audatis®
Datenschutz und Informationssicherheit | CONSULTING

EU-weite Cybersicherheit:

Umsetzung der NIS-2-Richtlinie in Deutschland

Inhalt

Zeitliche Übersicht

27.12.2022: Die NIS-2-Richtlinie wird im Amtsblatt der EU veröffentlicht. Das Ziel ist es, die Cyberresilienz der Einrichtungen und der Unternehmen zu stärken und somit einen einheitlichen Sicherheitsstandard für die Cyber- und Informationssicherheit in der EU zu schaffen. Die wichtigste Änderung zum vorherigen Gesetz: die Zielgruppe wurde massiv erweitert.

Semptember 2023: Der aktuellste Stand der deutschen Umsetzung wurde veröffentlicht. Es wurden einige Abschwächungen der Richtlinie vorgenommen und es ist davon auszugehen, dass sich dieser Entwurf von dem finalen Gesetz nicht viel unterscheiden wird.

März 2024: Der endgültige deutsche Gesetzesentwurf soll vorgestellt werden. Hierbei ist es wichtig zu beachten, dass betroffene Unternehmen nach Veröffentlichung der deutsche NIS-2-Umsetzung nur noch sechs Monate Zeit haben, um die Maßnahmen umzusetzen.

17.10.2024: Das NIS-2-Gesetz tritt in Kraft. Es ist keine Übergangsfrist für die betroffenen Unternehmen vorgesehen und die Regelungen gelten damit umgehend.

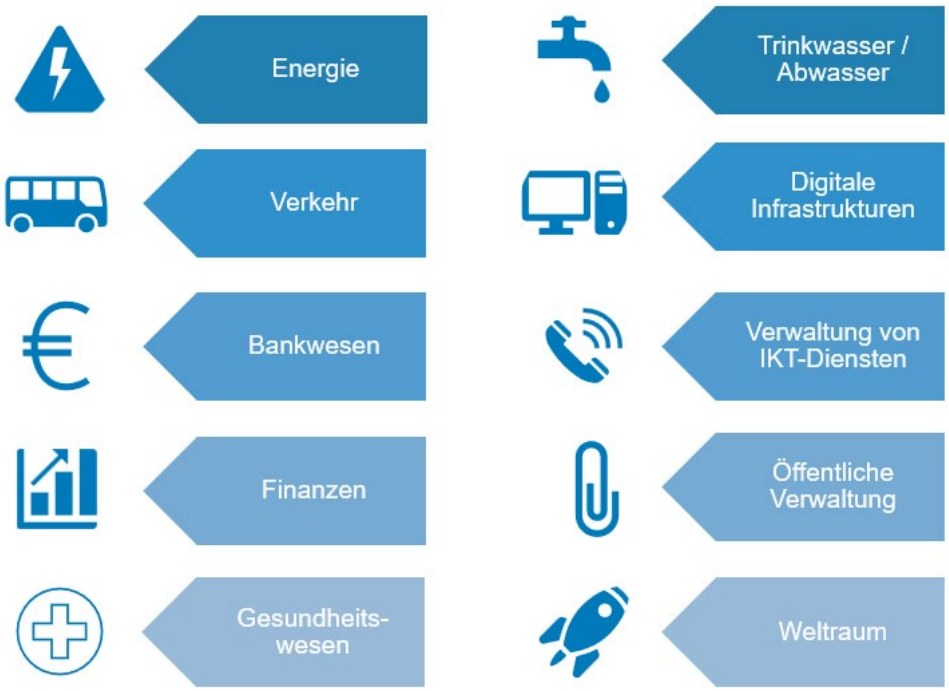
Wer ist von NIS-2 betroffen?

