BVMed Bundesverband Medizintechnologie e.V.

Infoblatt

# Umsetzung der NIS-2-Richtlinie im BSI-Gesetz

Juni 2026

Seit dem 6. Dezember 2025 gilt das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2-UmsuCG) in Deutschland, das Änderungen im BSI-Gesetz mit sich bringt. Es begründet weitreichende **Cybersicherheitspflichten** für Unternehmen in bestimmten Sektoren – darunter auch Hersteller von Medizinprodukten.

## Auf wen sind die Vorgaben anwendbar?

Das BSI-Gesetz (BSIG) ist auf Betreiber kritischer Anlagen sowie Betreiber (besonders) wichtiger Einrichtungen anwendbar. [1]

**Betreiber kritischer Anlagen** sind natürliche oder juristische Personen, die unter Berücksichtigung der **rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss** auf eine oder mehrere kritische Anlagen ausüben. Kritische Anlagen sind Betriebsstätten, die **kritische Dienstleistungen** erbringen zur Versorgung der Allgemeinheit in festgelegten Sektoren (Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, Transport und Verkehr, Siedlungsabfallentsorgung), deren Ausfall oder Beeinträchtigung zu **erheblichen Versorgungsengpässen** oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Die Einordnung als Betreiber kritischer Anlagen richtet sich nach den Sektoren und Schwellwerten nach dem KRITIS-Dachgesetz und der BSI-KritisV.

Das **BSIG** definiert in Umsetzung der NIS-2-Richtlinie nun besonders wichtige („wesentliche“ nach NIS-2 Richtlinie) und wichtige Einrichtungen. Für **Betreiber (besonders) wichtiger Einrichtungen** kommt es zunächst auf eine Tätigkeit in einem Sektor der **Anlage 1** (z. B. Gesundheit, Energie, digitale Infrastruktur) oder **Anlage 2** (z. B. Medizinprodukthersteller, verarbeitendes Gewerbe) an. Als nächster Schritt ist anhand von Schwellenwerte zu prüfen, ob eine **besonders wichtige Einrichtung** (mindestens 250 Mitarbeiter oder mehr als 50 Mio. EUR Jahresumsatz und mehr als 43 Mio. EUR Jahresbilanzsumme) oder eine **wichtige Einrichtung** (mindestens 50 Mitarbeiter oder mehr als 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme) vorliegt. Zu berücksichtigen ist, dass bestimmte Einrichtungen (z.B. Telekommunikationsdienste, Vertrauensdienstanbieter, Anbieter von Cloud-Computing, Rechenzentren und anderen digitalen Infrastrukturen.) **unabhängig** von ihrer Größe erfasst sind.

[1] Der Begriff der kritischen Anlagen findet sich nicht in der NIS-2 RL; er ist definiert im deutschen KRITIS-DachG. Das deutsche BSIG behandelt sowohl (besonders) wichtige Einrichtungen als auch kritische Anlagen.

# Wie werden die Schwellenwerte berechnet?

Die **Schwellenwerte** in Bezug auf Mitarbeiterzahl, Jahresumsatz und -bilanzsumme sind mit Hilfe der Empfehlung der Kommission zur Definition von Kleinstunternehmen, kleinen und mittleren Unternehmen (2003/361/EG) zu ermitteln. Zu beachten ist, **dass Partner- oder verbundenen Unternehmen** im Sinne der Empfehlung **nicht** in den Jahresumsatz bzw. die -bilanz hinzuzurechnen sind, 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.

