NIS-2 Richtlinie

Das ändert sich für Unternehmen!

PSW GROUP

Was ist NIS2?

- NIS2 ist eine aktualisierte und ergänzte Version der bestehenden Regelungen der EU-Richtlinie für Cybersicherheit NIS von 2016.
- NIS2 definiert dabei Mindeststandards um eine einheitliche und effektive Sicherheitsstruktur zu erreichen.
- Alle 27 EU-Mitgliedsstaaten müssen die NIS2-Richtlinie bis Oktober 2024 in ihre nationalen Gesetze aufnehmen.

PSW GROUP

NIS2 - Das Ziel

Grundsatz der Mindestharmonisierung

Höheres Sicherheitsniveau für kritische Infrastrukturen

NIS2 - Wer ist betroffen?

Sektoren mit hoher Kritikalität (festgelegt in Anhang I)

Energie:

- **Elektrizität**, einschließlich Erzeuger-, Verteiler- und Übertragungsnetze sowie Ladepunkte;
- **Fernwärme und -kälte**;
- **Öl**, einschließlich Produktion, Lager und Fernleitungen;
- **Gas**, einschließlich Versorgungs-, Verteiler- und Fernleitungsnetze und Speicheranlagen sowie
- **Wasserstoff**.

• **Verkehr**, Luftverkehr, Schienenverkehr, Schifffahrt und Straßenverkehr.

• **Bankwesen und Finanzmarktinfrastruktur** wie Kreditinstitute, Betreiber von Handelsplätzen und zentrale Gegenparteien.

• **Gesundheitswesen**, einschließlich Gesundheitsdienstleister, Einrichtungen, die pharmazeutische Erzeugnisse oder kritische Medizinprodukte herstellen, und EU-Referenzlaboratorien.

• **Trinkwasser**

PSW GROUP

NIS2 - Wer ist betroffen?

Sektoren mit hoher Kritikalität (festgelegt in Anhang I)

- **Abwasser**
- **Digitale Infrastruktur**, einschließlich Anbieter von Rechenzentrumsdiensten, Cloud-Computing-Diensten, öffentlicher elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste.
- **Verwaltung von IKT-Diensten** (Business-to-Business)
- **Weltraum**
- **Öffentliche Verwaltung** von Zentralregierungen und auf regionaler Ebene, ausgenommen Justiz, Parlamente und Zentralbanken. Dies gilt nicht für Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausgeübt werden.
- **Post- und Kurierdienste**
- **Abfallbewirtschaftung**

NIS2 - Wer ist betroffen?

Sonstige kritische Sektoren (festgelegt in Anhang II)

- **Chemische Stoffe:** Produktion, Herstellung und Handel
- **Lebensmittel:** Produktion, Verarbeitung und Vertrieb
- **Verarbeitendes Gewerbe/Herstellung von Waren**, insbesondere von Medizinprodukten, Datenverarbeitungsgeräten, elektronischen und optischen Geräten, bestimmter elektrischer Ausrüstung sowie Maschinen, Kraftwagen und sonstiger Fahrzeugbau;
- **Anbieter digitaler Dienste**, wie Online-Marktplätzen, Suchmaschinen und sozialen Netzwerken sowie
- **Forschungseinrichtungen**

NIS2 - Wer ist betroffen?

- **Mittelständischen Unternehmen** mit einer Größe von 50 - 250 Mitarbeitern und einem jährlichen Umsatz von 10-50 Mio. EUR bzw. einer Bilanzsumme von bis zu 43 Mio. EUR
- **Großunternehmen** ab einer Größe von 250 Mitarbeitern mit einem Umsatz ≥ 50 Mio . EUR / einer Bilanzsumme ab 43 Mio. EUR.

ACHTUNG **Unabhängig von der Größe der Einrichtungen gilt die Richtlinie auch für Einrichtungen der Sektoren aus Anhang I oder II, wenn**

a) die Dienste erbracht werden von:

i) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

ii) Vertrauensdiensteanbietern;

iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;

PSW GROUP

NIS2 - Wer ist betroffen?

b) es sich bei der Einrichtung in einem Mitgliedstaat um den **einzigen Anbieter eines Dienstes** handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;

c) sich eine **Störung** des von der Einrichtung erbrachten Dienstes **wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte**;

d) eine **Störung** des von der Einrichtung erbrachten Dienstes zu einem **wesentlichen Systemrisiko** führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

e) die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist;

NIS2 - Wer ist betroffen?

