Aulinger

IT-TRENDS 2025 DIGITAL & SICHER · 10.04.2025

Cybersicherheit im Dornröschenschlaf – Anforderungen und Umsetzung der NIS2-Richtlinie

Dr. Ralf Heine M.M.

Rechtsanwalt · Fachanwalt für Arbeits- und IT-Recht

Agenda

1. Einführung
2. Aktueller Stand der Umsetzung
3. Was gilt bereits jetzt?
4. Handlungsempfehlungen für Unternehmen
5. Fazit

1. Einführung

Die NIS2-Richtlinie - worum geht es?

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)

Die NIS2-Richtlinie - worum geht es?

- rechtliche Maßnahmen zur **Steigerung des Gesamtniveaus der Cybersicherheit** in der EU
- **Erschaffung und Verbesserung** eines **einheitlichen Sicherheitsniveau** in den Mitgliedstaaten der EU
- Grundsatz der **Mindestharmonisierung**

- **Umsetzung** der NIS2-Richtlinie in nationales Recht wahrscheinlich durch **Änderung des BSI-Gesetzes**

- nach Schätzungen fallen ca. **30.000 Unternehmen** deutschlandweit in den Anwendungsbereich der NIS2-Richtlinie
- Unternehmen müssen **angemessene, wirksame und geeignete Risikomanagementmaßnahmen** umsetzen, dokumentieren und regelmäßig überprüfen lassen

2. Aktueller Stand der Umsetzung

Aktueller Stand der Umsetzung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Aktueller Stand der Umsetzung

Aufgrund der vorgezogenen Wahlen konnte das parlamentarische Verfahren zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) nicht abgeschlossen werden. Die Umsetzung der NIS-2 Richtlinie bleibt weiterhin vordringlich.

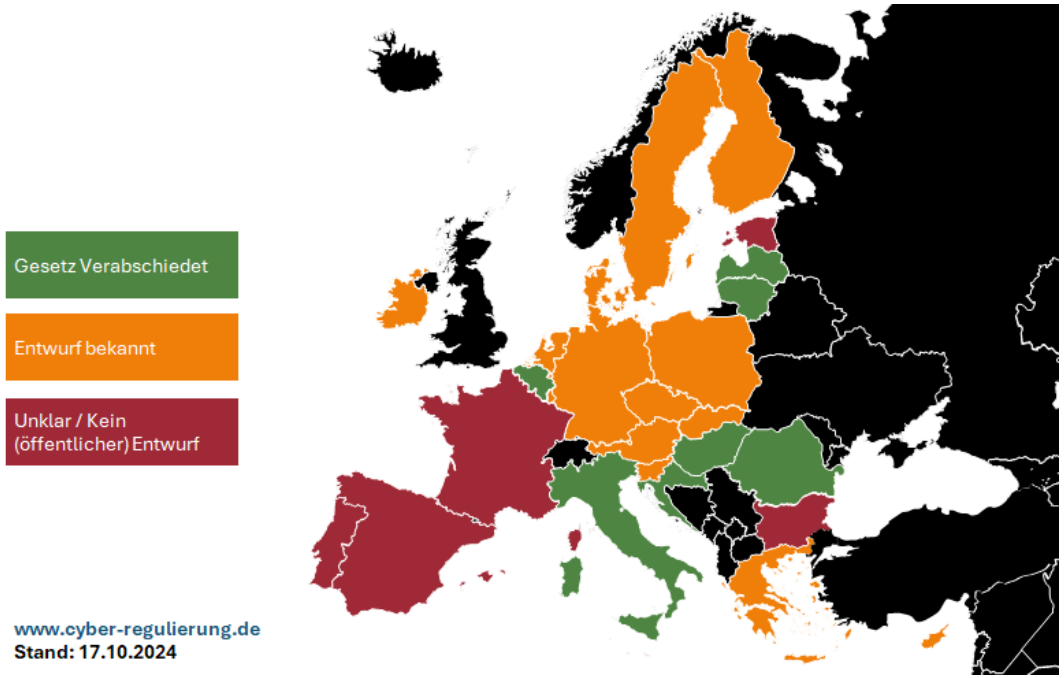
Quelle: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html (Abruf vom 08.04.2025)

Aktueller Stand der Umsetzung

- NIS2UmsuCG konnte wegen der **vorgezogenen Bundestagswahl** nicht mehr verabschiedet werden
- **Diskontinuitätsprinzip** für nicht-verabschiedete Vorlagen greift

- EU hat **Vertragsverletzungsverfahren** gegen Deutschland und weitere 22 EU-Mitgliedsstaaten eingeleitet