# Was sind (besonders) wichtige Einrichtungen?

**Besonders wichtige Einrichtungen oder wichtige Einrichtungen** (Anlage 1 BSIG) sind unter anderem:

- Gesundheitsdienstleister i.S.d. Richtlinie 2011/24/EU
- Hersteller von Pharmazeutika (NACE C 21)
- Referenzlaboratorien nach Art. 15 Verordnung (EU) 2022/2371
- Arzneimittelentwickler nach § 2 AMG
- Betreiber von Cloud-Computing und Rechenzentren

**Wichtige Einrichtungen** (Anlage 2 BSIG) sind u.a.:

- Hersteller von Medizinprodukten nach MDR (EU) 2017/745 und IVDR (EU) 2017/746
- Hersteller von Datenverarbeitungsgeräten (NACE C 26)

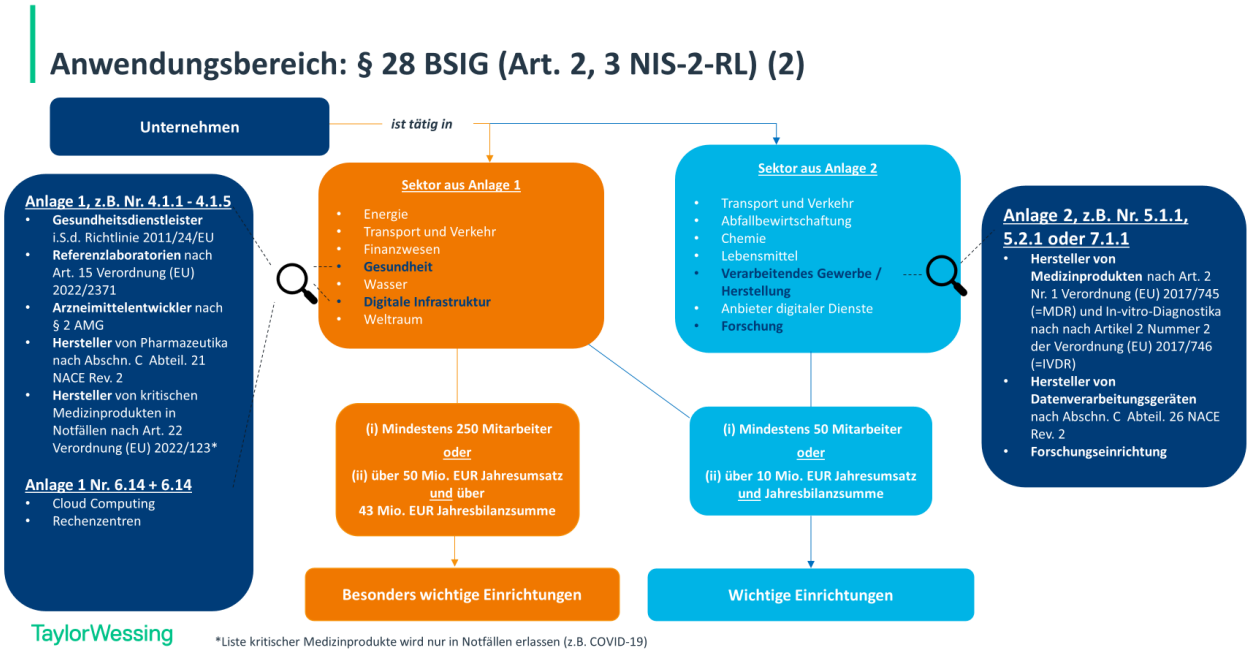


Abbildung 1: Eigene Darstellung

*Kritische Medizinprodukte werden über eine Liste definiert, welche nur in Notfällen erlassen wird (z.B. Pandemie). Einen solchen Notfall hat es seit dem Erlass der Verordnung im Jahr 2022 noch nicht gegeben. Im Fall eines Notfalls und des Erlasses einer solchen Liste könnte ein Hersteller von Medizinprodukten daher vom Betreiber einer wichtigen Einrichtung zum Betreiber einer besonders wichtigen Eirichtung werden.

