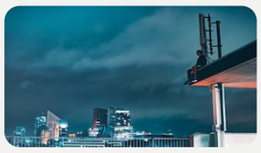
NIS2 Umsetzungsgesetz

Gesetze
NIS2-Umsetzung
KRITIS-Dachgesetz
Sektoren
Anlagen
Einrichtungen
Verordnung
Gesetzgebung
Behörden

Das Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit, das NIS2UmsuCG, wird ab 2024 in Kraft treten. Es überführt die EU-weiten Mindeststandards für Cybersecurity der EU-Direktive NIS2 in deutsche Regulierung. Die NIS2-Umsetzung wird große Teile der deutschen Wirtschaft mit bestimmt 30.000 Unternehmen betreffen.

Unternehmen | Cybersecurity | Informationen | Staat und BSI | Ausblick | *in English*

Das Gesetz liegt als Entwurf für das Kabinett von Juli 2024 vor und muss 2024 noch die Gesetzgebung auf Bundesebene durchlaufen. Geplant ist das Inkrafttreten nun März 2025. Neben NIS2 wird das KRITIS-Dachgesetz kritische Betreiber mit Resilienz und BCM regulieren. Das OpenKRITIS-Mapping von NIS2 auf ISO 27001 und KRITIS erleichtert die Umsetzung.



NIS2 und KRITIS-Dachgesetz: Was kommt auf Unternehmen zu?

Ausblick auf die neue KRITIS, NIS2 und CER-Regulierung ab 2024

Deutsch · PDF · Juli 2024 · OpenKRITIS-Briefing

Die Umsetzung von NIS2

Neue Cybersecurity-Regulierung ab 2024

Das NIS2-Umsetzungsgesetz ändert die deutsche KRITIS-Regulierung deutlich – neben den Betreibern kritischer Anlagen die »besonders wichtigen« und »wichtige Einrichtungen«. Für über 30.000 betroffene Unternehmen in Deutschland steigen die Security-Pflichten.

- Betreiber: Betroffen sind Betreiber kritischer Anlagen (KRITIS) und Einrichtungen nach Unternehmensgröße sowie Bundeseinrichtungen und einige Sonderfälle.
- Sektoren: Die KRITIS-Sektoren der kritischen Anlagen bleiben bestehen, die Einrichtungen umfassen wie in der EU in NIS2 neben Infrastruktur nun große Teile der Wirtschaft.
- Cybersecurity: Umfassende Sicherheitsmaßnahmen und großer Geltungsbereich im ganzen Unternehmen: Risikomanagement, Vorfallsmeldungen, technische Maßnahmen, Governance.
- Prüfungen: Nachweispflicht für Betreiber kritischer Anlagen alle drei Jahre, für Einrichtung

Dokumentationspflicht und Stichproben durch Behörden.

- Aufsicht: Mehr staatliche Befugnisse durch Registrierungen, Nachweise, Meldepflichten. Die geteilte Regulierung über verschiedene Behörden wie BSI, BBK, BNetzA etc. nimmt zu.
- Sektorgesetze: Ebenso geändert werden das TKG und EnWG, um Anforderungen von NIS2 für dortige Betreiber abzubilden. Für Finanzunternehmen wird DORA einschlägig.
- Sanktionen: Erweiterte Sanktionsvorschriften mit neuen Bußgeldtatbeständen und erhöhten Bußgeldern zwischen 100 Tsd. und 20 Mio. EUR, teils gekoppelt an den weltweiten Umsatz.

Stand der Dinge

Folgende öffentliche Entwürfe des NIS2-Umsetzungsgesetzes sind bekannt, Änderungen unten.

Nr.	Version	Datum	Kommentar
1.	Referentenentwurf	April 2023	
2.	Referentenentwurf	Juli 2023	
3.	Diskussionspapier	September 2023	unvollständig
3a.	Werkstattgespräch	Oktober 2023	Abstimmung Wirtschaft und BMI
4.	Referentenentwurf	Dezember 2023	
5.	Referentenentwurf	Mai 2024	Verbändeabstimmung
6.	Referentenentwurf	Juni 2024	Verbändeabstimmung
7.	Kabinettsversion	Juli 2024	beschlossene Version
8.	Regierungsversion	Oktober 2024	Bundestag 20/13184

Tabelle: *Versionen NIS2UmsuCG, Stand Oktober 2024*

Das NIS2-Umsetzungsgesetz wurde im Juli 2024 im Kabinett beschlossen und wird zeitnah den weitere Weg der Gesetzgebung nehmen. Der weitere Weg sieht die nächsten Schritte in der Gesetzgebung (Bundestag und Bundesrat) bis Ende 2024 und Inkrafttreten im März 2025 vor.

↑ UP

Betroffene Unternehmen

Unternehmen in Deutschland

Die von NIS2 betroffenen Unternehmen in Deutschland bestehen aus drei (vier) Gruppen: Die bestehenden Betreiber kritischer Anlagen (KRITIS), die besonders wichtigen sowie die wichtigen Einrichtungen und einige Bundeseinrichtungen: §28

1. Besonders wichtige Einrichtungen nach Größe des Unternehmens in Sektoren Anlage 1
   - G Unternehmen ab 250 Mitarbeitern **oder**
   - G Unternehmen über 50 Mio. EUR Umsatz und Bilanz über 43 Mio. EUR
   - U Größenunabhängig: qTSP, TLD, DNS, TK-Anbieter, kritische Anlagen
   - M Sonderfall: TK-Anbieter ab mittlere Größe
2. Wichtige Einrichtungen nach Größe des Unternehmens in Sektoren aus Anlage 1 2
   - M Unternehmen ab 50 Mitarbeitern **oder**
   - M Unternehmen über 10 Mio. EUR Umsatz und Bilanz über 10 Mio. EUR
   - U Vertrauensdienste und TK-Anbieter
3. Betreiber kritischer Anlagen (KRITIS-Betreiber) stellen weiterhin mit KRITIS-Methodik die Betroffenheit einzelner Anlagen fest, auch im KRITIS-Dachgesetz
   - KRITIS-Anlage über Schwellenwert, in der Regel ≥ 500 Tsd. versorgte Personen

4 Neben Einrichtungen werden auch Bundeseinrichtungen mit Pflichten reguliert §29

↑ UP

Einrichtungen

Besonders wichtige und wichtige Einrichtungen

Die **besonders wichtigen Einrichtungen** §28 (1) sind Großunternehmen bestimmter Sektoren, einige Unternehmen unabhängig ihrer Größe und Betreiber kritischer Anlagen. Die **wichtigen Einrichtungen** §28 (2) sind Großunternehmen und mittlere Unternehmen in vielen Sektoren.

Einrichtung	Größe	Sektoren
Besonders wichtig §28 (1)	Großunternehmen aus Anlage 1	Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum
	unabhängig	Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste
	ab mittlere Unternehmen	Öffentliche TK-Netze und TK-Dienste
	unabhängig	Betreiber kritischer Anlagen (KRITIS-Betreiber)
Wichtig §28 (2)	Mittlere Unternehmen aus Anlage 1	Energie, Transport/Verkehr, Finanzenwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum
	Großunternehmen Mittlere Unternehmen aus Anlage 2	Post/Kurier, Siedlungsabfallentsorgung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung
	unabhängig	Vertrauensdienste
	unabhängig	Öffentliche TK-Netze und TK-Dienste

Tabelle: *eigene Zusammenstellung Stand Juli 2024*

Weitere

Einrichtungen der Bundesverwaltung (Staat) sind separat reguliert und erben Pflichten der besonders wichtigen Einrichtungen §29 sowie eigene Pflichten aus Kapitel 3.

Die Unternehmen im besonderen öffentlichen Interesse (UBI) fallen als separate Kategorie weg und gehen größtenteils in den Einrichtungen auf: UBI 1 *Rüstung* fallen größtenteils in den NIS2-Sektor verarbeitendes Gewerbe, UBI 2 *volkswirtschaftliche Bedeutung* verteilen sich über alle NIS2-Sektoren und UBI 3 *Gefahrstoffe* fallen in den Sektor Chemie.

