betroffenheit ergibt sich, wenn eine Organisation in die Kategorien „besonders wichtige Einrichtungen" (§ 28 Abs. 1 BSIG) oder „wichtige Einrichtungen" (§ 28 Abs. 2 BSIG) fällt.

Als besonders wichtige Einrichtung gelten die folgenden Organisationen:

- Betreiber kritischer Anlagen, d.h. Anlagen, die für die Erbringung einer kritischen Dienstleistung erheblich sind

- Qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter

- Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
  - entweder mindestens 50 Mitarbeiter beschäftigen oder
  - einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen

- sonstige Organisationen, die einer der in Anlage 1 des BSIG bestimmten Einrichtungsarten zuzuordnen sind (Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur oder Weltraum) und
  - entweder mindestens 250 Mitarbeiter beschäftigen oder
  - einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.

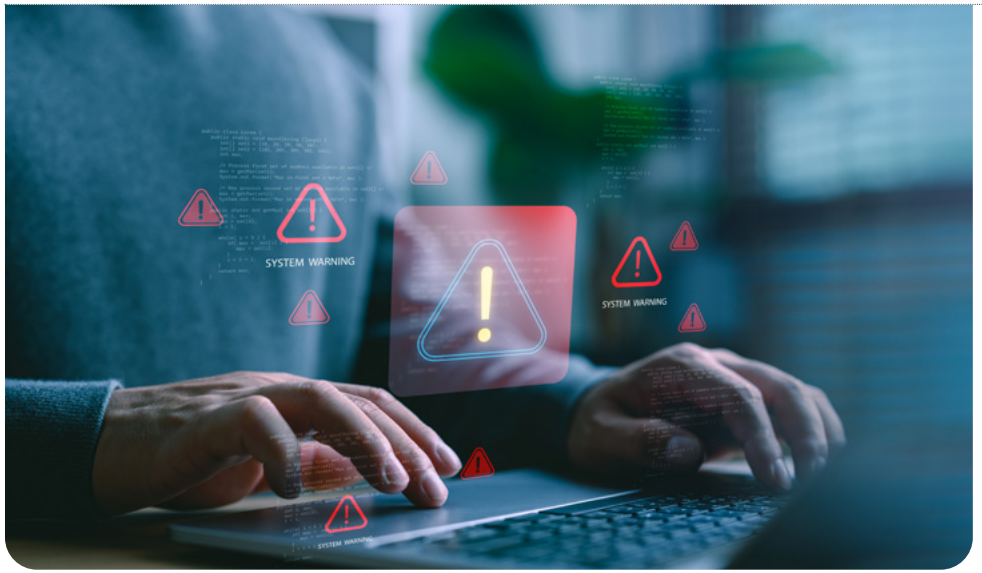
Wichtige Einrichtungen sind die folgenden Organisationen:

- Vertrauensdiensteanbieter

- Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die weniger als 50 Mitarbeiter beschäftigen und einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen

- sonstige Organisationen, die einer der in den Anlagen 1 und 2 des BSIG bestimmten Einrichtungsarten zuzuordnen sind (Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur, Weltraum, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste oder Forschung) und
  - entweder mindestens 50 Mitarbeiter beschäftigen oder
  - einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen

Darüber hinaus fallen auch Einrichtungen der Bundesverwaltung, wie Bundesbehörden, öffentlich-rechtlich organisierte IT-Dienstleister und bestimmte Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unter das NIS-2-Umsetzungsgesetz (§ 29 BSIG).



2. ANFORDERUNGEN AN DIE ORGANISATIONEN

Besonders wichtige und wichtige Einrichtungen müssen zentralen Risikomanagement-, Melde-, Registrierungs-, Überwachungs- und Schulungspflichten sowie Nachweispflichten nachkommen.

Risikomanagement (§ 30 und 31 BSIG)

Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, um Störungen zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten (§ 30 Abs. 1 BSIG).

Störungen beziehen sich auf die Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die die Einrichtungen für die Erbringung ihrer Dienste nutzen.

Die Maßnahmen – technische und organisatorische – müssen geeignet, verhältnismäßig und wirksam sein und den Stand der Technik einhalten. Sie sind zu dokumentieren. Der Mindestumfang dieser Maßnahmen ist in § 30 Abs. 2 BSIG geregelt und umfasst u.a.

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- grundlegende Schulungen und Sensibilisierungsmaßnahmen
- Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren
- Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung.

Für Betreiber kritischer Anlagen gilt die zusätzliche Verpflichtung, Systeme zur Angriffserkennung einzusetzen (§ 31 Abs. 2 BSIG).

