GPP-Blickpunkt #UPDATE

NIS-2 Relaunch: Aktuelle Entwicklungen und Handlungsbedarf für Unternehmen und Behörden

1. Wer ist betroffen?

Ist Ihr Unternehmen auf die neuen gesetzlichen Vorgaben vorbereitet? Mit dem NIS-2-Umsetzungsgesetz, das im Dezember 2025 in Kraft getreten ist, verschärfen sich die Anforderungen deutlich. Betroffen sind nicht nur Betreiber kritischer Infrastrukturen (KRITIS), sondern auch zahlreiche weitere Einrichtungen aus unterschiedlichen Sektoren – insgesamt rund 29.500 Unternehmen in Deutschland.

„NIS-2 macht Cybersicherheit zur Chefsache – mit neuen Pflichten und harten Konsequenzen."

Andrej Ditler
IT-Prüfer bei GPP

Unternehmen gelten als „besonders wichtige Einrichtungen" (bwE) oder „wichtige Einrichtungen" (wE), wenn sie in relevanten Bereichen wie Energie, Telekommunikation, Gesundheitsversorgung, Transport, aber auch in der Versicherungswirtschaft oder als digitale Energiedienstleister tätig sind. Maßgeblich ist dabei in der Regel eine Unternehmensgröße von mindestens 50 Mitarbeitenden oder ein Jahresumsatz bzw. eine Bilanzsumme von über 10 Millionen Euro.

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist? Mit unserer kurzen Betroffenheitsanalyse können Sie das hier schnell und einfach herausfinden.

! Eine Ausnahme bildet die sogenannte **Vernachlässigbarkeitsklausel**: Tätigkeiten, die nur in völlig untergeordneter Form im betroffenen Bereich ausgeübt werden, können

**Sehr geehrte Mandantinnen,
sehr geehrte Mandanten,
sehr geehrte Fachinteressierte,**

nachdem wir bereits in unserem GPP-Blickpunkt vom 15. Oktober 2024 über das Regelwerk für die Netzwerk- und Informationssicherheit in der zweiten Fassung (NIS-2) informiert haben, möchten wir mit diesem GPP-Blickpunkt ein Update geben.

Die Europäische Union (EU) hat mit der NIS-2 die Richtlinienkompetenz zum Schutz kritischer Infrastrukturen auf einen größeren Kreis von Unternehmen, die von der Richtlinie betroffen sind, erweitert.

Ziel der Richtline ist es, den wachsenden, schwerwiegenden Cyber-/Informationssicherheitsrisiken für Organisationen umfassend zu begegnen.

Hierfür wurde mit der NIS-2-Richtlinie das Rahmenwerk um ein umfassendes Meldewesen ergänzt und die Verantwortung der Einhaltung der zu ergreifenden Maßnahmen an die gesetzlichen Vertreter und die Geschäftsführung adressiert.

Als Wirtschaftsprüfungs- und Beratungsgesellschaft, die sich auf die Kommunalwirtschaft spezialisiert hat, möchten wir diese Gelegenheit nutzen, um Sie in diesem GPP-Blickpunkt über die jetzt notwendigen Maßnahmen zu informieren.

Wir wünschen Ihnen eine aufschlussreiche Lektüre und hoffen, Ihnen hiermit einen übersichtlichen Einstieg in das Thema zu verschaffen.

Bremen, 30. Januar 2026

Bernd Tameling-Meyer
Wirtschaftsprüfer
Steuerberater

Carsten Hartung
IT-Auditor IDW

unter bestimmten Bedingungen von den Pflichten ausgenommen sein. Neu ist zudem eine Registrierungspflicht beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Außerdem müssen Sicherheitsvorfälle in einem gestuften Verfahren gemeldet werden – mit einer ersten Meldung innerhalb von 24 Stunden.

Besonders ernst sollten Geschäftsleitungen die neuen Vorgaben nehmen: Sie sind künftig persönlich in der Pflicht, für die Einhaltung der Sicherheitsmaßnahmen zu sorgen. Bei Verstößen drohen empfindliche Bußgelder von bis zu 20 Millionen Euro bzw. 2 % des weltweiten Jahresumsatzes (für bwE) sowie bis zu 10 Millionen Euro bzw. 1,4 % Umsatz (für wE).

Um Unternehmen und Behörden bei der Klärung ihrer Betroffenheit zu unterstützen, haben wir eine Betroffenheitsprüfung entwickelt. Damit können Sie schnell und präzise feststellen, ob Ihr Unternehmen den neuen Pflichten unterliegt. Unser Ziel ist es, Ihnen frühzeitig Klarheit zu verschaffen und Sie bei der Umsetzung wirksamer Cybersicherheitsmaßnahmen zu begleiten.