↑ UP

Unternehmensgröße

Die Einrichtungen unterscheiden sich nach Unternehmensgröße: Mitarbeiter, Umsatz und Bilanz. Besonders wichtige Einrichtungen in §28 (1) und wichtige Einrichtungen in §28 (2).

Einrichtung	Sektoren	Größe	Mitarbeiter	Umsatz und Bilanz
Besonders wichtig	1	G Großunternehmen G Großunternehmen	≥ 250	> 50 Mio. + > 43 Mio. EUR
Wichtig	1 2	M ab mittlere Unternehmen M ab mittlere Unternehmen	≥ 50	> 10 Mio. + > 10 Mio. EUR

Die Mitarbeiter- und Finanzzahlen können dabei von Einrichtungen potenziell auf die "der Einrichtungsart zuzuordnenden Geschäftstätigkeit" spezifiziert werden. §28 (3)

↑ UP

Betreiber kritischer Anlagen (KRITIS)

Die bisherigen KRITIS-Betreiber, die Kritischen Infrastrukturen, werden zu **Betreibern kritischer Anlagen**. §28 (6) Die KRITIS-Logik von KRITIS-Sektoren, kritischen Dienstleistungen und Anlagen mit Schwellenwerten bleibt hier erhalten. Die Betreiber werden gleichzeitig auch *besonders wichtige Einrichtungen.* §28 (1) Nr. 1

Betreiber	Größe	Sektoren
Kritische Anlagen Verordnung	Anlagen mit Schwellenwerten §28 (7)	Energie, Transport und Verkehr, Finanz-/Versicherungswesen, Gesundheitsweisen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, Siedlungsabfallentsorgung

Tabelle: *eigene Zusammenstellung Juli 2024*

↑ UP

NIS2-Sektoren

In der NIS2-Umsetzung gibt es zwei Gruppen von Sektoren: Sektoren der Einrichtungen sind in Anlage 1 und 2 definiert, KRITIS-Sektoren für kritische Anlagen separat in der Verordnung. Für Einrichtungen sind 1 »Sektoren hoher Kritikalität« und 2 »Sonstige kritische Sektoren.«

KRITIS	Sektoren hoher Kritikalität 1 und Teilsektoren	Sonstige kritische Sektoren 2 und Teilsektoren
Energie	Energie Stromversorgung, Fernwärme/-kälte, Kraftstoff/Heizöl, Gas	
Transport/Verkehr	Transport/Verkehr Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr	Transport/Verkehr Post und Kurier
Finanzen/Versicherung	Finanzwesen Banken, Finanzmarkt-Infrastruktur	Chemie Herstellung, Importeure (NACE 20)
Gesundheit	Gesundheit Dienstleistungen, Referenzlabore, F&E, Pharma (NACE C 21), Medizinprodukte,	Forschung Forschungseinrichtungen
Wasser/Abwasser	Wasser/Abwasser Trinkwasser, Abwasser	Verarbeitendes Gewerbe Medizin/Diagnostika; DV, Elektro, Optik (NACE C 26 und 27); Maschinenbau (NACE C 28), Kfz/Teile (NACE C 29), Fahrzeugbau (NACE C 30)
IT und TK	Digitale Infrastruktur IXPs, DNS, TLD, Cloud Provider, RZ-Dienste, CDNs, TSP, elektronische Kommunikation/Dienste, Managed Services und Security Services	Digitale Dienste Marktplätze, Suchmaschinen, soziale Netzwerke
Weltraum	Weltraum Bodeninfrastrukturen	
Ernährung		Lebensmittel Großhandel, Produktion, Verarbeitung

Entsorgung	Entsorgung Abfallbewirtschaftung

Tabelle: *eigene Zusammenstellung Juli 2024*

Zusätzlich sind Einrichtungen der Bundesverwaltung separat reguliert: §29

Sektor	Einrichtungen
Bundesverwaltung	Bundesbehörden öffentliche IT-Dienstleister Bundesverwaltung weitere Körperschaften nach Bestimmung BSI
	Ausgeschlossen: Auswärtiges, Verteidigung, Nachrichtendienste

Tabelle: *eigene Zusammenstellung aus NIS2-Referentenentwurf Juli 2024*

↑ UP

Cybersecurity

Pflichten von Betreibern und Einrichtungen

Die Anforderungen an Betreiber und Einrichtungen ändern sich mit der NIS2-Umsetzung deutlich. Die bisherigen KRITIS-Pflichten aus dem BSI-Gesetz bleiben in Grundzügen erhalten, werden teils präzisiert, teils verschärft und neu strukturiert.

Pflicht	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich	Anlage (?)	Unternehmen	Unternehmen
Maßnahmen Risikomanagement §30	*	✓	✓
Höhere Maßstäbe für KRITIS §31 (1)	✓		
Besondere Maßnahmen SzA §31 (2)	✓		
Meldepflichten §32	*	✓	✓
Registrierung §33 §34	✓	✓	✓
Unterrichtungspflichten (Kunden) §35	*	✓	✓
Leitungsorgane Umsetzung §38	*	✓	✓
Nachweise §39	✓	tw. (§61)	tw. (§62)

Tabelle: *eigene Zusammenstellung Stand Juli 2024*
** - implizit, da Betreiber kritischer Anlagen auch besonders wichtige Einrichtungen sind*

Ein Mapping von NIS2 auf ISO 27001 erleichtert Einrichtungen die Umsetzung der Vorgaben.

Ausschlüsse

Es gibt diverse Ausnahmen und Sonderregeln für Unternehmen zu NIS2-Pflichten.

Einrichtung	Fundort	Ausschluss von
DNS, TLD, Cloud-Computing, Rechenzentren, CDNs, Managed Services und Security Services, Marktplätze, Suchmaschinen, soziale Netzwerke, Vertrauensdienste (Internet im Sektor IT)	§30 (3)	Einzelmaßnahmen §30 (2) (Vorrang Implementing Act)

Betreiber öffentlicher TK-Netze und TK-Dienste	§28 (4)	NIS2/KRITIS-Anforderungen Meldepflichten, Kunden, Nachweise §§30, 31, 32, 35, 36, 38, 39, 61 und 62
Betreiber Energieversorgungsnetze und Energieanlagen	§28 (4)	
Finanzunternehmen nach DORA (EU) 2022/2554	§28 (5)	NIS2 und KRITIS-Pflichten Meldepflichten, Kunden Nachweise, Leitung §§30, 31, 32, 35, 36, 38, 39
gematik	§28 (5)	
Betreiber kritischer Anlagen Finanzwesen (DORA)	§28 (6)	Meldepflicht §32
Nationale Sicherheit, öffentliche Sicherheit, Verteidigung, Strafverfolgung	§37	Risikomanagement und Meldepflichten §§30,32 + Registrierung §§33-34
Bundesverwaltung (separat in §29)	§28 (1) §28 (2)	Wichtige und besonders wichtige Einrichtungen
Rechtlich unselbstständige Organisationseinheiten und juristische Personen der öffentlichen Hand außer des Bundes, die für die öffentliche Verwaltung Leistungen erbringen und durch Landesrecht reguliert.	§28 (9)	

Tabelle: *eigene Zusammenstellung Juli 2024*
weitere Einzelausschlüsse sind möglich

> *In einzelnen Sektoren entsteht trotz Ausschlüssen eine Mehrfach-Regulierung in NIS2 mit unterschiedlichen Anforderungen je nach Anwendungsbereich von NIS2, KRITIS und Sektorgesetzen.*

↑ UP

Sicherheit und Risikomanagement

Besonders wichtige und wichtige Einrichtungen müssen **geeignete, verhältnismäßige und wirksame** technische und organisatorische Maßnahmen ergreifen, um die IT und Prozesse ihrer erbrachten Dienste zu schützen, Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu vermeiden und Auswirkungen von Sicherheitsvorfällen gering zu halten. §30 (1)

Betreiber sollen das Ausmaß der Risikoexposition, Größe der Einrichtung, Umsetzungskosten, Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie die "gesellschaftlichen und wirtschaftlichen Auswirkungen" berücksichtigen. §30 (1)

Geltungsbereich

Der Geltungsbereich in betroffenen Unternehmen wird durch NIS2 deutlich erweitert. In der NIS2-Umsetzung fallen große Teile innerhalb von Unternehmen unter die Regulierung – dort müssen Einrichtungen Risiko-Management und Maßnahmen nach §30ff umsetzen.