Von NIS-2 ist betroffen, wer zwei Kriterien erfüllt. Für die Erfüllung des ersten Kriteriums muss das Unternehmen in eine der drei folgenden Gruppen fallen:

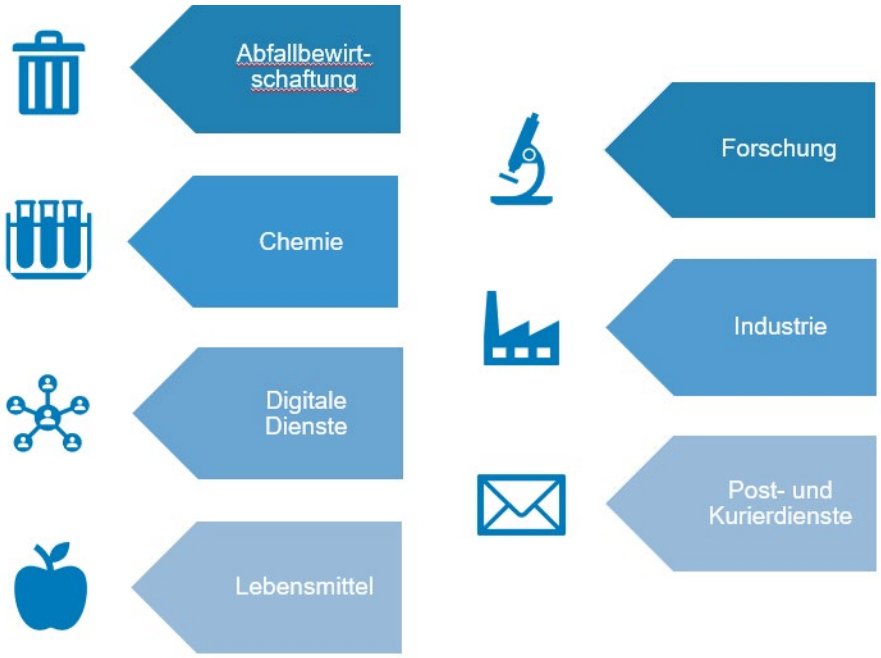
- KRITIS-Betreiber (die Einrichtung versorgt über 500.000 Personen)
- Besonders wichtige Einrichtungen (das Unternehmen hat über 250 Mitarbeiter ODER einen Umsatz von mehr als 50 Mio. €)
- Wichtige Einrichtungen (das Unternehmen hat über 50 Mitarbeiter ODER über 10 Mio. € Umsatz)

Zusätzlich zum ersten Kriterium muss die Einrichtung noch in einem der folgenden beiden Sektoren angesiedelt sein:

Besonders wichtige Sektoren:



Wichtige Sektoren:



Es können jedoch auch Unternehmen von der NIS-2-Richtlinie betroffen sein, die nicht unter die genannten Kriterien fallen (bspw. wichtige IT-Dienstleister eines besonders wichtigen Unternehmens)

Nachweise und Überwachungen

- KRITIS Betreiber müssen die Umsetzung der NIS-2-Richtlinie alle drei Jahre nachweisen
- Dies gilt nicht für besonders wichtige und wichtige Unternehmen
  - ➔ Müssen dem BSI aber ebenfalls Sicherheitsvorfälle melden
  - ➔ Besonders wichtige Einrichtungen können Anweisungen vom BSI erhalten und können auch zu Audits verpflichtet werden
- Betroffene Unternehmen müssen sich selbst als solche identifizieren und beim BSI registrieren
  - ➔ Ab dem 17.10.2024 haben die Unternehmen drei Monate Zeit, um sich zu registrieren
- Besonders wichtige Unternehmen müssen zusätzlich an einem Informationsaustausch teilnehmen (nach Inkrafttreten der NIS-2-Regel müssen sich die Unternehmen innerhalb eines Jahres auf der Austauschplattform des BSI anmelden)

Fristen der Meldepflicht und Strafmaße

Folgende Fristen gelten bei Sicherheitsvorfällen:

- Erstmeldung erheblicher Sicherheitsvorfälle innerhalb von 24 Stunden
- Innerhalb von 72 Stunden muss eine Bewertung der Erstmeldung erfolgen. Hierzu gehören die Schwere des Sicherheitsvorfalls, die Auswirkungen und die Kompromittierung.
- Nach vier Wochen muss eine Abschlussmeldung übermittelt werden. In dieser muss der Vorfall beschrieben und die Ursachen, die getroffenen Maßnahmen und die Auswirkungen genannt werden.
- Auf Nachfragen des BSI müssen Zwischenmeldungen erfolgen.
- Bei schweren Sicherheitsvorfällen muss zusätzlich eine Meldung an die Kunden erfolgen.
- KRITIS Betreiber müssen zusätzlich die betroffene Anlage, die kritische Dienstleistung und die Auswirkungen melden.