2. Meldepflichten und Sanktionen

Eine zentrale Fragestellung ist, wann Sie im Fall eines Sicherheitsvorfalls die Behörde informieren müssen, denn mit NIS-2 werden die Anforderungen verschärft.

> *Nach NIS-2 haften Geschäftsleitungen von wichtigen und besonders wichtigen Einrichtungen für die Umsetzung und Überwachung der Risikomanagementmaßnahmen.*

Thomas Lissowski
IT-Prüfer bei GPP

Im Meldewesen nach NIS-2 dreht sich alles um Sicherheitsvorfälle, welche Dienste schwerwiegend gestört, finanzielle Verluste verursacht oder Personen durch Schäden beeinträchtigt haben. Ebenfalls gilt dies, wenn diese Möglichkeiten noch eintreten könnten.

Für wichtige und besonders wichtige Einrichtungen gilt: Maximal 24 Stunden nach Kenntnisnahme eines Sicherheitsvorfalls muss eine Erstmeldung erfolgen. Diese soll unter anderem Ihre Einschätzung enthalten, ob der Vorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.

Spätestens 72 Stunden nach Kenntnisnahme ist ein Update zur Erstmeldung abzugeben, um die Informationen aus der Erstmeldung zu bestätigen oder zu korrigieren sowie eine erste Bewertung des Sicherheitsvorfalls abzugeben.

Dauert der Sicherheitsvorfall nicht mehr an, muss innerhalb eines Monats nach dem Update der Erstmeldung eine Abschlussmeldung über Schweregrad, Auswirkung, Beschreibung und Ursache des Vorfalls abgegeben werden. Ferner muss genannt werden, welche Maßnahmen bereits getroffen wurden oder noch anhalten. Dauert der Sicherheitsvorfall noch an, muss stattdessen eine Fortschrittsmeldung abgegeben werden. Die Abschlussmeldung muss in diesem Fall nach abgeschlossener Bearbeitung des Sicherheitsvorfalls eingereicht werden.

Betreiber kritischer Anlagen (ehemals KRITIS-Betreiber) müssen bei Sicherheitsvorfällen prüfen, ob diese Auswirkungen auf ihre Anlagen haben oder haben könnten. In diesem Fall sind Meldungen über die Art der Anlage, die betroffene kritische Dienstleistung und deren Auswirkungen erforderlich.

Darüber hinaus können seitens der Behörden Zwischenmeldungen über relevante Statusaktualisierungen verlangt werden. Details zum Meldeverfahren und der geforderten Inhalte werden auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) veröffentlicht.

Die möglichen Strafen für Verstöße gegen die NIS-2 sind gravierend: Unternehmen können mit Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes belegt werden, wobei der höhere Betrag fällig wird. Ein Compliance-Verstoß könnte also erhebliche finanzielle Schäden und Imageverluste bedeuten.

Nach NIS-2 haften Geschäftsleitungen von wichtigen und besonders wichtigen Einrichtungen für die Umsetzung und

Überwachung der Risikomanagementmaßnahmen für Cybersecurity nach dem NIS-2-Umsetzungsgesetz.

Sollte diese Pflicht verletzt werden, haftet die Geschäftsleitung persönlich für die verursachten Schäden gegenüber der Einrichtung.

3. Bausteine der NIS-2-Richtlinie

Die NIS-2-Richtlinie fordert von Organisationen eine klare Struktur im Bereich der Cybersicherheit.

Im Gegensatz zu bisherigen Vorgaben wird nun ein noch stärkerer Fokus auf die regelmäßige Überprüfung der IT-Sicherheitsmaßnahmen gelegt.

Dominik Giourtzakis
IT-Prüfer bei GPP

Die wichtigsten Bausteine der NIS-2-Richtlinie umfassen Maßnahmen zum Risikomanagement, zur Behandlung von Sicherheitsvorfällen und zur Sicherstellung der Business-kontinuität. Im Gegensatz zu bisherigen Vorgaben wird nun ein noch stärkerer Fokus auf die regelmäßige Überprüfung der IT-Sicherheitsmaßnahmen gelegt. Es müssen technische und organisatorische Maßnahmen dafür sorgen, dass die kritische IT und Dienstleistungen vor wesentlichen Störungen geschützt werden. Hierbei wird der Geltungsbereich im Vergleich zu früheren Regelungen deutlich erweitert.

Wichtige Aspekte der Richtlinie sind zudem der gezielte Einsatz von Verschlüsselung und sicheren Kommunikationskanälen sowie die Durchführung von Schulungen zur Informationssicherheit. Diese Maßnahmen helfen, sowohl interne als auch externe Sicherheitsrisiken zu minimieren.