Der Geltungsbereich von wichtigen und besonders wichtigen Einrichtungen wird in NIS2 sehr umfangreich: Begründung zu §30

- Der Geltungsbereich umfasst "sämtliche IT-Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden."
- Mit den Diensten meint der Gesetzgeber "sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden, dies beinhaltet beispielsweise auch Bfüro-IT oder andere IT-Systeme, die durch die Einrichtung betrieben werden"
- Die Maßnahmen im Geltungsbereich sollen in einem "angemessenen Verhältnis zu den Risiken stehen" und den "unterschiedlichen Grad der Risikoexposition" als Einrichtung/Betreiber berücksichtigen

Der Geltungsbereich von Betreibern kritischer Anlagen ist im Gesetz nicht genau definiert und war eigentlich begrenzter: Begründung zu §30

- Ursprünglich waren Geltungsbereich und Maßnahmen auf "IT-Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind", d.h. die

KRITIS-Anlage und notwendige und unterstützende Infrastruktur, begrenzt.

- Da Betreiber kritischer Anlagen mit NIS2 auch zu besonders wichtigen Einrichtungen werden, könnte sich dort der Geltungsbereich wie oben ausgeführt erweitern.

Dokumentation und Nachweise

Einrichtungen müssen die Umsetzung der Maßnahmen dokumentieren §30 (1) und im Zweifel dem BSI und auch Prüfer nachweisen.

↑ UP

Maßnahmen

Die von Betreibern und Einrichtungen umzusetzenden Maßnahmen müssen auf einem »gefahrenübergreifenden« Ansatz beruhen und "sollen" europäische und internationale Normen berücksichtigen.

Allgemeine NIS2-Maßnahmen

Die Maßnahmen sollen den Stand der Technik einhalten und müssen mindestens die folgenden Themen umfassen: §30 (2)

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, Beschaffung und Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Schulungen Cybersicherheit und Cyberhygiene
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

Betreiber kritischer Anlagen

Für Betreiber kritischer Anlagen gelten bei der Auswahl von Maßnahmen und Bewertung der Angemessenheit »höhere Maßstäbe« und weitere Anforderungen:

- Auch "aufwändigere Maßnahmen" gelten für §30 als verhältnismäßig §31 (2)
- Einsatz von Systemen zur Angriffserkennung §31 (2)
- Nachweispflichten (KRITIS-Prüfungen) für Maßnahmen und SzA §39 (1)

↑ UP

Konkretisierung

Eine genaue Konkretisierung der Maßnahmen durch BSI oder Verbände ist noch nicht bekannt, hier ist bis 2024 sicherlich noch Bewegung zu erwarten von Behörden aber auch Verbänden.

Mapping auf Standards

Von OpenKRITIS ist ein Mapping von NIS2 auf ISO 27001 und KRITIS sowie vom EU NIS2 Implementing Act auf ISO 27001 verfügbar.

Existierende ISMS-Zertifizierungen werden meist nicht ohne weiteres hinreichend für NIS2-Maßnahmen sein – der Geltungsbereich von NIS2 könnte über bestehende Zertifikate hinausgehen, die genannten Maßnahmen sind teils tiefer und weiter als übliche Rahmenwerke.

Sektorregelungen

Bestimmte Sektoren sind von den Vorgaben zu Risikomanagement §30 und §31 teils ausgeschlossen und werden durch sektor-spezifische Regulierung konkretisiert oder umgesetzt.

- DNS, TLD, Cloud, Rechenzentren, CDNs, Managed Services und Security Services, Online-Marktplätze und Suchmaschinen, soziale Netzwerke und Vertrauensdienste werden (sollen) durch einen Implementing Act Vorgaben zu Maßnahmen nach §30 (2) erhalten.
- Betreiber öffentlicher TK-Netze und TK-Dienste erhalten durch das TKG und den BNetzA-Sicherheitskatalog Vorgaben zu äquivalenten Maßnahmen nach §30.
- Betreiber von Energieversorgungsnetzen und Energieanlagen erhalten durch EnWG und den BNetzA-Sicherheitskatalog Vorgaben zu äquivalenten Maßnahmen nach §30.
- Einrichtungen gem. Art. 2 (4) der Verordnung (EU) 2022/2554 erhalten äquivalenten Maßnahmen durch DORA (Teile des Finanzsektors).

Implementing Acts der EU

Die Kommission kann nach Art. 21 (5) NIS2 in Durchführungsrechtsakten (Implementing Acts) konkretere technische und methodische Anforderungen erlassen, die dann direkt verbindlich werden und dann vor der obigen Liste §30 (2) Vorrang haben. §30 (3)(4) Das Innenministerium kann, falls die Rechtsakte nicht abschließend sind, eigene Konkretisierungen erlassen. §30 (5)

Implementing Act	EU NIS2	NIS2 DE	Gruppe	Status	Roadmap
Cybersecurity Internet	Art. 21 (5) UA 1	§30 (3)	Internet/Digitale	Veröffentlicht	Oktober 2024
Cybersecurity	Art. 21 (5) UA 2	§30 (4)	allgemein	»kann«	unklar
Erhebliche Vorfälle	Art. 23 (11)	§2 (2)	Internet/Digitale	Veröffentlicht	Oktober 2024

Tabelle: *eigene Zusammenstellung, Stand Juni 2024*

↑ UP

Produkte

Zertifizierte Produkte

Verwenden besonders wichtige oder wichtige Einrichtungen bestimmte, noch zu benennende, IKT-Produkte, Dienste oder Prozesse, müssen diese über eine Cybersicherheits-Zertifizierung gem. Art. 49 EU 2019/881 verfügen §30 (6). Welche Produkte, Dienste oder Prozesse betroffen sind, wird noch in der Rechtsverordnung nach §56 (4) bestimmt.

Kritische Komponenten

Der Einsatz sogenannter kritischer Komponenten muss durch Betreiber kritischer Anlagen *vor Beginn des Einsatzes* dem Innenministerium gemeldet werden §41 (1). Kritische Komponenten und Funktionen müssen in separaten Gesetzen festgelegt werden.

Das Innenministerium darf den Einsatz kritischer Komponenten untersagen aufgrund:

- "Beeinträchtigung der öffentlichen Ordnung und Sicherheit" — wenn der Hersteller von der Regierung, staatlichen Stellen oder den Streitkräften eines Drittstaats kontrolliert wird, an "nachteiligen Aktivitäten" gegen die öffentliche Ordnung und Sicherheit Deutschlands, der EU, EFTA oder NATO beteiligt war oder ist, oder wenn der Einsatz nicht mit "sicherheitspolitischen Zielen" Deutschlands, der EU oder der NATO im Einklang ist. §41 (2)
- Fehlender Vertrauenswürdigkeit des Herstellers durch Garantieerklärung, Sicherheitstests und Schwachstellen und Manipulationen in den betreffenden Produkten. §41 (4) (5)

Die kritischen Komponenten dürfen in KRITIS-Anlagen nur mit einer »Garantieerklärung« zur Vertrauenswürdigkeit des Herstellers eingesetzt werden, die von KRITIS-Betreibern dem Innen-

ministerium bei der Anzeige vom Einsatz in KRITIS-Anlagen vorzulegen ist. Die Erklärung muss durch den Hersteller gegenüber dem Betreiber abgegeben werden. §41 (3)

Der Einsatz bestimmter Komponenten oder Hersteller darf bei schwerwiegenden Verstößen auch längerfristig untersagt werden. §41 (6) (7)

↑ UP

Informationen

Registrierung und Kontaktstelle

Einrichtungen und Betreiber müssen sich selbst identifizieren und beim BSI registrieren. Für bestimmte Unternehmen gelten spezielle Registrierungsregeln. §33 §34

