ENTWURF EINES GESETZES ZUR UMSETZUNG DER NIS-2-RICHTLINIE

und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Am 23. Juni 2025 hat das BMI einen Referentenentwurf (RefE)[1] des deutschen NIS-2-Umsetzungsgesetzes veröffentlicht, welcher auch die Basis für die Beteiligung der Fachkreise und Verbände dargestellt hat. Die entsprechende Anhörung fand am 4. Juli 2025 statt.

Der neue NIS-2-Referentenentwurf nennt sich „Entwurf eines Gesetzes zur Umsetzung der EU-NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung". Es gibt einige Konkretisierungen und Änderungen im Gesetz, auf die wir hier näher eingehen werden.

Die Vernetzung und enge Verzahnung gerade der Wirtschaft innerhalb Deutschlands und der Europäischen Union resultieren in Interdependenzen bei der Cybersicherheit. Deshalb sind die Cybersicherheitsanforderungen der NIS-2-Richtlinie an juristische und natürliche Personen ausgerichtet, die wesentliche Dienste erbringen oder Tätigkeiten ausüben.

ZIEL DER DEUTSCHEN NIS-2-UMSETZUNG

Entsprechend unionsrechtlicher Vorgaben der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen erweitert.

Die Sicherstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der gesamten EU ist das Ziel der NIS-2-Richtlinie. Das soll durch die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft erreicht werden. Wichtige und besonders wichtige Einrichtungen sollen vor Schäden durch Cyberangriffe geschützt und die Funktionsweise des europäischen Binnenmarktes verbessert werden.

WICHTIGE ÄNDERUNGEN DER DEUTSCHEN NIS-2-UMSETZUNG

In diesem Abschnitt werden einige der konkreten Änderungen und Anpassungen der Vorgaben aus dem RefE vom 23. Juni 2025 aufgezeigt, die eine maßgebliche Rolle für die Umsetzung des deutschen NIS-2-Umsetzungsgesetzes spielen.

Im Anwendungsbereich der deutschen NIS-2-Umsetzung sind Änderungen vorgenommen worden, wie beispielsweise der Geltungsbereich zur Anwendung des Gesetzes und damit auch wer wie stark davon betroffen sein wird. Dazu wurde der § 28 (3) zur Bestimmung der Einrichtungsart neu definiert:

> *„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."*

Des Weiteren können gemäß § 28 (3) bei einer Zuordnung zu den Einrichtungsarten nach Anlage 1 und 2 die Geschäftstätigkeiten unberücksichtigt bleiben, die bezogen auf die gesamte Geschäftstätigkeit der Einrichtung „vernachlässigbar" sind. Wann aber eine Geschäftstätigkeit „vernachlässigbar" sein soll, wird im Gesetzentwurf nicht näher definiert. Eine mögliche Herausforderung hierbei

[1] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE_2025.pdf?__blob=publicationFile&v=8

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

könnte die erhebliche Erweiterung des Geltungsbereiches sein. Aktuell wird dies in den einschlägigen Fachkreisen diskutiert.

Im § 56 (4) und (5) teilweise gestrichen, dass die Wissenschaft, die KRITIS-Betreibende und ihre Verbände angehört werden müssen, wenn Änderungen der KRITIS-Verordnung als auch bei der Rechtsverordnung, wann und warum es sich um einen erheblichen Sicherheitsvorfall handelt, vorgenommen werden. Die „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende" wurden wieder als KRITIS aufgenommen, sie waren zeitweise in den Vorfassungen nicht mehr enthalten.

Die Gesetzesbegründung zu § 5c (2) Energiewirtschaftsgesetz (EnWG) „IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz" wurde um Abschnitte zur Zusammenarbeit von BSI und Bundesnetzagentur (BnetzA) erweitert. Bislang oblag die Aufsicht über KRITIS-Betreibende im Sektor Strom zur Einhaltung von Cybersicherheitsmaßnahmen primär bei der BNetzA. Über die geänderte Einvernehmensregelung bekommt das BSI größeren Einfluss auf die IT-Sicherheitsanforderungen im Sektor Energie. Das BSI kann so ein einheitliches Cybersicherheitsniveau über alle KRITIS-Sektoren sicherstellen. Des Weiteren darf das BSI nach § 11 (4) i. V. m. § 3 (7) KRITIS-Dachgesetz erforderliche Infos zu Sicherheitsvorfällen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) austauschen.