## Welche Pflichten haben Betreiber (besonders) wichtiger Einrichtungen?

Die **Leitungsorgane** sind für die Umsetzung der Risikomanagementmaßnahmen verantwortlich. Regelmäßige Schulungen sind verpflichtend. Weitere zentrale Pflichten im Überblick:

- **Risikomanagementmaßnahmen** (§§ 30, 31 BSIG): Risikoanalyse, Lieferkettensicherheit, Krisenmanagement, Cyberhygiene, Multi-Faktor-Authentifizierung, Verschlüsselung.
- **Meldepflichten** (§ 32 BSIG): Erstmeldung innerhalb von 24 Stunden, Folgemeldung innerhalb von 72 Stunden, Abschlussmeldung innerhalb eines Monats.
- **Registrierung** (§§ 33, 34 BSIG): Eigenständige Identifikation und Registrierung innerhalb von drei Monaten.
- **Unterrichtung von Kunden** (§ 35 BSIG): U.U. müssen Kunden über Sicherheitsvorfälle informiert werden.
- **Nachweise** (§ 39 BSIG): Betreiber kritischer Anlagen müssen alle drei Jahre Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen.

## Was sind Risikomanagementmaßnahmen?

Einrichtungen müssen **geeignete, verhältnismäßige und wirksame** technische und organisatorische Maßnahmen ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer IT-Systeme, Komponenten und Prozesse zu vermeiden.

Mindestanforderungen umfassen u. a.:

- Konzepte zur Risikoanalyse und IT-Sicherheit,
- Prozesse zur Bewältigung von Sicherheitsvorfällen und zum Krisenmanagement,
- Maßnahmen zur Sicherung der Lieferkette,
- Verfahren zur Bewertung der Wirksamkeit der Maßnahmen, Cyberhygiene und Schulungen,
- Konzepte und Verfahren zur Kryptografie und Verschlüsselung, Zugriffskontrolle und Multi-Faktor-Authentifizierung.

Für Betreiber kritischer Anlagen gelten über das Schutzniveau der (besonders) wichtigen Einrichtungen hinausgehende Maßnahmen als **verhältnismäßig**, sofern der Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls steht. Zusätzlich müssen sie zwingend ein System zur Erkennung von Angriffen einsetzen. Die Maßnahmen sind am Stand der Technik auszurichten, der eine fortlaufende Anpassung an technische Entwicklungen und Bedrohungslagen verlangt. Hilfestellung können allgemeine oder branchenspezifische **technische Standards** wie Durchführungsverordnung (EU) 2024/2690, ISO 27001, oder IEC 81001-5-1 bieten.

## Wie funktionieren die Meldepflichten?

Betreiber kritischer Anlagen, besonders wichtige und wichtige Einrichtungen müssen erhebliche Sicherheitsvorfälle unverzüglich an das BSI melden.

Das Melderegime ist dreistufig ausgestaltet:

- **Erstmeldung** binnen 24 Stunden mit einer ersten Einschätzung, ob rechtswidrige oder böswillige Handlungen oder grenzüberschreitende Auswirkungen vorliegen,
- **Meldung** binnen 72 Stunden mit erster Bewertung von Schwere, Auswirkungen und Kompromittierungsindikatoren,

- **Abschluss- oder Fortschrittsmeldung** spätestens einen Monat nach Abschluss bzw. fortlaufende Fortschrittsberichte bei andauernden Vorfällen.

Die letzte Meldung sollte einen **ausführlichen Bericht** einschließlich Schweregrad, Auswirkungen, Angaben zur Bedrohung, bzw. zugrunde liegende Ursachen, getroffene und laufende Abhilfemaßnahmen, ggf. grenzüberschreitende Auswirkungen enthalten.

## Wer muss sich registrieren?

Betreiber mit Hauptniederlassung in Deutschland müssen sich innerhalb von **drei Monaten** ab Geltung als (besonders) wichtige Einrichtung, kritischer Anlage, oder bestimmte weitere Akteure (z. B. Anbieter von Cloud-Diensten, Rechenzentren, Domain-Name-Registry-Diensteanbieter) beim BSI registrieren (https://portal.bsi.bund.de/). Für bestehende Einrichtungen ist diese Frist am 6. März 2026 abgelaufen.