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

i) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung der Zentralregierung ist oder

ii) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung auf regionaler Ebene ist, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

NIS2 – Was ist zu tun?

Die konkret umzusetzenden Mindestanforderungen sind im Kapitel 4, in Artikel 20 und 21 der NIS2-Richtlinie geregelt:

Artikel 20

Governance

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Artikel 23

Berichtspflichten

Artikel 20 - Governance

(1) Die Leitungsorgane wesentlicher und wichtiger Einrichtungen sind zur Einhaltung der im Artikel 21 beschriebenen **Risikomanagementmaßnahmen** verpflichtet. Sie müssen ihre Umsetzung überwachen und können für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden.

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

(2) Die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen **an Schulungen teilnehmen**. Zudem müssen allen **Mitarbeitern regelmäßig** entsprechende **Schulungen** angeboten werden, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Artikel 21 - Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
- Incident Management: Bewältigung von Sicherheitsvorfällen
- Business Continuity: wie Backup-Management, Disaster Recovery, Krisen-Management
- Sicherheit in der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

  => Ausweitung der Anforderungen auf andere Branchen und auch kleinere Unternehmen möglich
- Sicherheit bei Beschaffung (Erwerb, Entwicklung und Wartung von Netz und IT-Systemen)
- Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Cyberhygiene und Schulungen im Bereich der Cybersicherheit

Artikel 21 - Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- Vorgaben für Kryptographie und Verschlüsselung
- Sicherheit des Personals
- Zugangskontrolle
- Asset-Management
- Multi-Faktor-Authentifizierung und SSO
- Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- Einsatz gesicherter Notfall-Kommunikations-Systeme

PSW GROUP

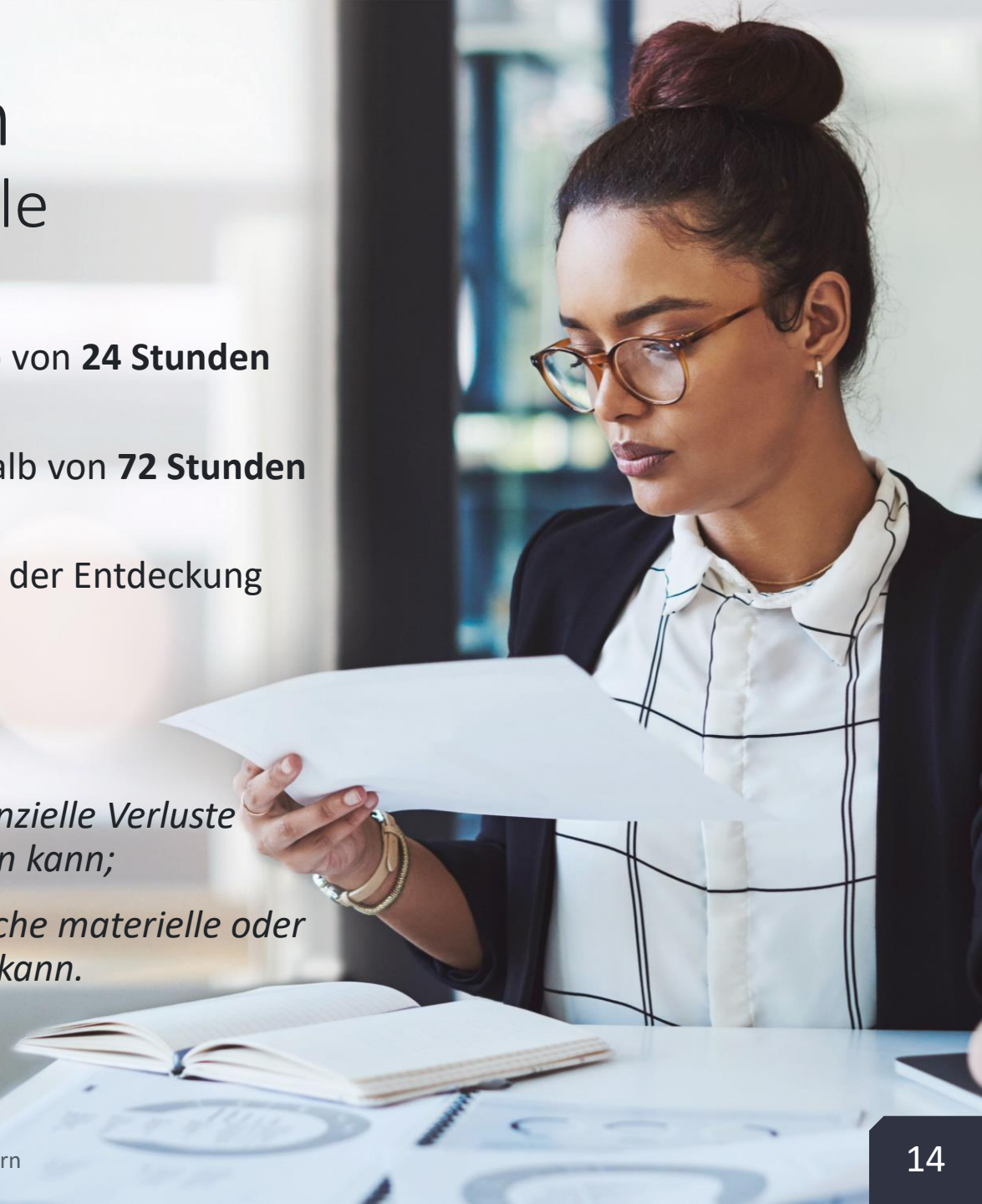
Artikel 23 – Berichtspflichten
Strengere Meldepflichten für Vorfälle