ANWENDUNGSBEREICH

Als besonders wichtige Einrichtungen gelten:

- Betreibende kritischer Anlagen (KRITIS)
- qualifizierte Vertrauensdiensteanbietende
- Top Level Domain Name Registries
- DNS-Dienstanbietende
- Anbietende öffentlich zugänglicher Telekommunikationsdienste
- Betreibende öffentlicher Telekommunikationsnetze, die mindestens 50 Mitarbeitende beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen
- natürliche oder juristische Personen
- rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die entgeltlich Waren oder Dienstleistungen anbieten, in **Anlage 1 bestimmten Einrichtungsarten** zuzuordnen sind, **mindestens 250 Mitarbeitende** beschäftigen oder einen **Jahresumsatz von über 50 Millionen Euro** ausweisen, zudem eine **Jahresbilanzsumme von über 43 Millionen Euro** aufweisen

Ausgenommen sind:

- Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreibende kritischer Anlagen sind

Als wichtige Einrichtungen gelten:

- Vertrauensdiensteanbietende
- Anbietende öffentlich zugänglicher Telekommunikationsdienste
- Betreibende öffentlicher Telekommunikationsnetze, die weniger als 50 Mitarbeitende beschäftigen und einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen
- natürliche oder juristische Personen
- rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, in einer der **Anlagen 1 und 2 bestimmten Einrichtungsarten** zuzuordnen sind und **mindestens 50 Mitarbeitende** beschäftigen oder einen **Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro** aufweisen

Ausgenommen sind:

- besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung

RISIKOMANAGEMENTMASSNAHMEN BESONDERS WICHTIGER EINRICHTUNGEN UND WICHTIGER EINRICHTUNGEN

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind nach § 30 (1) dazu verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen. Diese Maßnahmen dienen dem Ziel, Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für die Erbringung ihrer Dienste verwendet werden, zu verhindern.

Bei der Bewertung der erwähnten Verhältnismäßigkeit der Maßnahmen sind „das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen" zu beachten und die Einhaltung durch die Einrichtungen zu dokumentieren. Die Risikomanagementmaßnahmen sollen den Stand der Technik einhalten, die europäischen und internationalen Normen berücksichtigen und sie müssen auf einem gefahrenübergreifenden Ansatz beruhen.

HISOLUTIONS

AUTOREN

Rozerin Karaterzi
Manuel Atug

HISOLUTIONS

Die Maßnahmen müssen nach § 30 (2) mindestens folgende Punkte umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs wie Back-up-Management und Wiederherstellung nach einem Notfall und Krisenmanagement
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietende oder Diensteanbietende
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 kryptografischen Verfahren
9. Erstellung von Konzepten für die Sicherheit des Personals, 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.

BESONDERE ANFORDERUNGEN AN DIE RISIKOMANAGEMENTMASSNAHMEN VON BETREIBENDEN KRITISCHER ANLAGEN (KRITIS)

Für Betreibende kritischer Anlagen gelten bei informationstechnischen Systemen, Komponenten und Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen entscheidend sind, auch über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 (1) Satz 1 als verhältnismäßig, sofern der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Störung der Anlage steht.

Für die Betreibenden kritischer Anlagen ist weiterhin gemäß § 31 (2) verpflichtend vorgegeben, dass sie Systeme zur Angriffserkennung einsetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen sowie auswerten. Die Systeme zur Angriffserkennung sollten in der Lage sein, Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen festzulegen. Es ist die gesetzliche Vorgabe, dass dabei der Stand der Technik berücksichtigt und eingehalten wird. Der zu diesem Zweck erbrachte Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlagen stehen.

Allgemein gilt für besonders wichtige Einrichtungen und wichtige Einrichtungen:

- § 32 Meldepflicht
- § 33 Registrierungspflicht
- § 35 Unterrichtungspflicht
- § 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

Für Betreibende kritischer Anlagen gilt darüber hinaus:

- § 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibenden kritischer Anlagen
- § 39 Nachweispflichten für Betreibende kritischer Anlagen

WAS SIND DIE UNTERSCHIEDE ZUR CER-RICHTLINIE (KRITIS-DACHGESETZ)?

Grundsätzlich haben die NIS-2-Richtlinie und die CER-Richtlinie klare Überschneidungen, denn beide EU-Richtlinien verpflichten betroffene Einrichtungen dazu, Risikomanagementmaßnahmen zu implementieren. Der wesentliche Unterschied liegt im Anforderungsbereich der beiden Richtlinien. Während die CER-Richtlinie sich auf die allgemeine Resilienz gegenüber **physischen und hybriden Bedrohungen** wie z. B. Sabotage, Terrorismus und Naturereignisse fokussiert, konzentriert sich die NIS-2-Richtlinie auf die Cybersicherheit von **Netz- und Informationssystemen**, um diese vor Cyberbedrohungen zu schützen. Die festgelegten Anforderungen der NIS-2 sind den entsprechenden Verpflichtungen der CER-Richtlinie äquivalent, denn beide Richtlinien ergänzen sich und fordern die EU-Mitgliedstaaten auf, nationale Strategien zur Resilienz der kritischen Einrichtungen zu konzipieren und die Zusammenarbeit auf EU-Ebene zu intensivieren.

„Es ist wichtig, dass die Mitgliedstaaten sicherstellen, dass die Anforderungen nach der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555 komplementär umgesetzt werden und dass kritische Einrichtungen keinem Verwaltungsaufwand ausgesetzt sind, der über das zur Erreichung der Ziele dieser und jener Richtlinie erforderliche Maß hinausgeht."

ErwGr 24 Satz 2 CER-Richtlinie[2]

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557