- Besonders wichtige und wichtige Einrichtung sowie DNS-Registries müssen sich innerhalb von drei Monaten beim BSI registrieren, u.a: Name, Rechtsform, Kontaktdaten, Mail/Telefon, IP-Adressbereiche, Sektor und Teilsektor, EU-Staaten mit Geschäftsaktivitäten. §33 (1)
- Betreiber kritischer Anlagen müssen zusätzliche Informationen bei der Registrierung übermitteln. §33 (2) Die Registrierung dieser Betreiber wird vom BSI im Einvernehmen mit dem BBK eingerichtet (auch relevant für KRITIS-Dachgesetz). §33 (6)
- Bestimmte Einrichtungen, die in §60 definiert sind, müssen sich innerhalb von drei Monaten beim BSI registrieren. §34 (Cloud, IT, DNS usw. mit Hauptsitz Deutschland)

Änderungen der registrierten Daten in (1) und (2) müssen jährlich an das BSI gemeldet werden, “alle andere Angaben” unverzüglich, innerhalb von zwei Wochen. §33 (5)

Das BSI kann besonders wichtige und wichtige Einrichtung sowie DNS-Registries von sich aus registrieren. Dazu kann das BSI Unterlagen und Einzelheiten anfordern, und das Verfahren noch genauer definieren. §33 (2) (6)

↑ UP

Meldewesen

Mit NIS2 kommen auf betroffene Einrichtungen viele Informations- und Meldepflichten zu, die über die bisherigen §8b BSIG Meldepflichten (KRITIS) hinausgehen.

Meldung von Sicherheitsvorfällen

Besonders wichtige Einrichtungen (damit auch Betreiber kritischer Anlagen) und wichtige Einrichtungen müssen dem BSI Sicherheitsvorfälle melden, in sehr kurzen Fristen (24h) §32

- Erstmeldung bei erheblichen Sicherheitsvorfällen unverzüglich, spätestens innerhalb von 24h
- Folgemeldung über einen erheblichen Sicherheitsvorfall innerhalb von 72h mit Bewertung der Erstmeldung (Schwere, Auswirkungen, Kompromittierung)
- Zwischenmeldungen auf Nachfrage des BSI
- Abschlussmeldung oder Fortschrittsmeldung innerhalb eines Monats mit Beschreibung, Ursachen, Maßnahmen, grenzüberschreitenden Auswirkungen
- Betreiber kritischer Anlagen müssen zusätzlich die Anlagen, kritische Dienstleistung und Auswirkungen melden
- Das BSI informiert zuständige Aufsichtsbehörden des Bundes unverzüglich über eingegangene Meldungen. §32 (5)

Das BSI richtet die Meldemöglichkeit im Einvernehmen mit dem BBK ein, für NIS2 und das KRITIS-Dachgesetz, und kann weitere Vorgaben zum Meldeverfahren erlassen. §32 (4)

Das BSI kann meldenden Unternehmen Unterstützungsangebote machen. §32 (6)

Meldungen an Kunden und Öffentlichkeit

Bei erheblichen Sicherheitsvorfällen kann das BSI besonders wichtige und wichtige Einrichtungen anweisen, ihre Kunden ("Empfänger ihrer Dienste") zu unterrichten. §35 (1)

Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, IKT-Dienste und Digitale Dienste müssen von einer "erheblichen Cyberbedrohung" potenziell betroffene Kunden **unverzüglich** informieren, einschließlich möglicher durch die Kunden zu ergreifenden Gegenmaßnahmen. §35 (2)

Das BSI meldet sich "nach Möglichkeit" innerhalb von 24h bei Unternehmen nach Eingang der Meldung zurück, ggf. mit möglichen Nachfragen, Unterstützungsangeboten und Informationen. §36 (1) Falls eine Sensibilisierung der Öffentlichkeit erforderlich oder im öffentlichen Interesse ist, so kann das BSI die Öffentlichkeit informieren oder Unternehmen dazu auffordern. §36 (2).

↑ UP

Nachweise und Prüfungen

Die Umsetzung der NIS2-Maßnahmen muss dem BSI von Betreibern kritischer Anlagen nach drei Jahren spätestens nachgewiesen und dann alle drei Jahre geprüft werden.

	Betreiber kritischer Anlagen		Einrichtungen	
			Besonders wichtig	Wichtig
Gesetz	NIS2UmsuCG	DachG	NIS2UmsuCG	NIS2UmsuCG
Zeitraum	ab 2025	ab 2026	ab 2025	ab 2025
Pflicht	§39 (1)	§11	§61	§62
Prüfungen	alle drei Jahre	Teil von Audits	Stichproben durch BSI	
Inhalt	IT-Sicherheit Meldepflicht SzA	Resilienz	IT-Sicherheit Meldepflicht	IT-Sicherheit Meldepflicht
Scope	Unternehmen*	Unternehmen*	Unternehmen	Unternehmen
Stichproben	Tiefenprüfung	Nachweisqualität	Risikobasiert	bei Anlass
Empfänger	BSI	BBK	BSI	BSI

Tabelle: *eigene Zusammenstellung nach Referentenentwürfen, Stand Juli 2024*
** - Scope der Prüfungen noch nicht ganz klar*

Betreiber kritischer Anlagen

Die Betreiber von kritischen Anlagen müssen Nachweise für die Umsetzung der Maßnahmen nach §30 (1), §31 (1) und (2) durch "Audits, Prüfungen oder Zertifizierungen" nach §39 (1) spätestens alle drei Jahre dem BSI nachweisen, wie bisher bei KRITIS-Prüfungen.

Für Betreiber, die bereits als KRITIS-Betreiber geprüft werden, wird das BSI "den Zeitpunkt der Nachweiserbringung auf spätestens drei Jahre nach Erbringung des letzten Nachweises nach §8a (3) BSIG" festlegen – der nächste Nachweis verschiebt sich also ggf. um ein Jahr. §39 (3)

Das BSI hat die Befugnis, von sich aus Betreiber kritischer Anlagen als besonders wichtige Einrichtung zu prüfen §61 (5) und kann Vorgaben für Nachweis-Prüfungen festlegen. §39 (2)

Einrichtungen

Alle Einrichtungen müssen die Umsetzung der Maßnahmen dokumentieren. §30 (1)

Einrichtungen müssen dem BSI die Umsetzung der §30 Maßnahmen und §32 Meldepflichten nicht regelmäßig nachweisen, das BSI kann Einrichtungen aber zu "Audits, Prüfungen oder Zertifizierungen" verpflichten und mit Tiefenprüfungen prüfen. §61 (1) (5)

Das BSI darf, analog zu Nachweispflichten bei Betreibern kritischer Anlagen, bei Einrichtungen Nachweise verlangen, frühestens in drei Jahren. §61 (3) Tiefenprüfungen davon unbenommen.

Bei der Auswahl der Einrichtungen soll das BSI risikoorientiert vorgehen, und das "Ausmaß der Risikoexposition, die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von möglichen Sicherheitsvorfällen sowie ihre möglichen gesellschaftlichen und wirtschaftlichen Auswirkungen" in Betracht ziehen. §61 (4)

Das BSI kann Vorgaben für diese Nachweis-Prüfungen festlegen. §61 (2)

↑ UP

Produkte

Konformitätsbewertungen

Das BSI kann in einer Technischen Richtlinie (TR) Anforderungen an IT-Produkte, Dienste und Prozesse definieren (keine Verbraucherprodukte). Für diese Anforderungen kann das BSI eine Konformitätsbewertung vornehmen oder eine Selbstbewertung zulassen. §53

Zertifizierungen

Bestimmte Produkte und Leistungen können durch das BSI zertifiziert werden – als Sicherheits- oder Personenzertifizierungen. Das BSI kann auf Sachverständige zurückgreifen und zertifizieren basierend auf Kriterien oder Schutzprofilen. §52

Sicherheitskennzeichen

Für Verbraucherprodukte führt das BSI ein Sicherheitskennzeichen zur Bewertung und Information der IT-Sicherheit ein. Das BSI definiert Vorgaben (Updates, Schwachstellen etc.) und vergibt das Kennzeichen nach Freigabe. §55