- **Erstmeldung** eines erheblichen Sicherheitsvorfalls innerhalb von **24 Stunden** nach Entdeckung.
- **Erste Bewertung** des erheblichen Sicherheitsvorfalls innerhalb von **72 Stunden** nach der Entdeckung.
- **Detaillierter Abschlussbericht** innerhalb **eines Monats** nach der Entdeckung muss eingereicht werden.

Ein Sicherheitsvorfall gilt als erheblich, wenn

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

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



PSW GROUP

Artikel 23 – Berichtspflichten
Strengere Meldepflichten für Vorfälle

In Deutschland übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Aufsichtsaufgaben. Das BSI überwacht die Anwendung der Anforderungen aus der NIS2-Richtlinie,

Zu den Aufgaben gehört unter anderem:

- Regelmäßige Berichterstattung der Organisationen an das BSI
- Audits
- Durchführung von Vor-Ort-Prüfungen

PSW GROUP

NIS2 - Sanktionen

- Die Mitgliedstaaten können bei bestimmten Verstößen oder Zuwiderhandlungen Geldbußen von bis zu **10 Millionen Euro oder 2 % des Jahresumsatzes** verhängen.
- Darüber hinaus können Leitungsorgane **persönlich** für Verstöße **haftbar** gemacht werden

NIS2 - Umsetzungsgesetz

- Das Gesetz zur Umsetzung von EU NIS2 ist das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG)
- Trifft 2024 in Kraft – derzeit liegt der dritter Entwurf (Diskussionspapier) von September 2023 vor
- Es überführt die EU-weiten Mindeststandards für Cybersecurity der EU-Direktive NIS2 in deutsche Regulierung.
- Die NIS2-Umsetzung wird mindestens 30 Tsd. Unternehmen in Deutschland betreffen.

