Cyberresilienz

NIS-2-Richtlinie

05.03.2025 - Dr. jur. Timo Bittner

SCON

Neue rechtliche Anforderungen im Bereich der Cyberresilienz

NIS-2

Was Sie wissen müssen…

Anforderungen, Pflichten und Umsetzungsempfehlungen

Wer ist S-CON?

- Sitz an der Podbielskistraße in Hannover
- Beratungserfahrung seit Jahrzehnten
- 35 angestellte Mitarbeiter – Juristen, Anwälte, Informatiker, IT-Forensiker und viele andere spezialisierte Berater und Auditoren
- Beratungsbereiche:
  - Datenschutz
  - Informationssicherheit und Cyberresilienz
  - IT-Sicherheit
  - Compliance
  - Whistleblowing / Hinweisgebersystem
  - Lieferkettenmanagement
  - Sanktionslisten-Screening
  - Qualitätsmanagement
  - Akademie

Was uns besonders macht:

- Synergien nutzen – alles aus einer Hand!
- Mittels **ISO 9001 Zertifikat** bestätigte Beratungsqualität
- Vorbildliche Sicherheit über **ISO 27001 Zertifikat**
- Feste Ansprechpartner mit Redundanz
- Einsparung von eigenen Ressourcen und Ausbildungskosten
- Hohe Flexibilität, Erreichbarkeit und Servicegedanke
- Hohe Versicherung (10 Mio. Euro) für theoretische Schäden aus Fehlberatungen
- Einbringen neuer Impulse durch gleichgelagerte Projekte
- Deutliche Vorteile im Zusammenhang mit Zertifizierungsaudits
- Vollständige Beratungsleistung in englischer Sprache bei Bedarf möglich
- Viel Erfahrung im Umgang mit behördlichen Prüfungen
- **… und unsere Philosophie.**

410 Mandanten

- Unternehmen jeder Größe: Kleinstunternehmen bis hin zu Konzernen mit 5.000 Mitarbeitern
- Öffentliche Einrichtungen
- Schwerpunkte liegen im Mittelstand
- Weitere Schwerpunkte:
  - Stadtwerke und Energieversorger
  - produzierendes Gewerbe und Chemiebranche
  - Immobilienbranche und Wohnungswirtschaft
  - soziale Einrichtungen
  - diakonische Einrichtungen
  - IT- und Dienstleistungsbranche
  - Consultingbranche
  - uvm. von der Eventagentur über die Nahverkehrsgesellschaft bis zu Versicherungsunternehmen

Übersicht über die Historie des IT-Sicherheitsrechts

IT- und Informationssicherheitsrecht gewinnt seit vielen Jahren an Bedeutung…

IT-Sicherheitsgesetz 1.0 – 2015

BSI-KRITIS-VERORDNUNG 1.0 – 2016

NIS-Richtlinie – 2016

NIS-Umsetzungsgesetz – 2017

Änderung der BSI-KRITIS-VERORDNUNG – 2017

IT-Sicherheitsgesetz 2.0 – 2019

BSI-KRITIS-VERORDNUNG 1.5 – 2021

NIS-2-Richtlinie – 2023

CER-Richtlinie – 2023

Und es wird weitergehen…

KRITIS-DachG – 2025

NIS2UmsuCG – 2025

Weitere VERORDNUNGEN – 2025/26

Rechtliche Grundlagen und Zweck von NIS-2 (1)

- Die Abkürzung **NIS-2** steht wortwörtlich für: **"Network and Information Systems Directive 2**„ = "Richtlinie über Netz- und Informationssicherheit 2„.

- Dies ist die überarbeitete Version der ursprünglichen **NIS-Richtlinie** (2016), die in der EU Mindestanforderungen für die Cybersicherheit kritischer und wesentlicher Infrastrukturen festlegt.

- Auf der NIS-Richtlinie basiert die **Cyberresilienz** und bestimmt **Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen** in der EU.

- Cyberresilienz bezeichnet hierbei die Fähigkeit einer Organisation, Cyberangriffe und andere digitale Bedrohungen zu überstehen, sich davon zu erholen und kontinuierlich weiterzuarbeiten.

Rechtliche Grundlagen und Zweck von NIS-2 (2)

- **Ziel von NIS-2 ist:**
  - der unionsweite **Aufbau von Cybersicherheitskapazitäten**,
  - die **Eindämmung von Bedrohungen** für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden,
  - und die **Sicherstellung der Kontinuität** solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen.

- Demnach liegt ein **legitimer und nachvollziehbarer Zweck** vor.

- Das Handeln der EU-Legislative hätte verhindert werden können, wenn die Wirtschaft initiativ ausreichende Maßnahmen zum Schutz ergriffen hätte. Dies ist aber leider nicht eingetreten.