↑ UP

Staat und BSI

Aufsicht und Zuständigkeit

Das BSI ist die zuständige Aufsichtsbehörde für besonders wichtige und wichtige Einrichtungen mit Niederlassung in Deutschland, für Betreiber kritischer Anlagen auf deutschem Hoheitsgebiet und Einrichtungen der Bundesverwaltung. §59

EU-Betreiber

Für bestimmte Einrichtungen, die in der **Europäischen Union** tätig sind und Hauptsitz in Deutschland haben, ist das BSI zentral in der EU zuständig (Territorialitätsprinzip): §60

- DNS-Dienste, Domain Registries und TLD Registries
- Cloud Computing (Provider), Anbieter von Rechenzentren und Content Delivery Networks

- Managed Service und Managed Security Service Provider
- Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke

Die Mitgliedstaat der Hauptniederlassung ist im Gesetz als der Ort definiert, wo: §60 (2)

- Entscheidungen zu »Cybersicherheitsrisikomanagement« vorwiegend getroffen werden
- Cybersicherheitsmanahmen durchgeführt (falls die Entscheidungen ausserhalb der EU getroffen werden)
- die Niederlassung mit der höchsten Beschäftigtenzahl in der EU ist

Bietet ein §60-Unternehmen Dienste in der EU an, hat aber keine Niederlassung in der Union, muss das Unternehmen einen Vertreter benennen, der in der EU niedergelassen ist. §60 (3)

Das BSI muss Amtshilfeersuchen anderer Behörden zu §60-Unternehmen in Deutschland nachkommen und dann Aufsichts- und Durchsetzungsmaßßnahmen einleiten. Dies gilt auch für Einrichtungen, die ihren Hauptsitz analog in der EU haben und dort reguliert werden. §60 (5)

Überwachung

Das BSI hat umfangreiche Aufsichts- und Durchsetzungsmaßnahmen bei Einrichtungen zur Überwachung der NIS2-Compliance. §61 §62

Für besonders wichtige Einrichtungen darf das BSI:

- Einrichtungen zu Prüfungen und Audits verpflichten §61 (1) und für deren Durchführung Vorgaben erlassen §61 (2)
- Nachweise von Einrichtungen zur Umsetzung von Anforderungen verlangen §61 (3) und dabei risikobasierte Auswahlen treffen §61 (4)
- Bei einzelnen Einrichtungen die Einhaltung der Anforderungen überprüfen §61 (5)
- Einrichtungen Anweisungen zur Verhütung oder Behebung von Vorfällen geben §61 (6)
- Einrichtungen *verbindliche* Anweisungen zur Umsetzung der Pflichten geben §61 (7)
- Einrichtungen verpflichten, Kunden über Maßnahmen gegen Cyberbedrohungen zu unterrichten §61 (8)
- Aufsichtsbehörden unterrichten, Genehmigungen aussetzen, und Geschäftsleitungen die Tätigkeit untersagen §63 (9)
- Einrichtungen bei Nicht-Nachkommen von Anforderungen die Zulassung zu entziehen und Geschäftsführung die Leitungsaufgaben untersagen §63 (10)
- und weiteres

Für wichtige Einrichtungen darf das BSI: §62

- Bei gerechtfertigten Tatsachen die Einhaltung von §§30, 32, 38 überprüfen und Maßnahmen nach §61 treffen

Meldestelle

Das BSI ist zentrale Meldestelle für Bundesbehörden §4 und für Einrichtungen. §40 Das BSI darf zur Abwehr von Gefahren Informationen sammeln, auswerten und mit anderen Behörden austauschen.

↑ UP

Sanktionen und Bußgelder

Das NIS2-Umsetzungsgesetz definiert Bußgeldvorschriften in §65. Die KRITIS-Bußgelder werden dabei um neue Tatbestände erweitert und bestehende Bußgelder teils deutlich erhöht.

Geschäftsleitung

Geschäftsleitungen von Einrichtungen müssen die Risikomanagement-Maßnahmen für Cyber-security “umsetzen” und die Umsetzung in der Einrichtung überwachen. §38 (1) Werden diese Pflichten verletzt, ergibt sich aus »allgemeinen Grundsätzen (bspw. §93 AktG)« eine Binnenhaftung der Geschäftsleitung gegenüber der Einrichtung B. Besonderer Teil, zu §38 (2).

Die Einrichtung kann Ersatzansprüche stellen, ein Verzicht oder “ein in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis stehender Vergleich” ist unwirksam. §38 (2)

Geschäftsleiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Bewertung von Risiken und Maßnahmen sicherzustellen. §38 (3) Leiter von Einrichtungen der Bundesverwaltung gelten nicht als Geschäftsleitung.

Tatbestände

Die Bußgeldtatbestände nach §65 (5)-(7) gelten meist für alle Einrichtungs-Gruppen – einzelne Stellen unterscheiden in der Bußgeldbewährung zwischen den Gruppen.

Höhe	Verstöße
10 Mio. EUR *wenn Umsatz größer 500 Mio. Euro: Bußgeldhöhe 2% vom weltweiten Umsatz*	• *Besonders wichtige Einrichtungen:* Anordnung des BSI zur Information von Kunden oder Öffentlichkeit über Sicherheitsvorfall wird zuwidergehandelt. §35 (1) Satz 1 oder §36 (2) Satz • *Besonders wichtige Einrichtungen:* Vorkehrungen zur Cybersicherheit nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen. §30 (1) Satz 1 • *Besonders wichtige Einrichtungen:*Einhaltung der Vorkehrungen nicht, nicht richtig oder nicht vollständig dokumentiert. §30 (1) Satz 3 • *Besonders wichtige Einrichtungen:* Meldungen werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt. §32 (1) Satz 1 • *Besonders wichtige Einrichtungen:* Abschlussmeldungen werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorgelegt. §32 (2) Satz 2 • *Besonders wichtige Einrichtungen:* Mitteilungen (an Kunden oder Öffentlichkeit) werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht. §35 (2) Satz 1,2
7 Mio. EUR *wenn Umsatz größer 500 Mio. Euro: Bußgeldhöhe 1,4% vom weltweiten Umsatz*	• *Wichtige Einrichtungen:* Anordnung des BSI zur Information von Kunden oder Öffentlichkeit über Sicherheitsvorfall wird zuwidergehandelt. §35 (1) Satz 1 oder §36 (2) Satz • *Wichtige Einrichtungen:* Vorkehrungen zur Cybersicherheit nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen. §30 (1) Satz 1 • *Wichtige Einrichtungen:*Einhaltung der Vorkehrungen nicht, nicht richtig oder nicht vollständig dokumentiert. §30 (1) Satz 3 • *Wichtige Einrichtungen:* Meldungen werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt. §32 (1) Satz 1 • *Wichtige Einrichtungen:* Abschlussmeldungen werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorgelegt. §32 (2) Satz 2 • *Wichtige Einrichtungen:* Mitteilungen (an Kunden oder Öffentlichkeit) werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht. §35 (2) Satz 1,2
2 Mio. EUR	• *Hersteller von IT-Systemen:* durch BSI angewiesene Mitwirkung an Wiederherstellung der Sicherheit oder Funktionsfähigkeit eines IT-Systems wird verweigert. §11 (6) • *TK-Anbieter:* durch BSI angewiesene Maßnahmen zur Abwehr konkreter erheblicher Gefahren werden nicht getroffen. §16 (1) Satz 1 auch i.V.m. §16 (3) • *Telemedien:* durch BSI angewiesene Maßnahmen zur Abwehr konkreter erheblicher Gefahren werden nicht getroffen. §17 Satz 1 • *Betreiber kritischer Anlagen:* geeigneter Nachweis über die erfolgte Mängelbeseitigung wird nicht vorgelegt. §39 (1) Satz 5 *Hinweis: Anwendung von §30 (2) 3 OWiG*
1 Mio. EUR	• *Betreiber kritischer Anlagen:* Nachweis über Erfüllung der Anforderungen wird nicht richtig oder nicht vollständig erbracht. §39 (1) Satz 1 i.V.m. VO §56 (4) Satz 1 • *Betreiber kritischer Anlagen:* Nachweis über Erfüllung der Anforderungen wird nicht oder nicht rechtzeitig erbracht. §39 (1) Satz 1 i.V.m. VO §56 (4) Satz 1
500.000 EUR	• *Hersteller von IT-Systemen:* durch BSI angewiesene Mitwirkung an der Beseitigung oder Vermeidung von erheblichen Sicherheitsvorfällen bei IKT-Produkten verweigert. §18 • *Betreiber kritischer Anlagen:* Zuwiderhandlung gegen Anordnung des BSI, zur Bewältigung einer Störung notwendige Informationen inkl. personenbezogenen Daten herauszugegeben. §40 (5) Satz 1 • *Besonders wichtige und wichtige Einrichtungen:* Zuwiderhandlung gegen Anordnung des BSI zur Vorlage von Nachweisen über die Erfüllung von Verpflichtungen. §61 (3) Satz 1, auch i.V.m. §62 • *Besonders wichtige und wichtige Einrichtungen:* Anordnung des BSI zur Umsetzung erforderlicher Maßnahmen nach § 30 (1) Satz 1 inkl. Mängelbeseitigungsplan und Nachweiserbringung wird zuwidergehandelt, oder Frist wird nicht eingehalten. §61 (6) Satz 1 und 3, auch i.V.m. §62 • *Besonders wichtige und wichtige Einrichtungen:* Zuwiderhandlung gegen Anordnung des BSI zur Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen, oder nicht fristgerechte Umsetzung. §61 (7) Satz 1 und 3, auch i.V.m. §62 • *Besonders wichtige und wichtige Einrichtungen:* Anordnung des BSI zur Unterrichtung oder Öffentlichmachung von Informationen wird zuwidergehandelt. §61 (8), auch i.V.m. §62 • Angabe oder Änderung bei Registrierung wird nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt. §33 (1) oder (2) Satz 1 i.V.m. VO nach §56 (4) Satz 1, oder §34 (1)