PSW GROUP

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG

KRITIS	SEKTOREN ANLAGE 1	SEKTOREN ANLAGE 2
Energie	**Energie** Stromversorgung, Fernwärme/-kälte, Kraftstoff/Heizöl, Gas	
Transport/Verkehr	**Transport/Verkehr** Luftverkehr Schienenverkehr, Schifffahrt, Straßenverkehr	**Transport/Verkehr** Post und Kurier
Finanz/Versicherung	**Finanz/Versicherung** Banken, Finanzmarkt-Infrastruktur	**Chemie** Herstellung, Handel, Produktion
Gesundheit	**Gesundheit** Dienstleistungen, Referenzlabore, F&E, Pharma (NACE C Abt. 21), Medizinprodukte,	**Forschung** Forschungseinrichtungen
Wasser/Abwasser	**Wasser/Abwasser** Trinkwasser, Abwasser	**Verarbeitendes Gewerbe** Medizin/Diagnostika; DV, Elektro, Optik (NACE C Abt. 26 und 27); Maschinenbau (NACE C 28), Kfz/Teile (NACE C 29), Fahrzeugbau (NACE C 30)
IT und TK	**IT und TK** IXPs, DNS, TLD, Cloud Provider, RZ-Dienste, CDNs, TSP, elektronische Kommunikation/Dienste, Managed Services und Security Services	**Digitale Dienste** Marktplätze, Suchmaschinen, soziale Netzwerke
Weltraum	**Weltraum** Bodeninfrastrukturen	
Ernährung		**Lebensmittel** Großhandel, Produktion, Verarbeitung
Entsorgung		**Entsorgung** Abfallbewirtschaftung

Sektoren
Die Sektoren weichen von früheren Definitionen und auch EU NIS2 leicht ab.

KRITIS-Sektoren sind separat in §28 (6) definiert.

Unternehmensgröße
Unterscheidung nach Unternehmensgröße bei Mitarbeitern und Umsatz.

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG

Mittlere Unternehmen - Mitarbeiter ≥ 50, Umsatz ≥ 10 Mio. EUR, Bilanzsumme ≥ 10 Mio. EUR

Großunternehmen - Mitarbeiter ≥ 250, Umsatz ≥ 50 Mio. EUR, Bilanzsumme ≥ 43 Mio. EUR

KATEGORIE	GRÖßE	SEKTOREN
Besonders wichtige Einrichtungen (NIS2)	Großunternehmen	Energie, Transport und Verkehr, Finanzen und Versicherungen, Gesundheit, Trinkwasser und Abwasser, IT und TK, Weltraum
	Größenunabhängig	Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste
	Größenunabhängig	Zentralregierung
	Mittlere Unternehmen	Anbieter öffentlicher TK-Netze und TK-Dienste
	KRITIS-Anlagen	Betreiber kritischer Anlagen
Wichtige Einrichtungen (NIS2)	Mittlere Unternehmen	Energie, Transport und Verkehr, Finanzen und Versicherungen, Gesundheit, Trinkwasser und Abwasser, IT und TK, Weltraum
	Großunternehmen Mittlere Unternehmen	Post und Kurier, Entsorgung, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste, Forschung
	Größenunabhängig	Vertrauensdienste
Betreiber Kritischer Anlagen (NIS2 und DachG)	*KRITIS-Anlagen*	Energie, Transport und Verkehr, Finanzen und Versicherungen, Gesundheit, Trinkwasser und Abwasser, Ernährung, IT und TK, Weltraum, Entsorgung

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

PSW GROUP

NIS2UmsuCG

Pflichten von Betreibern und Einrichtungen

PFLICHT	BETREIBER KRITISCHER ANLAGEN	BESONDERS WICHTIGE EINRICHTUNG	WICHTIGE EINRICHTUNG
Geltungsbereich	Anlage(n)	Unternehmen	Unternehmen
Risikomanagement	✓	✓	✓
Höhere Maßstäbe für KRITIS	✓		
Besondere Maßnahmen z.B. Einsatz von Systemen zur Angriffserkennung	✓		
Registrierung	✓	✓	✓
Meldepflichten	✓	✓	✓
Nachweise	✓		
Informationsaustausch	✓	✓	
Unterrichtungspflichten	✓	✓	✓
Governance Leitungsorgane	✓	✓	✓

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG - Risikomanagement

- ✓ Risikoanalyse und Sicherheit für Informationssysteme
- ✓ Bewältigung von Sicherheitsvorfällen
- ✓ Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- ✓ Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- ✓ Sicherheit in der Entwicklung, Beschaffung und Wartung
- ✓ Management von Schwachstellen
- ✓Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- ✓Schulungen Cybersicherheit und Cyberhygiene
- ✓Kryptografie und Verschlüsselung
- ✓Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- ✓Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- ✓Sichere Kommunikation (Sprach, Video- und Text)
- ✓Sichere Notfallkommunikation

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG - Nachweise und Prüfungen

Die Umsetzung der NIS2-Maßnahmen muss dem BSI von Betreibern kritischer Anlagen alle drei Jahre nachgewiesen werden.