Umsetzung in deutsches Recht

- Sekundäres EU-Recht in der Form von Richtlinien muss immer (noch) **in nationales Recht** umgesetzt werden.
- Die NIS-2 entfaltet **keine direkte Wirkung** auf die Wirtschaft. Strittig ist dies für Einrichtungen des öffentlichen Rechts.
- Zur Umsetzung der Richtlinie in deutsches Recht gibt es bereits mehrere Entwürfe. Bis zum **17.10.2024 hätte das deutsche Gesetz in Kraft treten müssen**. Hierbei ist der deutsche Gesetzgeber offensichtlich im Verzug. Der Inhalt steht aber bereits weitestgehend durch die NIS-2 fest.
- Abzuwarten bleibt, wann das Gesetz tatsächlich verabschiedet wird.

Klare Tendenzen

- NIS2-2 und die deutschen Gesetzesentwürfe zielen jedoch alle in eine sich verschärfende Richtung ab.
- Dem entspricht auch der letzte Entwurf für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz:

Deutscher Bundestag **Drucksache 20/13184**

20. Wahlperiode 02.10.2024

Gesetzentwurf

der Bundesregierung

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

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Wer ist von NIS-2 betroffen? (1)

- **Energie:** Elektrizität, Fernwärme, Erdöl, Erdgas und Wasserstoff
- **Transport:** Luft, Schiene, Wasser, Straße, ÖPNV, Post- und Kurierdienste
- **Finanzwesen:** Bankwesen und Finanzmarktinfrastrukturen und Handelsplätze
- **Gesundheit:** Gesundheitsdienstleister, EU-Referenzlabore, Medizinforschung, Pharmazeutik und Medizinprodukthersteller
- **Wasser:** Trinkwasserversorgung und Abwasserbeseitigung
- **Digitale Infrastruktur:** Betreiber von Internet Exchange Points, DNS-Dienstanbieter, Top Level Domain Name Registry, Anbieter von Cloud-Computing-Diensten oder Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Vertrauensdienstanbieter, Betreiber öffentlicher Telekommunikationsnetze, Anbieter öffentlich zugänglicher Telekommunikationsdienste, Managed Services Provider, Managed Security Services Provider,
- **Raumfahrt:** Bodeninfrastruktur
- **Abfallwirtschaft:** Abfallbewirtschaftung
- **Chemie:** Produktion, Herstellung und Handel mit chemischen Stoffen
- **Lebensmittel:** Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- **Verarbeitendes Gewerbe:** Herstellung von Medizinprodukten und In-vitro-Diagnostika, Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, Herstellung von elektrischen Ausrüstungen, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen sowie sonstiger Fahrzeugbau
- **Digitale Dienste:** Anbieter von Online-Marktplätzen, Anbieter von Online-Suchmaschinen und Anbieter von Plattformen für Dienste sozialer Netzwerke
- **Forschung:** Forschungseinrichtungen
- **Öffentliche Verwaltung:** Zentralregierung

Wer ist von NIS-2 betroffen? (2)

- Neben der Sektorzugehörigkeit gibt es noch weitere Kriterien:
  - **Mitarbeiterzahl** – 250 / 50
  - **Umsatz / Bilanzsumme** 50 / 43 Mio. Euro oder 10 / 10 Mio. Euro
- Daraus resultiert, ob eine Einrichtung als eine besonders wichtige, wichtige oder eine nicht betroffene Einrichtung definiert ist.
- Insbesondere die Prüfung der Betroffenheit für **verbundene Unternehmen und KRITIS** ist ein weiterer wichtiger Schritt.

Was fordert NIS-2?

- Besonders wichtige und wichtige Einrichtungen müssen 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 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.

Risikomanagement

- Die Umsetzung gestaltet sich nach einem risikobasierenden Ansatz.
- Ein Risikomanagement muss in dokumentierter Form vorliegen, Risiken ermitteln sowie Eintrittswahrscheinlichkeiten und Schadenshöhen definieren.
- Die danach zu treffenden Maßnahmen sollten sich immer an dem Stand der Technik orientieren:

"Stand der Technik" bezeichnet den aktuellen Entwicklungsstand von Technologien, Methoden und Verfahren, die sich in der Praxis bewährt haben und als effizient sowie sicher gelten.

Anforderungskatalog aus § 30 Abs. 2 NIS2UmsuCG

- Die 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.

Leitfaden zur Umsetzung

- Schritt 1: Bestandsaufnahme und Risikoanalyse
- Schritt 2: Ermittlung des Schutzbedarfs
- Schritt 3: GAP-Analyse
- Schritt 4: Umsetzung der Anforderung gem. § 30 Abs. 2 NIS2UmsuCG
- Schritt 5: Aufrechterhaltung und kontinuierliche Verbesserung

Meldepflicht gegenüber der Behörde – Art. 23 NIS-2

- **Sicherheitsvorfälle** sind an die zukünftig zuständige Behörde zu melden.
  - **a) Erstmeldung** innerhalb von **24 Stunden** nach Kenntnisnahme des erheblichen Sicherheitsvorfalls (**Frühwarnung**),
  - **b) Zweitmeldung** innerhalb von **72 Stunden** nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, (**Aktualisierung der Erstmeldung** und eine **erste Bewertung** des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren) und
  - **c) Drittmeldung** spätestens **einen Monat** nach Übermittlung der Meldung des Sicherheitsvorfalls (**Abschlussbericht**).
  - **d) Zwischenberichte** auf Nachfrage

