DEUDAT
Datenschutz und Informationssicherheit

DIE NIS2 - RICHTLINIE

WAS KOMMT AUF UNS ZU?

AUSWIRKUNGEN – ANFORDERUNGEN – UMSETZUNG

www.deudat.de

INHALTSVERZEICHNIS

EINLEITUNG

Die NIS2-Richtlinie (Network and Information Systems Directive 2) stellt eine umfassende Überarbeitung der ursprünglichen NIS-Richtlinie dar, die 2016 in Kraft trat. Diese neue Richtlinie wurde von der EU eingeführt, um die Cybersicherheit in Europa zu stärken und die Widerstandsfähigkeit kritischer Infrastrukturen zu verbessern. Mit einer Frist zur Umsetzung bis zum 17. Oktober 2024 bringt NIS2 erweiterte Pflichten und strengere Anforderungen für Unternehmen mit sich, die wesentliche und wichtige Dienste in der EU erbringen.

Die NIS2-Richtlinie zielt darauf ab, die Widerstandsfähigkeit von Netz- und Informationssystemen in der EU zu erhöhen, indem sie einen Rahmen für die Sicherheitsanforderungen festlegt und die Zusammenarbeit zwischen den Mitgliedstaaten fördert. Diese Initiative ist eine Reaktion auf die zunehmende Bedrohungslage durch Cyberangriffe, die sowohl die öffentlichen als auch die privaten Sektoren betreffen. Unternehmen, die als Betreiber kritischer Infrastrukturen (KRITIS) gelten, müssen nun umfassendere Maßnahmen ergreifen, um ihre Cybersicherheit zu gewährleisten.

Die Bedeutung der NIS2-Richtlinie wird besonders deutlich angesichts der aktuellen geopolitischen Lage und der damit verbundenen Cybersicherheitsbedrohungen. Der Angriffskrieg auf die Ukraine hat die Verwundbarkeit kritischer Infrastrukturen in Europa aufgezeigt und die Notwendigkeit einer robusten Cybersicherheitsstrategie unterstrichen.

Die EU hat daher die NIS2-Richtlinie verabschiedet, um sicherzustellen, dass die Mitgliedstaaten und Unternehmen besser auf Cyberbedrohungen vorbereitet sind und ein hohes gemeinsames Sicherheitsniveau erreichen.

ROADMAP: VON NIS1 ÜBER IT-SIG 2.0 ZU NIS2

Die Entwicklung der NIS-Richtlinie umfasst mehrere wesentliche Stationen zur Stärkung der Cybersicherheit in Europa.

Einführung der NIS1-Richtlinie (2016)
Die erste Network-and-Information-Security-Richtlinie (NIS1-RL) wurde 2016 eingeführt, um die Cybersicherheit in der EU zu harmonisieren.

Umsetzung in nationales Recht (2017)
Der deutsche Gesetzgeber setzte die NIS1-RL 2017 durch das IT-Sicherheitsgesetz (IT-SiG) um, das umfangreiche Anforderungen für Betreiber kritischer Infrastrukturen (KRITIS) einführte.

Verabschiedung der NIS2-Richtlinie (2022)
Im Dezember 2022 verabschiedeten der Rat und das Europäische Parlament die NIS2-RL (Richtlinie (EU) 2022/2555), die die Anforderungen an die Cybersicherheit in der gesamten EU überarbeitete und erweiterte.

IT-Sicherheitsgesetz 2.0 (2021)
2021 erweiterte Deutschland das IT-Sicherheitsgesetz zu IT-SiG 2.0, um den Kreis der betroffenen Einrichtungen zu vergrößern und die Sicherheitsanforderungen zu verschärfen.

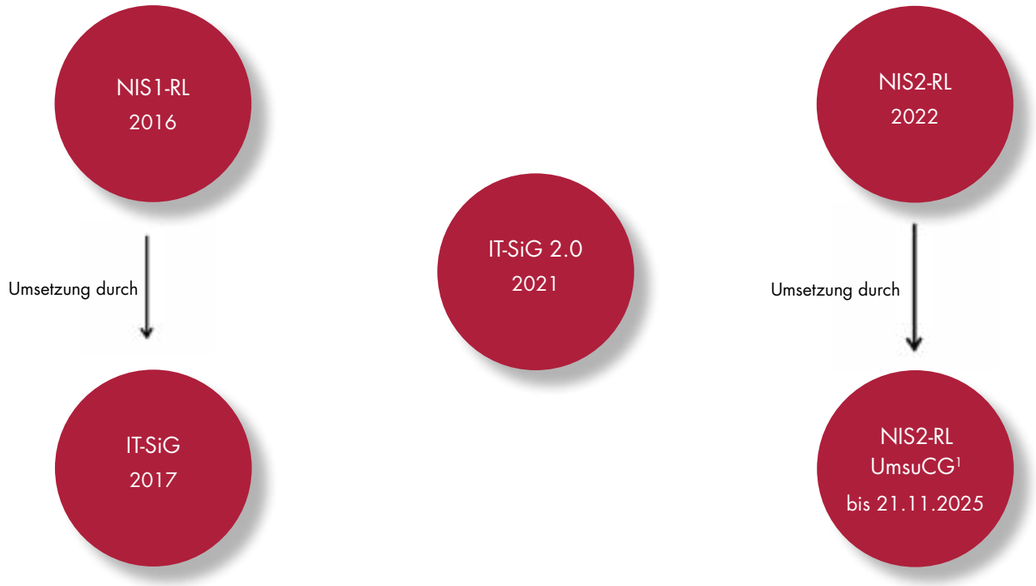
Aktuell: Meilenstein erreicht: Bundesrat billigt Entwurf zum deutschen NIS2-Umsetzungsgesetz