	• Das BSI wird über Änderungen an Registrierungsdaten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterichtet. §34 (2) • *TLDN-Registries und Domain-Name-Registry-Dienstleister:* Vorgaben oder Verfahren zur Sicherstellung genauer und vollständiger Angaben in Datenbank werden nicht eingehalten oder nicht, nicht in der vorgeschrieben Weise oder nicht rechtzeitig zugänglich gemacht. §49 (3) Satz 1 oder §49 (3) Satz 2 oder (4) • *TLDN-Registries und Domain-Name-Registry-Dienstleister:* Zugang zu den Domain-Namen-Registrierungsdaten wird nicht oder nicht rechtzeitig gewährt. §50 (1) Satz 1 • Nicht-konforme Verwendung eines Zertifikats, einer Erklärung oder eines Kennzeichens nach §52 (2) Satz 4, §53 (1) Satz 4, §54 (6) Satz 2 oder §55 (4) Satz 1 • Tätig als akkreditierte Konformitätsbewertungsstelle ohne Erlaubnis. §53 (3) Satz 2 oder §54 (2) Satz 2 • Vorsätzlicher oder fahrlässiger Verstoß gegen (EU) 2019/881 über ENISA und Zertifizierung: Angaben oder Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig.
100.000 EUR	• Zuwiderhandlung durch Hersteller gegen Anordnung zur Auskunft zu Produkten und Sytemen, insb. auch technischen Details. §14 (2) Satz 1 • Kontaktstelle ist nicht erreichbar. §33 (2) Satz 2 • *Besonders wichtige Einrichtungen:* Betreten eines Raums nicht gestattet oder Aufzeichnung, Schriftstück oder Unterlage nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorgelegt oder Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. §61 (5) Satz 3 • *Betreiber kritischer Anlagen:* Fahrlässig einen Nachweis nicht richtig oder nicht vollständig erbringen. §39 (1) Satz 1

Tabelle: *eigene Zusammenstellung aus NIS2-Referentenentwurf Stand Juli 2024*

↑ UP

Bundeseinrichtungen

Im Sektor Staat sind in der NIS2-Umsetzung Einrichtungen der Bundesverwaltung reguliert. Diese übernehmen die Pflichten besonders wichtiger Einrichtungen und erhalten zusätzlich eigene Pflichten.

In der Bundesverwaltung reguliert werden, sofern es keine expliziten Ausnahmen gibt: §29

- Bundesbehörden
- öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung
- Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, soweit durch BSI angeordnet

Es gibt diverse Ausschlüsse und Abgrenzungen bei Einrichtungen der Bundesverwaltung:

- Geschäftsbereich des Bundesministeriums der Verteidigung
- Geschäftsbereich Auswärtiges Amt
- Nachrichtendienste (BND und BfV)
- Bundesländer sind nicht direkt reguliert

Anforderungen

An Bundeseinrichtungen werden damit folgende Anforderungen an Cybersicherheit gestellt:

- Meldepflichten für Sicherheitsvorfälle nach §31
- Umsetzungs- und Überwachungspflichten nach §38

Bundeseinrichtungen müssen zusätzlich erfüllen:

- Informationssicherheitsmanagement unter Berücksichtigung von IT-Grundschutz bzw. Mindeststandards für die Sicherheit der Informationstechnik des Bundes §43 §44 (1)

Steuerung

Es müssen weiterhin Strukturen auf Bundesebene und bei Einrichtungen geschaffen werden:

- Bundes-CISO: Es soll einen Koordinator für Informationssicherheit auf Bundesebene, gestellt durch die Bundesregierung geben. §48

- ISB von Einrichtungen der Bundesverwaltung ist für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung verantwortlich §45
- ISB der Ressorts initiiert und koordiniert die Fortschreibung von Informationssicherheitsleitlinien für sein oder ihr Ressort §46
- ISB für wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes wegen der zunehmenden Bedeutung und Größe als eigene ISBs §47

Länder und Kommunen

Länder und Kommunen sind in der deutschen NIS2-Umsetzung nicht direkt reguliert – der Gesetzgeber (Bund) verweist auf Zuständigkeit der Länder und dortige Gesetzgebung.

Aus der Definition der normalen Einrichtungen sind explizit öffentliche IT-Dienstleister ausgeschlossen, die sich 100 Prozent im Besitz von Ländern oder Kommunen befinden, keine Dienstleistungen für den Bund erbringen und durch Landesgesetze reguliert werden. §28 (9)

↑ UP

Ausblick

Gesetzgebung

Das NIS2-Umsetzungsgesetz sollte ursprünglich im Oktober 2024 in Kraft treten, das bisherige BSIG dann außer Kraft. Seit Sommer 2023 sind Referentenentwürfe vom NIS2UmsuCG publik. Die Einhaltung der EU-Frist zum Oktober 2024 scheint mittlerweile fraglich, nach Presseberichten aus September 2024 wird nun das erste Quartal 2025 angestrebt.