Meldepflicht gegenüber Kunden u. Ä. – Art. 23 NIS-2

- Potenziell von einer erheblichen Cyberbedrohung betroffene **Kunden sind unverzüglich zu informieren, über:**
  - **die Cyberbedrohung selbst und**
  - **Maßnahmen und Abhilfemaßnahmen**, die der Kunde ergreifen kann

Was ist ein erheblicher Sicherheitsvorfall?

Ein Sicherheitsvorfall gilt als erheblich, wenn:

a) dieser schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;

b) dieser andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Sicherheitsvorfall – Art. 23 NIS-2

Potenziell von einer erheblichen Cyberbedrohung betroffene **Kunden sind unverzüglich zu informieren, über:**

- **die Cyberbedrohung selbst und**
- **Maßnahmen und Abhilfemaßnahmen**, die der Kunde ergreifen kann

Nachweispflicht

Das zuständige Bundesamt kann die Vorlage von Nachweisen über die Erfüllung einzelner oder aller genannten Verpflichtungen anordnen.

Registrierungspflicht

Von NIS-2 betroffene Einrichtungen sind verpflichtet, spätestens drei Monate, nachdem sie erstmals oder erneut unter NIS-2 fallen, sich bei dem zuständigen Bundesamt registrieren zu lassen.

Bußgeldsanktionen

- Die angedrohten Bußgelder sollen gemäß EU Richtlinie wirksam, verhältnismäßig und abschreckend sein.
- Das deutsche Gesetz bringt weitere Verschärfungen mit sich und muss diese konkretisieren.
- Die deutschen Gesetzesentwürfe sehen **Bußgelder bis zu 10 Millionen Euro oder 2% des weltweit erzielten Jahresumsatzes** vor.
- Hierbei sind klare Analogien zur DSGVO erkennbar.

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

- Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.
- Verstoßen Geschäftsleitungen gegen diese Pflichten, haften diese ihrer Einrichtung gegenüber für einen schuldhaft verursachten Schaden.
- Die Geschäftsleitungen müssen regelmäßig an einschlägigen Schulungen teilnehmen und auch Ihre Mitarbeiter schulen lassen.

ISO 27001 Zertifikat als Lösung

Ein ISO 27001 Zertifikat ist die beste Möglichkeit, um den Nachweis der Umsetzung von NIS-2 zu erbringen, weil die Norm ein etabliertes, international anerkanntes Rahmenwerk für Informationssicherheitsmanagement ist.

Sie deckt alle wesentlichen Sicherheitsanforderungen ab, darunter Risikomanagement, Sicherheitsmaßnahmen und kontinuierliche Verbesserung, die auch NIS-2 fordert.

Unternehmen, die ISO 27001 implementieren, haben bereits klare Prozesse zur Risikobewertung, Incident Response und Dokumentation – zentrale Elemente der NIS-2-Umsetzung.

Zudem erleichtert die Zertifizierung den Nachweis der Einhaltung gegenüber Behörden, minimiert Haftungsrisiken und verschafft Vorteile bei dem Abschluss einer Cyberversicherung.

Angebot von S-CON - Alleinstellungsmerkmale

Das Angebot von **S-CON** beinhaltet ein „**Rund-um-sorglos-Paket“** zur Umsetzung der rechtlichen und organisatorischen Schritte.

Dieses umfasst:

- Stellung eines **Informationssicherheitsbeauftragten (ISB)**
- Beratung und Unterstützung sowie Entlastung von Aufgaben (z. B. **Aufbau eines Risikomanagements**, Prozessdokumentation, Erstellen von Richtlinien, Abgleich mit den Anforderungen aus Standards (**ISO 27001 / BSI-Grundschutz / B3S / TISAX, oder anderen Standards**)
- Aufbau eines **BCM** und Erstellung eines **Notfallkonzepts**
- **E-Learning / Live-Schulungen** online oder vor Ort sowie **digitale Awareness-Kampagnen**
- **(stetiges) IT-PEN-TESTING**, Sicherheitsmonitoring und **Phishing-Simulationen**
- **24/7-Unterstützung** bei der Meldung von Sicherheitsvorfällen
- Software für ein **Sanktionslisten-Screening**
- Software zur **Lieferantenabfrage und Lieferantenbewertung**

Zeit für Ihre Fragen.

Ich freue mich auf Ihren Besuch in meinem Workshop oder Ihre Kontaktaufnahme.

S-CON GmbH & Co. KG

Dr. jur. Timo Bittner LL.M. LL.M.

Mobil: 0170 9649193

E-Mail: Timo.Bittner@s-con.de