## Wann müssen Kunden unterrichtet werden?

Das BSI kann Betreibern kritischer Anlagen, besonders wichtiger und wichtiger Einrichtungen anordnen, ihre Kunden über erhebliche Sicherheitsvorfälle zu unterrichten. Die Unterrichtung kann auch durch Veröffentlichung auf der **Internetseite** der Einrichtung erfolgen, es ist keine unmittelbare Kontaktaufnahme notwendig.

In **bestimmten Sektoren** (Finanzwesen, Sozialversicherungsträger, Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste) müssen Einrichtungen ihre Kunden und das BSI **eigenständig** über Abhilfemaßnahmen und erhebliche Cyberbedrohungen informieren, wenn die Interessen der Kunden überwiegen.

## Welche Nachweise sind zu erbringen?

Betreiber kritischer Anlagen müssen **regelmäßig nachweisen**, dass sie die Risikomanagementmaßnahmen (einschließlich Systemen zur Angriffserkennung) umgesetzt haben, z. B. durch Audits, Prüfungen oder Zertifizierungen.

## Welche Befugnisse hat das BSI?

Für Betreiber kritischer Anlagen und besonders wichtige Einrichtungen sind anlasslose Überprüfungsmaßnahmen möglich, etwa stichprobenartige Audits, Prüfungen oder Zertifizierungen.

Das BSI kann Nachweise über die Erfüllung der Verpflichtungen verlangen und bei Verstößen verschiedene Maßnahmen anordnen, etwa:

- Anweisungen zur Verhütung oder Behebung von Vorfällen,
- Anordnung zur Unterrichtung potenziell betroffener Personen,
- Aussetzung fachrechtsspezifischer Genehmigungen.

Bei wichtigen Einrichtungen kann das BSI entsprechende **Maßnahmen ergreifen**, wenn Tatsachen die Annahme rechtfertigen, dass NIS-2-Pflichten nicht oder nicht richtig umgesetzt sind.

## Welche Sanktionen gibt es?

Die Leitungsorgane sind verpflichtet, die **Risikomanagementmaßnahmen** umzusetzen und deren Umsetzung zu überwachen. Sie haften nach den allgemeinen gesellschaftsrechtlichen Grundsätzen (Binnenhaftung); § 38 Abs. 2 BSIG enthält einen Auffangtatbestand, soweit keine spezielle Haftungsregelung besteht.

Für Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen sind **regelmäßige Schulung zur Cybersicherheit** verpflichtend; das BSI stellt hierzu eine Handreichung zur Verfügung.

Verstöße gegen die Pflichten nach dem BSIG können zu **erheblichen Bußgeldern** führen: Für Betreiber kritischer Anlagen und besonders wichtige Einrichtungen bis zu 10 Mio. EUR oder bis zu 2 % des weltweiten Jahresumsatzes bei Umsätzen über 500 Mio. EUR, für wichtige Einrichtungen bis zu 7 Mio. EUR oder bis zu 1,4 % des weltweiten Jahresumsatzes bei Umsätzen über 500 Mio. EUR. Unabhängig davon gibt es **allgemeine Bußgeldtatbestände** mit Höchstbeträgen von 100.000 EUR bis 2 Mio. EUR je nach Verstoß.

**Kontakt**
**Natalie Gladkov**
Referat Digitale Medizinprodukte
gladkov@bvmed.de

**Dr. Katja Marx**
Referat Recht
marx@bvmed.de

**BVMed**
Bundesverband Medizintechnologie e.V.
Georgenstraße 25, 10117 Berlin
+49 30 246 255 - 0
info@bvmed.de
www.bvmed.de

Lobbyregister beim Deutschen Bundestag: R000486
EU-Transparenzregister: 103122495301-83