Frühestens ab **2027** und abhängig von der eigenen Registrierung soll es dann alle drei Jahre Prüfungen geben, analog zu bisherigen KRITIS-Nachweisprüfungen.

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG - Meldewesen

- Meldung von Sicherheitsvorfällen
  - Erstmeldung bei erheblichen Sicherheitsvorfällen unverzüglich, innerhalb von 24h
  - Meldung über einen erheblichen Sicherheitsvorfall innerhalb von 72h mit Bewertung der Erstmeldung (Schwere, Auswirkungen, Kompromittierung)
  - Zwischenmeldungen auf Nachfrage des BSI
  - Abschlussmeldung oder Fortschrittsmeldung innerhalb eines Monats mit Beschreibung, Ursachen, Maßnahmen, grenzüberschreitenden Auswirkungen
- Meldungen an Kunden und Öffentlichkeit
  - Bei erheblichen Sicherheitsvorfällen kann das BSI besonders wichtige und wichtige Einrichtungen anweisen, ihre Kunden (Empfänger ihrer Dienste) zu unterrichten.
- Registrierung und Kontaktstelle
  - Betreiber müssen sich selbst identifizieren und beim BSI registrieren.
  - Für bestimmte Unternehmen gelten spezielle Registrierungsregeln.
- Informationsaustausch
  - Besonders wichtige Einrichtungen müssen innerhalb eines Jahres nach Inkrafttreten (d.h. 2025) am Informationsaustausch über die zentrale Austauschplattform des BSI teilnehmen.

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

PSW GROUP

NIS2UmsuCG - Ausschlüsse

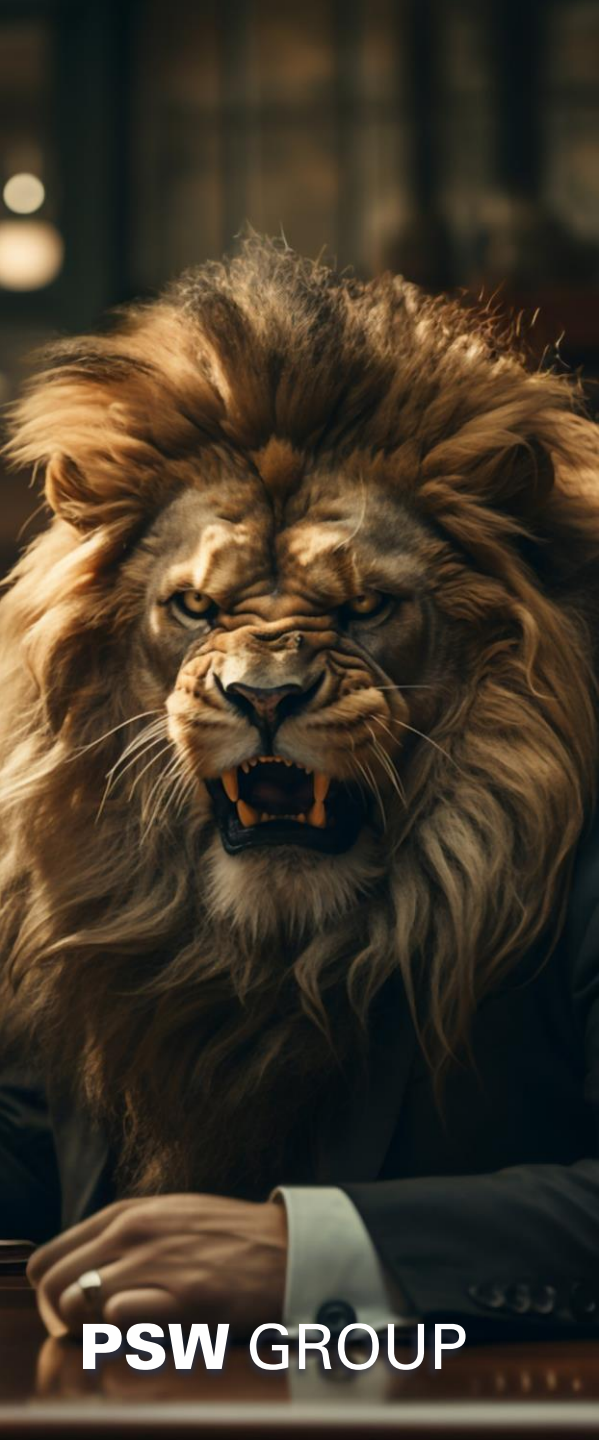
- Für diverse Unternehmen bestehen Ausnahmen und Sonderregeln zu NIS2-Pflichten.