Nach unserer Einschätzung sind Unternehmen gut beraten, ihre bestehenden Sicherheitsmaßnahmen kritisch zu überprüfen, um den gestiegenen Anforderungen der NIS-2-Richtlinie gerecht zu werden. Der neue risikobasierte Ansatz der Richtlinie erfordert, dass Unternehmen ihre Sicherheitsstrategien regelmäßig evaluieren und anpassen. Dies ist entscheidend, um Sanktionen zu vermeiden und eine robuste Sicherheitskultur zu etablieren.

4. Wirksame Maßnahmen zum Schutz

Die NIS-2-Richtlinie erfordert umfassende Sicherheitsmaßnahmen, von der Einführung eines ISMS über technische und organisatorische Vorkehrungen bis hin zur kontinuierlichen Überwachung und Optimierung.

Mit NIS-2 kommen viele neue Anforderungen auf Sie zu, doch wir sind uns sicher, dass Sie diese mit den richtigen Maßnahmen stemmen können!

Tizian Stemmer
IT-Prüfer bei GPP

Hierfür empfehlen wir Ihnen zunächst, mindestens zwei Personen innerhalb Ihres Unternehmens zu benennen, welche die Verantwortung für die Koordination der Informationssicherheit nach der Richtlinie übernehmen. Ebenfalls sollte eine erste Bestandsaufnahme Ihrer Informationssicherheit erfolgen. Für die Umsetzung der Sicherheitsstandards nach der NIS-2-Richtlinie ist die Einführung eines Informationssicherheitsmanagementsystems (ISMS) unerlässlich, um die bestehenden Standards zu verbessern. Dies umfasst regelmäßige Risikobewertungen zur Identifizierung potenzieller Bedrohungen.

Im nächsten Schritt sollten sowohl technische Maßnahmen, wie die Implementierung von Firewalls und Intrusion Detection Systemen als auch organisatorische Maßnahmen, wie Zugangskontrollen und Schulungen für MitarbeiterInnen, umgesetzt werden.

Beziehen Sie auch Ihre IT-Lieferkette einschließlich unmittelbarer Zulieferer aktiv in Ihre Sicherheitskonzepte ein. Bei unmittelbaren Zulieferern handelt es sich um Anbieter, die direkt IT-Dienste, Software oder andere digitale Leistungen für Ihr Unternehmen bereitstellen. Mit diesen Zulieferern sollten Sicherheitsanforderungen vertraglich festgelegt werden. So stellen Sie sicher, dass auch externe Partner nachweislich zur Sicherheit

Ihrer Systeme beitragen. Regelmäßige Bewertungen und gemeinsame Notfallübungen stellen sicher, dass auch externe Partner im Ernstfall vorbereitet sind.

Ein weiterer wesentlicher Aspekt ist die Überwachung und das Incident Management. Implementieren Sie Systeme zur kontinuierlichen Überwachung und Protokollierung sicherheitsrelevanter Ereignisse. Zudem sollten Prozesse zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen entwickelt und getestet werden. Diese Maßnahmen müssen den aktuellen technischen Standards entsprechen und Konzepte zur Risikoanalyse, zur Sicherheitsvorfallbewältigung sowie zur Betriebskontinuität und zum Krisenmanagement umfassen.

! **Dokumentieren Sie alle umgesetzten Sicherheitsmaßnahmen lückenlos, um im Falle einer BSI-Prüfung den Nachweis über die Erfüllung Ihrer Pflichten erbringen zu können.**

Die interne und externe Kommunikation ist ebenfalls von großer Bedeutung. Stellen Sie sicher, dass alle Mitarbeitenden über die Sicherheitsrichtlinien und -verfahren informiert sind und diese verstehen. Etablieren Sie zudem Kommunikationskanäle zu relevanten Behörden und Partnern, um im Falle eines Sicherheitsvorfalls schnell und effektiv reagieren zu können. Auch Stellvertretungsregelungen sollten eindeutig definiert und formalisiert werden.

Abschließend sind regelmäßige Überprüfungen und Verbesserungen der Sicherheitsmaßnahmen unerlässlich. Dies beinhaltet Sicherheitsaudits und Penetrationstests, um die Wirksamkeit der implementierten Maßnahmen zu überprüfen. Nutzen Sie die Ergebnisse dieser Überprüfungen, um die Sicherheitsvorkehrungen kontinuierlich zu optimieren. Die NIS-2-Richtlinie ist flexibel formuliert, sodass Unternehmen angemessene Maßnahmen entsprechend ihrer Risikolage und Infrastruktur ergreifen können. Diese werden anhand von Kriterien wie Gefährdungslage, Unternehmensgröße, Kosten und Auswirkungen definiert.