Meldepflichten (§ 32 BSIG)

Bei erheblichen Sicherheitsvorfällen, d.h. Sicherheitsvorfällen, die (1) entweder schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht haben oder verursachen können oder (2) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt haben oder beeinträchtigen können, gilt ein dreistufiges Meldeverfahren:

- innerhalb von 24 Stunden muss eine frühe Erstmeldung an das BSI erfolgen
- innerhalb von 72 Stunden muss eine aktualisierte Meldung mit der Bewertung des Sicherheitsvorfalls an das BSI erfolgen
- innerhalb eines Monats muss schließlich eine detaillierte Abschlussmeldung an das BSI erfolgen.

Registrierungspflichten (§ 33 und 34 BSIG)

Besonders wichtige und wichtige Einrichtungen sowie Domain-Name-Registry-Dienstleister müssen sich innerhalb von drei Monaten, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name-Registry-Dienste anbieten, beim BSI registrieren und bestimmte Angaben übermitteln, u.a. IP-Adressbereiche.

Überwachungs- und Schulungspflichten (§ 38 BSIG)

Mitglieder der Geschäftsleitung sind verpflichtet, die Umsetzung der Risikomanagementmaßnahmen zu überwachen. Sie müssen darüber hinaus regelmäßig an Schulungen teilnehmen, um Risiken und Risikomanagementmaßnahmen richtig einschätzen zu können.

Nachweispflichten (§ 39 BSIG)

Betreiber kritischer Anlagen unterliegen der Pflicht, dem BSI die Umsetzung der Maßnahmen alle drei Jahre durch entsprechende Prüfungen nachzuweisen.

3. HANDLUNGSEMPFEHLUNGEN FÜR POTENZIELL BETROFFENE

Unternehmen wird empfohlen, zeitnah festzustellen, ob sie in den Anwendungsbereich des NIS-2-Umsetzungsgesetz fallen. Hierzu kann u.a. die NIS2-Betroffenheitsprüfung des BSI genutzt werden[3]. Sie haben sich innerhalb von drei Monaten im BSI-Portal zu registrieren. Weitere Schritte zur Einhaltung der Anforderungen aus dem NIS-2-Umsetzungsgesetz können u.a. sein:

- Identifizierung und Analyse relevanter Anforderungen und Pflichten sowie die Berücksichtigung branchenspezifischer Besonderheiten
- Festlegung von Verantwortlichkeiten
- Analyse und Berücksichtigung von Lieferketten
- Erhebung des Ist-Zustands im Hinblick auf Cybersicherheitsmaßnahmen
- individuelle Risikobewertung und Ableitung von Handlungsbedarfen im Sinne einer Gap-Analyse
- Umsetzung von Risikomanagementmaßnahmen (Anpassung von Prozessen, Umsetzung von technischen und organisatorischen Maßnahmen)
- Einrichtung von Meldeprozessen sowie
- Schulung der Mitarbeiter.

4. HINWEISE FÜR WIRTSCHAFTSPRÜFER

Wirtschaftsprüfer können die Unternehmen bei der Umsetzung der erforderlichen Maßnahmen aus dem NIS-2-Umsetzungsgesetz unterstützen und Prüfungen im Rahmen der Nachweispflichten (§ 39 BSIG) durchführen.

Bei Abschlussprüfungen können Maßnahmen aus der NIS2-Umsetzung genutzt werden: So können die vom Unternehmen umgesetzten Maßnahmen aus dem NIS-2-Umsetzungsgesetz sowie die Ergebnisse von Prüfungen im Rahmen der Nachweispflichten verwendet werden. Sie helfen ggf. dabei, Risken aus dem IT-Einsatz zu erkennen und festzustellen, ob generelle IT-Kontrollen eingerichtet sind und ob diese wirksam sind.

Erlangt der Abschlussprüfer Kenntnis davon, dass das zu prüfende Unternehmen, sich nicht über das BSI-Portal registriert hat, obwohl es offensichtlich in den Anwendungsbereich des NIS-2-Umsetzungsgesetzes fallen würde, sollten die verantwortlichen Unternehmensorgane hierüber zeitnah in Kenntnis gesetzt werden. Darüber hinaus kann eine Berichtspflicht im Prüfungsbericht vorliegen, sofern es sich dabei um eine Tatsache handelt, die schwerwiegende Verstöße der gesetzlichen Vertreter gegen Gesetz, Gesellschaftsvertrag oder Satzung erkennen lassen (§ 321 Abs. 1 S. 3 HGB).

FUSSNOTEN

1 Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, BGBl. 2025 I Nr. 301 vom 05.12.2025.

2 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022.

3 Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html (Stand: 06.02.2026)

Dieses Knowledge Paper wurde von der IDW Geschäftsstelle erarbeitet.

Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an Grit Baum, Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf oder an grit.baum@idw.de senden.

INSTITUT DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E.V.

Roßstraße 74
40476 Düsseldorf

Postfach 32 05 80
40420 Düsseldorf

Telefon: +49 (0) 211/4561-0
Telefax: +49 (0) 211/4561097

E-Mail: info@idw.de
Web: www.idw.de