Aktueller Stand der Umsetzung



(mögliche) Unmittelbare Wirkung

Eine Richtlinie hat **unmittelbare Wirkung**, wenn:

– ihre Bestimmungen **uneingeschränkt und hinreichend klar und eindeutig** sind und

– wenn der Mitgliedstaat die Richtlinie **nicht fristgerecht umgesetzt** hat

- Aufsichtsmaßnahmen greifen nicht, da Behörden für Eingriffe Rechtsgrundlage brauchen
- Sorgfaltspflichten und Haftungsregelungen für Einrichtungen können u.U. im privatrechtlichen Rechtsverkehr nicht ausgeschlossen werden

3. Was gilt bereits jetzt?

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

- Cybersicherheit nicht nur für Kritische Infrastrukturen, sondern **flächendeckend als allgemeine Compliance-Anforderung** für die Wirtschaft
- NIS2-Richtlinie grundsätzlich anwendbar auf **öffentliche und private Einrichtungen**, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben – mit Ausnahmen und Einschränkungen für den öffentlichen Bereich
- **qualitative** (Anhang I und Anhang II) sowie **quantitative Konkretisierung** der betroffenen Unternehmen
- Mitgliedstaaten erstellen bis zum 17.04.2025 eine Liste wesentlicher und wichtiger Einrichtungen, die Domänennamen-Registrierungsdienste erbringen

- **Grundsatz der Mindestharmonisierung**

Was gilt bereits jetzt?

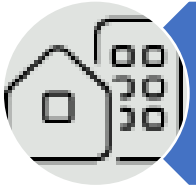
Inhalt der NIS2-Richtlinie

Bisherige KRITIS-Unternehmen

Diese Unternehmen müssen bestimmte Schwellenwerte überschreiten, um als KRITIS-Betreiber eingestuft zu werden. Ein typischer Schwellenwert ist die Versorgung von mindestens 500.000 Einwohnern.

Wesentliche Einrichtungen

Großunternehmen mit mehr als 250 Mitarbeitern fallen in diese Kategorie. Ebenso gehören Unternehmen mit einem Jahresumsatz von mindestens 50 Millionen Euro dazu. Auch Unternehmen mit einer Bilanz von mindestens 43 Millionen Euro fallen darunter.



Wichtige Einrichtungen

Mittlere Unternehmen mit mehr als 50 Mitarbeitern werden als wichtige Einrichtungen betrachtet. Ebenso gehören Unternehmen mit einem Jahresumsatz von mindestens 10 Millionen Euro in diese Kategorie. Auch Unternehmen mit einer Bilanz von mindestens 10 Millionen Euro fallen darunter.

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

Quelle: www.netplans.de/it-security/nis2/ (Abruf am 08.04.2025)

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Was gilt bereits jetzt?

Meldung von Sicherheitsvorfällen

- **Wesentliche und wichtige Einrichtungen** sowie Betreiber kritischer Anlagen müssen **erhebliche Sicherheitsvorfälle** der zuständigen Aufsichtsbehörde melden
    - **Erhebliche Sicherheitsvorfälle** sind z.B. schwerwiegende Betriebsstörungen, führen zu finanziellen Verlusten oder Schäden für Dritte

- **Meldefristen**: unverzüglich, in jeden Fall aber 24 h für die Erstmeldung sowie 72 h für eine Folgemeldung; abschließend 30 Tage für Abschlussmeldung/Folgemeldung

- Meldung beinhaltet eine Bewertung des Vorfalls inkl. Schweregrad, Auswirkungen, Kompromittierungsindikatoren sowie Kontaktinformationen

4. Handlungsempfehlungen

Handlungsempfehlungen

NIS2-“Kontaktstelle“

Quelle: BSI #nis2know

Einrichtung einer Kontaktstelle ist für wesentliche und wichtige Einrichtungen nach Auffassung des BSI sehr empfehlenswert, um den Meldepflichten nachzukommen. Die Kontaktstelle nimmt Informationen der Aufsichtsbehörde auf und gibt sie intern weiter. Die Kontaktstelle gewährleistet die bidirektionale Kommunikation mit der Aufsichtsbehörde.