- DNS, TLD, Cloud-Computing, Rechenzentren, Content Delivery Networks, Managed Services und Managed Security Services, Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke und Vertrauensdienste (§30 (2) Risikomanagementmaßnahmen) =>Eigene Maßnahmen werden definiert - Durchführungsrechtsakt der EU-Kommission

- Betreiber öffentlicher TK-Netze und TK-Dienste, Betreiber von Energieversorgungsnetzen oder Energieanlagen, gematik (Risikomanagementmaßnahmen, Meldepflichten)

- Von den besonders wichtigen und wichtigen Einrichtungen ausgeschlossen werden Einrichtungen gem. Art. 2 (4) der Verordnung (EU) 2022/2554 (DORA).

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html



NIS2UmsuCG - Sanktionen und Bußgelder

- NIS2-Umsetzungsgesetz definiert Bußgelder in §60.

- Die bisherigen KRITIS-Bußgelder werden dabei um einige neue Tatbestände erweitert und bestehende Bußgelder teils deutlich erhöht.

- Die Bußgelder und Sanktionen unterscheiden sich nach Gruppe:
  - Bußgelder für allgemeine Tatbestände §60 (5)
    - Allgemeine Bußgeldtatbestände unterscheiden in der Bußgeldbewährung nicht zwischen den unterschiedlichen Betreiber-Gruppen.
    - 100.000 EUR - 2 Mio. EUR
  - Bußgelder für wichtige Einrichtungen §60 (6)
    - 100.000 EUR - 7 Mio. EUR oder 1,4 Prozent Umsatz
  - Bußgelder für Betreiber kritischer Anlagen und besonders wichtige Einrichtungen §60 (7)
    - 100.000 EUR - 10 Mio. EUR oder 2 Prozent Umsatz

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

NIS2UmsuCG - Fristen und Umsetzung

- Das Gesetz NIS2UmsuCG selbst soll im Oktober 2024 in Kraft treten.
- Besonders wichtige Einrichtungen
  - Registrierung innerhalb von drei Monaten nach Identifizierung
  - Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten
- Wichtige Einrichtungen
  - Registrierung innerhalb von drei Monaten nach Identifizierung
- Betreiber kritischer Anlagen
  - Registrierung innerhalb von drei Monaten nach Identifizierung
  - Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt: frühestens drei Jahre nach Inkrafttreten des Gesetzes, d.h. ab 2027.
  - Fortlaufende Nachweise über Maßnahmenumsetzung anschließend alle drei Jahre
  - Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten

*Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

PSW GROUP

Empfehlung

- Prüfen Sie, ob Ihr Unternehmen in den Anwendungsbereich fällt.
- Fangen Sie mit der Risiko-Analyse an. Implementieren Sie **angemessene** technische und organisatorische Maßnahmen.
- Implementieren Sie ein Krisen-Management um bei einem Sicherheitsvorfall schnell, fristgerecht und mit entsprechender Berichterstattung reagieren zu können.
- Rahmenwerke und Standards passend zur Branche und Unternehmensgröße unterstützen bei der Umsetzung
  - ISO 27001
  - BSI IT-Grundschutz

So können wir Sie unterstützen

- Umfangreiches Angebot an digitalen Zertifikaten um die Anforderungen aus dem Bereich der Kryptographie zu erfüllen
- Unterstützung bei der Umsetzung der Anforderungen aus der ISO 27001
- Workshops im Bereich Risikomanagement
- Qualifizierung des Fachpersonals und Schulung der Mitarbeiter im Bereich ISO 27001 (Foundation, Officer, Auditor)
- Bereitstellung einer Notfallinfrastruktur inkl. sichere Kommunikation im Krisenfall


Vielen
Dank!