Version	Status	Datum	Akteur
NIS	Deadline nationale Umsetzung	Mai 2018	Mitgliedstaaten
IT-Sicherheitsgesetz 2.0	Inkrafttreten	Mai 2021	Bundesrat
NIS2	EU 2022/2555 Final	Dez 2022	Amtsblatt
NIS2-Umsetzungsgesetz	Referentenentwurf	Apr 2023	Innenministerium
NIS2-Umsetzungsgesetz	Referentenentwurf	Jul 2023	Innenministerium
NIS2-Umsetzungsgesetz	»Diskussionspapier«	Sep 2023	Innenministerium
NIS2-Umsetzungsgesetz	Referentenentwurf	Dez 2023	Innenministerium
NIS2-Umsetzungsgesetz	Referentenentwurf	Mai 2024	Innenministerium
NIS2-Umsetzungsgesetz	Referentenentwurf	Jun 2024	Innenministerium
NIS2-Umsetzungsgesetz	Beschluss	Jul 2024	Bundeskabinett
NIS2-Umsetzungsgesetz	1. Durchgang, Stellungnahme	Sep 2024	Bundesrat
NIS2-Umsetzungsgesetz	1. Lesung, 20/13184	Okt 2024	Bundestag
EU NIS2	Frist nationale Umsetzung EU	Okt 2024	Mitgliedstaaten
NIS2-Umsetzungsgesetz	2./3. Lesung *plan*	Dez 2024	Bundestag
NIS2-Umsetzungsgesetz	2. Durchgang *plan*	Feb 2025	Bundesrat
NIS2-Umsetzungsgesetz	Inkrafttreten *plan*	Mar 2025	Bundesgesetzblatt
Rechtsverordnung(en)	fehlt noch	unsicher	Innenministerium

Tabelle: *Ablauf NIS2, Stand Oktober 2024, Quelle: Presseberichte*

Evaluierung

In der NIS2-Umsetzung ist **keine Evaluierung** in Deutschland vorgesehen, da EU NIS2 durch die

Europäische Kommission evaluiert werden soll Begründung A. VII. und “eine (auf … Deutschland isolierte) Evaluierung der Umsetzung nicht zielführend” sei. Zu Art. 7

Zusätzlich wird im Umsetzungsgesetz die weitere Evaluierung des IT-Sicherheitsgesetzes 2.0 zum Mai 2025 gestrichen (aufgehoben). Art. 7 Die Evaluierung dieser Vorschriften erübrigen sich, weil “diese in weiten Teilen im Zuge der NIS-2-Umsetzung geändert werden.” Zu Art. 7

Die Ergebnisse der teilweisen Evaluierung des IT-Sicherheitsgesetzes 2.0 flossen in das NIS2-Umsetzungsgesetz wohl ein, so die Begründung.

↑ UP

Auswirkungen

Wirtschaft

In Deutschland geht der Gesetzgeber von etwa 30 Tausend betroffenen Unternehmen aus, von denen nur 17 Prozent “im Grundsatz ausreichende” Maßnahmen ergriffen haben.

- Besonders wichtige Einrichtungen: 8.250 Unternehmen
- Wichtige Einrichtungen: 21.600 Unternehmen

Abzüglich der bestehenden Betreiber haben über 20 Tausend Unternehmen Handlungsbedarf. Dafür berechnet der Entwurf Aufwände für Unternehmen für neue Pflichten und Anpassung von Prozessen: 2,1 Mrd. EUR einmalige Kosten und 2,2 Mrd. EUR jährliche Kosten.

Bundesverwaltung

Bei Bundeseinrichtungen kalkuliert der Gesetzgeber für die Umsetzung der NIS2-Pflichten zusätzliche Aufwände analog zu Unternehmen. Behörden gehen von 1.396 zusätzlichen Stellen aus mit einmaligen Aufwand von 286 Mio. EUR.

Für die Regulierungsbehörden kalkuliert der Gesetzgeber zusätzliche Vollzugsaufwände bei BSI, BBK, BNetzA, BfDI und BMI für NIS2: zusätzliche 931 Stellen und Sachkosten von 73 Mio. jährlich und 36 Mio. EUR einmalig. Begründung A. VI.

↑ UP

Fristen und Umsetzung

Das Gesetz NIS2UmsuCG tritt am Tag nach der Verkündung in Kraft, es sollte eigentlich im Oktober 2024 in Kraft treten. Das bisherige BSI-Gesetz tritt in der alten Fassung dann außer Kraft. Art. 33 (1)

Artikel 30, 31 und 32 treten erst mit einer neuen Rechtsverordnung in Kraft. Artikel 30 betrifft vor allem Definitionen von kritischen Anlagen (KRITIS) und Fristen, die dann aufgehoben und anderswo definiert werden. Die NIS2-Pflichten für Unternehmen (Einrichtungen) gelten ab dann, mit wenigen Fristen. Art. 33 (2)

Es gibt keine Übergangsfristen zur Umsetzung der Pflichten.

Besonders wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1)
- Restliche NIS2-Pflichten nach der Registrierung

Wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1)
- Restliche NIS2-Pflichten nach der Registrierung

Betreiber kritischer Anlagen

- Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1) und §33 (2)
- Restliche NIS2- und KRITIS-Pflichten nach der Registrierung
- Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt: frühestens drei Jahre nach Inkrafttreten des Gesetzes §39 (1), d.h. ab 2027.
- Fortlaufende Nachweise über Maßnahmenumsetzung anschließend alle drei Jahre §39 (1)

↑ UP

Rechtsverordnung

Verschiedene Anforderungen aus dem **NIS2UmsuCG** sollen durch eine oder mehrere Rechtsverordnungen konkretisiert oder definiert werden: §56

- Als kritisch anzusehende Dienstleistungen, deren Versorgungsgrad sowie welche Anlagen oder Teile davon als kritische Anlagen im Sinne des Gesetzes gelten §56 (4)
- Details über die Erteilung von Sicherheitszertifikaten und Anerkennung nach §52 §56 (1)
- Einzelheiten des IT-Sicherheitskennzeichens nach §55, sowie Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und der Freigabe §56 (2)
- Produkte, Dienste oder Prozesse, die von besonders wichtigen oder wichtige Einrichtungen eingesetzt werden, die über eine Zertifizierung §30 (6) verfügen müssen §56 (3)

Die Rechtsverordnung soll im Einklang mit dem KRITIS-Dachgesetz definiert werden und Betreiber und Einrichtungen in einer Verordnung zusammenfassen, damit "betroffene Unternehmen zentral in einer Tabelle" relevante Kategorien und Schwellenwerte finden.

Ein Entwurf der Rechtsverordnung(en) ist noch nicht verfügbar.

Branchenstandards

Besonders wichtige Einrichtungen, d.h. auch Betreiber kritischer Anlagen, können weiterhin branchenspezifische Sicherheitstandards (B3S) zur Umsetzung der §30 (1) Maßnahmen vorschlagen. Das BSI stellt die Eignung der B3S fest. §30 (8)(9)

↑ UP

Auswirkung auf weitere Gesetze

Telekommunikationsgesetz

Das TKG wird mit der NIS2-Umsetzung angepasst, der Referentenentwurf enthält die entsprechenden Änderungen in Artikel 26. Dort sind einige Klarstellungen und Anpassungen des TKG enthalten, ebenso werden die §30 BSIG-E Sicherheitsmaßnahmen aus NIS2 analog in §165 (2a) TKG-E überführt.

Anbieter von TK-Diensten und Netzen müssen damit als NIS2-Einrichtungen über das TKG analoge Maßnahmen umsetzen. Die Änderungen im Gesetz sprechen dafür, ebenso die Begründung zu Aufwänden bei der BNetzA. Dort wird auch der TK-Sicherheitskatalog nicht erwähnt, anscheinend wird es nicht unbedingt einen neuen TK-Sicherheitskatalog geben.

Energiewirtschaftsgesetz

Das EnWG wird mit der NIS2-Umsetzung angepasst, der Entwurf enthält die Änderungen in Artikel 17. Dort ist ein neuer §5c EnWG-E vorgesehen, der Inhalte des bisherigen §11 EnWG entsprechend der NIS2-Vorgaben anpasst. Unter anderem werden die §30 BSIG-E Sicherheitsmaßnahmen aus NIS2 analog in §5c (3) EnWG-E überführt

Die Regulierung für Energiebetreiber bleibt zwischen BSI und BNetzA geteilt: Registrierung und Nachweispflichten vermutlich bei der BNetzA, Meldung von Sicherheitsvorfällen ans BSI. Analog zu den bisherigen IT-Sicherheitskatalogen soll die BNetzA anscheinend zwei aktualisierte (oder neue) IT-Sicherheitskataloge nach §5c (1) bzw. §5c (2) EnWG-E erstellen.