Handlungsempfehlungen

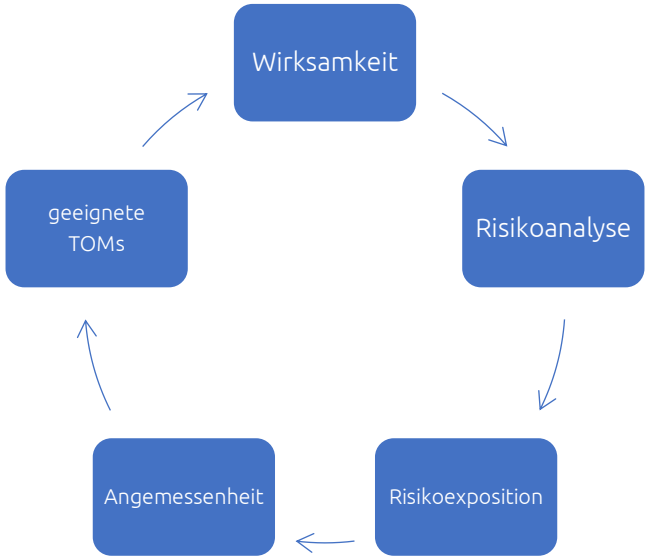
NIS2-“Kontaktstelle“

<u>Empfehlungen des BSI an die Kontaktstelle:</u>

- Kontaktstelle ist ein **Funktionspostfach**, das 24/7 (technisch) ausgelesen wird
- **telefonische** Erreichbarkeit im Falle einer **Meldung** empfehlenswert
- Kontaktstelle kann sowohl **intern als auch extern**, beispielsweise durch einen Dienstleister, besetzt
- werden
- Kontaktstelle kann auch **Rolle oder Gruppe**, wie etwa ein Security Operations Center (SOC) sein
- Für die Kontaktstelle sollten **zwei Personen** benannt werden: Hauptansprechperson / organisatorische Ansprechperson

Handlungsempfehlungen

Risikoanalyse



Handlungsempfehlungen

Risikomanagementmaßnahmen

- **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung von Sicherheitsvorfällen**
- Aufrechterhaltung und Wiederherstellung, **Backup-Management**, Krisen-Management
- **Sicherheit der Lieferkette**
- Sicherheit in der **Entwicklung, Beschaffung und Wartung**
- **Management von Schwachstellen**
- Bewertung der Effektivität von **Cybersicherheit und Risiko-Managementmaßnahmen**
- **Schulungen Cybersicherheit und Cyberhygiene**
- **Einsatz von Kryptografie und Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und Management von Anlagen
- **Multi-Faktor-Authentifizierung**
- gesicherte **Sprach- Video und Textkommunikation** sowie gesicherte **Notfallkommunikationssysteme**

5. Fazit

To-Do‘s zur Umsetzung

1. Ermittlung der Betroffenheit
2. Klärung der Verantwortlichkeiten
3. Risikoanalyse
4. Umsetzung der Maßnahmen
5. Kontinuierliche Prüfung

To-Do‘s zur Umsetzung

1. Es fehlt eine abschließende Konkretisierung der Maßnahmen durch EU, BSI oder Verbände

2. Ebenso sind noch keine offizielle Ableitungen auf existierende Cybersecurity Standards wie ISO 27001 oder C5 verfügbar, welche die Maßnahmen in Rahmenwerke einordnen

3. Wahrscheinlich sind existierende ISMS-Zertifizierungen nicht ohne weiteres schon hinreichend für NIS2-Maßnahmen – der Geltungsbereich (Scope) von NIS2 könnte über bestehende Zertifikate hinausgehen, die genannten Maßnahmen sind teils tiefer und teils weiter als übliche Rahmenwerke.

Vielen Dank.

Dr. Ralf Heine M.M.

Rechtsanwalt | Partner

Tel. +49 201 9598648

ralf.heine@aulinger.eu

Qualifikation

- mehr als 15 Jahre Berufserfahrung in den Bereichen Arbeitsrecht, IT- und Datenschutzrecht
- Fachanwalt für Arbeitsrecht und Informationstechnologierecht
- zert. Datenschutzauditor- und beauftragter
- gelistet als einer der „**Best Lawyers Germany – IT-Recht**“ 2024

Tätigkeitsschwerpunkte

- Rechtssichere und risikominimierende Gestaltung von IT-Verträgen sowie Nutzungsbedingungen
- Geltendmachung von und Verteidigung gegen Schadensersatzansprüche im IT-Bereich
- Verhandlungen von Datenschutzverträgen
- Erstellung der erforderlichen Datenschutzdokumentationen
- Führen von Auseinandersetzung mit Datenschutz-Aufsichtsbehörden in einem datenschutzrechtlichen Kontroll- oder Bußgeldverfahren

Aulinger

Ihr Ansprechpartner

Dr. Ralf Heine M.M.
Rechtsanwalt | Partner
Fachanwalt für Arbeits- und IT-Recht

+49 201 9598648
+49 201 9598699
ralf.heine@aulinger.eu

Aulinger Bochum
Josef-Neuberger-Straße 4
44787 Bochum

Aulinger Essen
Frankenstraße 348
45133 Essen