Bei den Strafmaßen wird zwischen den besonders wichtigen und den wichtigen Unternehmen unterschieden. Falls beispielsweise Vorkehrungen zur Cybersicherheit nicht rechtzeitig getroffen wurden oder Meldungen nicht übermittelt wurden, können besonders wichtige Unternehmen mit einer Strafe bis zu 10 Mio. € oder 2% des weltweiten Jahresumsatzes belegt werden, während wichtige Einrichtungen bis zu 7 Mio. € oder 1,4% des weltweiten Jahresumsatzes zahlen müssten.
Für den Fall, dass Unternehmen sich gar nicht oder verspätet registrieren oder dem BSI verlangte Informationen nicht preisgeben, drohen sowohl den besonders wichtigen als auch den wichtigen Einrichtungen eine Geldstrafe von 500.000 €.

Maßnahmen Checkliste

Folgende Maßnahmen sollten Sie in Ihrem Unternehmen umgesetzt haben, um gut auf die NIS-2-Richtlinie vorbereitet zu sein:

- ☐ Schulungen der Mitarbeiter (zum Thema Cybersicherheit), z.B. durch Awareness-Trainings und Phishing-Kampagnen
- ☐ Backup-Management, um beispielsweise auf Ransomware Angriffe reagieren zu können
- ☐ Regelmäßig erprobtes Notfall- und Krisenmanagement
- ☐ Risikoanalyse / Sicherheitskonzepte für Informationssysteme
- ☐ Schutz der Daten vor unerlaubtem Lesen durch Nutzung von Kryptographie und Verschlüsselung
- ☐ Sicherheit der Kommunikation
- ☐ Zugriffsmanagement nach dem Need-to-know und Least-privilege Prinzip
- ☐ Sicherheitsmaßnahmen in der Lieferkette, um unter anderem Ausfälle zu vermeiden
- ☐ Business Continuity Management (Sicherstellung, dass der Betrieb des Unternehmens auch bei unplanmäßigen Vorfällen wie einem Wasserschaden, einem Feuer oder ähnlichem weiterläuft)
- ☐ Bewältigung von Sicherheitsvorfällen

Empfehlungen von audatis

Man sollte sich auf jeden Fall rechtzeitig mit dem Thema auseinandersetzen, da es nur noch sechs Monate bis zur Veröffentlichung der Richtlinie sind

1. Identifikation, ob das eigene Unternehmen betroffen ist, gefolgt von der Registrierung beim BSI
2. Was ist vorhanden? Sind bereits ein ISMS oder sogar Zertifizierungen wie die ISO 27001 vorhanden? Ein ISMS würde nämlich eine solide Basis schaffen und bereits viele Anforderungen der NIS-2-Richtlinie abdecken.
3. An welchen Punkten sollte nachgebessert werden? Hierfür sollte das Unternehmen einer Analyse unterzogen werden, um festzustellen, an welchen Stellen nachgebessert oder vielleicht auch überhaupt erstmal angesetzt werden muss.
4. Zum Schluss sollte man sich damit beschäftigen, ob gewisse Punkte aus 3. bereits firmenintern bearbeitet werden können und an welchen Stellen Hilfe von außerhalb nötig ist.

Bei jedem dieser Punkte können wir Sie unterstützen. Seien es nur ein paar Stellschrauben, an denen noch nachgebessert werden muss oder die Etablierung eines ISMS, zögern Sie nicht uns anzusprechen!

Kontakt

Sascha Knicker

Senior Consultant Informationssicherheit

Fon: 05221 87292-07 | Fax: 05221 87292-49
E-Mail: s.knicker@audatis.de

audatis CONSULTING GmbH

Luisenstraße 1 | 32052 Herford
Fon: 05221 87292-0 | Fax: 05221 87292-49
E-Mail: info@audatis.de
www.audatis.de