Weitere Gesetze

Gesetz	Änderung	NIS2UmsuCG
BSI-Gesetz	NIS2-Änderungen	Art. 1
BND-Gesetz, SÜFV, TTDSG, GleibWV	Verweise	Art. 2-6
IT-Sicherheitsgesetz 2.0	Evaluierung zum 1. Mai 2025 gestrichen	Art. 7
BSIZertV, BSI-ITSiKV, De-Mail-Gesetz, EGovG, PassDEÜV, PAuswV, KassenSichV, ATG	Verweise	Art. 8-16
EnWG	NIS2-Änderungen	Art. 17
MsbG, EnSiG, WPG, SGB V, DiGAV, SGB VI, BFSGV, SGB XI	Verweise und Definitionen	Art. 18-25
TKG	NIS2-Änderungen	Art. 26
KHSFV, AWV, VDG	NIS2-Änderungen	Art. 27-29
BSIG, TKG, AWV	Definitionen und Anpassungen für KRITIS-DachG	Art. 30-32
NIS2UmsuCG	Inkrafttreten	Art. 33

Tabelle: *Gesetzesänderungen, Stand Oktober 2024*

↑ UP

Änderungen der Referentenentwürfe

Es gab bisher mehrere bekannte Entwürfe von NISUmsuCG seit April 2023:

Juli 2024 (siebter Entwurf, für das Kabinett) zu Juni 2024:

- Weitere Anpassungen Geltungsbereich TK und Energiesektor und Erweiterung TKG und EnWG
- Definitionen betroffener Bundeseinrichtungen präzisiert, Ausschlüsse teils wieder gestrichen
- Avisierte Aufwände und Personal-/Budgetbedarf wurden drastisch reduziert
- Paragraphen umstrukturiert und angepasst
- KRITIS-Sektoren sind nicht mehr im Gesetz definiert, Verweis auf kommende Verordnung

Juni 2024 (sechster Entwurf, nach Verbändeabstimmung) zu Mai 2024:

- Konkretisierung und Einschränkung Geltungsbereich TK und Energiesektor, speziell auch Ausschluss §30 NIS2-Maßnahmen
- Umbenennung Sektoren: IT und TK in Digitale Infrastruktur, Finanz- und Versicherungswesen in Finanzwesen
- Anpassungen Zuständigkeiten Bund
- Anpassungen und Ausblick (KRITIS-Verordnung) zu Zuständigkeiten KRITIS-Anlagen
- Umstrukturierung Paragraphen
- Haftungsregeln und Verantwortung Geschäftsleitung §38 präzisiert

Mai 2024 (fünfter Entwurf, zur Verbändeabstimmung) zu Dezember 2023:

- Definition der Einrichtungen umorganisiert in §28
- Finanzunternehmen sind nun (doch) Einrichtungen §28, aber von allen Pflichten bis auf Registrierung ausgenommen
- Ausschlüsse für öffentliche IT und Cloud Provider umgeschrieben §28
- Ausschlüsse von Pflichten anders gefasst §28 (4)
- Bundeseinrichtungen in §29: berufsständische Körperschaften (öR), Industrie- und Handelskammern (IHK) ausgeschlossen
- Authentizität nun kein Schutzziel mehr bei §30 Maßnahmen
- Neuer Paragraph §55 Konformitätsbewertung
- Bußgeldvorschriften angepasst in Tatbeständen und Höhe
- Pflicht zur Teilnahme am Informationsaustausch für Einrichtung fällt weg
- Erhöhung der Prognose für betroffene Einrichtungen auf 8.250 (besonders wichtig) und 21.600 (wichtig)

Dezember 2023 (vierter Entwurf) zu September 2023:

- Fehlende Paragraphen wieder enthalten
- Zentralregierung nicht mehr als besonders wichtige Einrichtung, dafür mit deren Pflichten
- Ausnahmen für Finanzen und Versicherungen (DORA) gestrafft
- Ausnahme und Überschneidung für EnWG/BNetzA-regulierte Energiebetreiber angepasst
- Frist für bestehende KRITIS-Prüfungen um ein Jahr verlängert
- Ausnahme für Energie-/TK-/Finanzunternehmen von §30 gestrichen (Ausnahmen gelten nun für §§31, 32, 35 und 39)
- Sanktionen gestrafft und Fehler behoben
- Nächste KRITIS-Prüfung um ein Jahr verlängert

September 2023 (dritter Entwurf, Diskussionspapier) zu Juli 2023:

- Harmonisierung der Sektordefinitionen
- Vereinfachung der Unternehmensgrößen und Einrichtungen
- Nachweise bei Betreibern kritischer Anlagen (KRITIS) nur noch alle 3 Jahre, nicht mehr 2
- Keine regelmäßigen Nachweise bei besonders wichtigen und wichtigen Einrichtungen
- Konkrete Anhaltspunkte zur Maßnahmenauswahl: Risiken, Größe, Exposition, Kosten etc.
- Anforderungen an die Sicherheit in der Lieferkette wurden gelockert.
- Weitere Regulierung bestimmter Sektoren ist immer noch nicht geklärt (TK, Energie)
- Aufweichen der Schulungspflichten
- Registrierungspflichten gelockert, teils in Verbindung mit dem KRITIS-Dachgesetz

Juli 2023 (zweiter Entwurf) zu April 2023:

- Weltraum wird analog zum KRITIS-Dachgesetz ein neuer Sektor, Digitale Infrastruktur heißt wieder IT und TK, Bankwesen ist wieder Finanz- und Versicherungswesen.
- Für technische und organisatorische Maßnahmen nach §30 wird neben Verhältnismäßigkeit nun explizit Eignung und Wirksamkeit gefordert.
- Betreiber kritischer Anlagen müssen bei der Angemessenheit von Maßnahmen die aktuellen Lageberichte des BSI zu Bedrohungen für die Versorgungssicherheit berücksichtigen.
- Die Frist für erstmalige Nachweise wurde verlängert auf vier Jahre nach Inkrafttreten.
- Geschäftsleiter besonders wichtiger Einrichtungen im Teilsektor Zentralregierung werden aus der sogenannten »Managerhaftung« ausgeschlossen.
- Die angestrebte Vereinfachung der Regulierung im Energiesektor mit BSI und BNetzA wird (leider) wieder aufgelöst: die bisherige Regulierung soll bestehen bleiben, Maßnahmen zum Risikomanagement und verschärfte Meldepflichten aus dem NIS2UmsuCG sollen stattdessen ins EnWG durchgereicht werden.

April 2023 (erster Entwurf): Erste Version der deutschen NIS2-Umsetzung.

↑ UP

Weitere Informationen

Literatur

1. Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft, Webseite des Bundesamt für Sicherheit in der Informationstechnik, 2024
2. Fragen und Antworten zu NIS-2, FAQs, Webseite des Bundesamt für Sicherheit in der Informationstechnik, 2024
3. NIS-2-Betroffenheitsprüfung, Webseite des Bundesamt für Sicherheit in der Informationstechnik, 2024

Quellen

1. Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie, 20/13184, Gesetzesentwurf Bundesregierung, Bundestag, 02.10.2024
2. Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, Referentenentwurf, Innenministerium, 22.07.2024
3. Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, Referentenentwurf, Innenministerium, 24.06.2024
4. Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, Referentenentwurf, Innenministerium, 07.05.2024
5. Werkstattgespräch– Diskussionspapier, des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-RL, Innenministerium, Intrapol, 26.10.2023
6. Diskussionspapier des Bundesministeriums des Innern und für Heimat - NIS2UmsuCG, dritter Entwurf, AG KRITIS, 27.09.2023
7. Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, AG KRITIS, 3. Juli 2023
8. Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Intrapol, 3. April 2023
9. 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 (NIS2-Richtlinie), 27.12.2022
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 27.12.2022

OpenKRITIS · Das unabhängige Nachschlagewerk für KRITIS-Betreiber und Kritische Infrastrukturen.
53227 Bonn · info@openkritis.de · ISSN 2748-565X

Paul Weissmann ist der Herausgeber von OpenKRITIS und publiziert seit 1999 das PA-RISC-Referenzwerk und Insel Westberlin. OpenKRITIS hat keinen Anspruch auf Vollständigkeit oder Korrektheit und stellt keine Rechtsberatung dar.

Copyright © 2021-2024 · Impressum · Datenschutz · About und Kontakt