5. Was muss jetzt getan werden?

Der Bundestag hat das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsucG) am 13. November 2025 beschlossen. Das Gesetz ist am 6. Dezember 2025 in Kraft getreten. **Daraus ergibt sich eine formaljuristische Pflicht für betroffene Unternehmen sich bis zum 6. März 2026 bei der verantwortlichen Behörde BSI** (Bundesamt für Sicherheit in der Informationstechnik) **zu registrieren. Es gibt keine weitere Schonfrist!** Es ergeben sich für betroffene Unternehmen unmittelbar folgende Handlungsnotwendigkeiten: !

1. **Betroffenheitsüberprüfung**
   Führen Sie die oben genannte Betroffenheitsprüfung durch!

2. **IT-Compliance Berichterstattung**
   Diskutieren Sie mit den Verantwortlichen die Ergebnisse der Betroffenheitsüberprüfung und starten Sie eine IT-Compliance-Berichterstattung zu wesentlichen IT-Prozessen, -Dienstleistungen und betroffenen Lieferketten.

3. **Security-Awareness-Programm**
   Entwickeln Sie eine Strategie zum Umgang mit einem IT-Sicherheitsvorfall. Schulen Sie Ihre Mitarbeitenden im sicheren Umgang mit IT-Systemen.

4. **FIT-GAP-Analyse**
   Identifizieren Sie im Rahmen einer Lückenanalyse die kritischen Prozesse, die für die Bereitstellung Ihrer wesentlichen Dienste verantwortlich sind und stellen Sie fest, ob Ihre bisherigen angewandten Cyber-Sicherheitsmaßnahmen ausreichend sowie wirksam sind und die NIS-2 Anforderungen erfüllen.

Unternehmen und Organisation haben keine weiteren Übergangsfristen. Die Maßnahmen zur Umsetzung müssen umgehend erfolgen. Der Beginn dieser Maßnahmen und der Projektplan müssen bei einer Überprüfung nachgewiesen werden. **Gerne begleiten wir Sie im Rahmen von Informationsvermittlung und Beratungsdienstleistungen zu Ihrer IT-Compliance auf dem Weg zur Erfüllung Ihrer NIS-2 Anforderung.**

Für Rückfragen und einen konstruktiven Austausch zu der Thematik stehen wir Ihnen gerne zur Verfügung! Nehmen Sie hierzu gerne an unserem kostenfreien Webinar teil:

Webinar

NIS-2-Richtlinie verstehen und umsetzen

26. Februar 2026

10.00 Uhr bis 12.00 Uhr

Die neue NIS-2-Richtlinie und das Umsetzungsgesetz stellen Unternehmen vor umfangreiche Pflichten – von Risikomanagement über Governance bis hin zu Haftungsfragen für Leitungsorgane. In unserem Webinar zeigen wir, worauf es jetzt wirklich ankommt.

Erfahren Sie kompakt und praxisnah:

- Welche Anforderungen NIS-2 an Ihr Unternehmen stellt.
- Wie Sie Prozesse, IT-Sicherheit und Compliance effizient ausrichten.
- Welche Bußgelder und Haftungsrisiken drohen – und wie Sie diese vermeiden.
- Welche Schritte Sie jetzt für eine revisionssichere Umsetzung einleiten sollten.

Für weiterführende Informationen und zur Anmeldung bitte hier klicken.

Göken, Pollak, Partner
Treuhandgesellschaft mbH

Schwachhauser Heerstraße 67
28211 Bremen
Tel. 0421 35048-200
bremen@gpp-treuhand.de

Beyerstraße 25
09113 Chemnitz
Tel. 0371 43100-0
chemnitz@gpp-treuhand.de

Lütticher Straße 132
40547 Düsseldorf
Tel 0211 5381993-0
duesseldorf@gpp-treuhand.de

Hansestraße 37
20144 Hamburg
Tel. 0421 35048-200
hamburg@gpp-treuhand.de

Alte Gärtnerei 1
55128 Mainz
Tel. 06131 231832
mainz@gpp-treuhand.de

Maxfeldstraße 9
90409 Nürnberg
Tel. 0911 217959-70
nuernberg@gpp-treuhand.de

Humboldtstraße 2
14467 Potsdam
Tel. 0331 743826-0
potsdam@gpp-treuhand.de

Keesburgstraße 36a
97074 Würzburg
Tel. 0931 99161-997
wuerzburg@gpp-treuhand.de