Der Bundesrat hat dem Gesetzentwurf zur Umsetzung der NIS2-Richtlinie am 21. November 2025 zugestimmt.

Der Deutsche Bundestag hat das Gesetz am 13. November 2025 verabschiedet.

Der Bundesrat hat das Gesetz in seiner Sitzung am 21. November 2025 gebilligt.

Inkrafttreten: 6. Dezember 2025 (in Deutschland).



AUFBAU DER NIS2 - RICHTLINIE

Die NIS2-Richtlinie ist umfassend strukturiert und beginnt mit einer Präambel, in der in 144 Punkten der Hintergrund der Richtlinie und einige Leitlinien für deren Anwendung erläutert werden. Der Hauptteil der Richtlinie ist in 46 Artikel gegliedert, die in neun Kapitel unterteilt sind. Diese Struktur hilft, die verschiedenen Aspekte der Cybersicherheit und die entsprechenden Anforderungen klar zu definieren.

Präambel.

Die Präambel der NIS2-Richtlinie bietet eine detaillierte Einführung in den Kontext und die Zielsetzung der Richtlinie, die den Hintergrund und die Notwendigkeit für verstärkte Cybersicherheitsmaßnahmen erläutern. Diese Einleitung schafft die Grundlage für die nachfolgenden Artikel und Kapitel.

KAPITEL DER NIS2-RICHTLINIE

Kapitel I — Allgemeine Bestimmungen: Dieses Kapitel enthält grundlegende Definitionen und Bestimmungen, die für das Verständnis der Richtlinie erforderlich sind.

Kapitel II — Koordinierte Rahmen für die Cybersicherheit: Hier werden die koordinierten Rahmenbedingungen für die Cybersicherheit auf europäischer Ebene beschrieben, um eine harmonisierte Herangehensweise zu gewährleisten.

Kapitel III — Zusammenarbeit auf Unions- und internationaler Ebene: Dieses Kapitel fördert die Zusammenarbeit zwischen den EU-Mitgliedstaaten und internationalen Partnern im Bereich der Cybersicherheit.

Kapitel IV — Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit: Dieses Kapitel ist besonders relevant für wesentliche und wichtige Einrichtungen, da es die spezifischen Maßnahmen beschreibt, die diese zur Einhaltung der NIS2 ergreifen müssen.

Kapitel V — Zuständigkeit und Registrierung: Es behandelt die Zuständigkeiten der Mitgliedstaaten und die Registrierungspflichten für betroffene Unternehmen.

Kapitel VI — Informationsaustausch: Dieses Kapitel fördert den Austausch von Informationen über Cybersicherheitsrisiken und -vorfälle zwischen den Mitgliedstaaten und relevanten Akteuren.

Kapitel VII — Aufsicht und Durchsetzung: Es beschreibt die Aufsichts- und Durchsetzungsmechanismen, die sicherstellen sollen, dass die Richtlinie korrekt implementiert wird.

Kapitel VIII — Delegierte Rechtsakte und Durchführungsrechtsakte: Hier werden die Befugnisse der EU-Kommission zur Annahme delegierter und Durchführungsrechtsakte festgelegt.

Kapitel IX — Schlussbestimmungen: Dieses Kapitel enthält die abschließenden Bestimmungen der Richtlinie.

ANHÄNGE

Anhang I — Sektoren mit hoher Kritikalität: Eine Liste der Sektoren, die als besonders kritisch angesehen werden und daher strenge Sicherheitsanforderungen erfüllen müssen.

Anhang II — Sonstige kritische Sektoren: Diese Liste umfasst weitere Sektoren, die ebenfalls wesentliche Sicherheitsmaßnahmen umsetzen müssen.

Anhang III — Entsprechungstabelle NIS2 zu NIS: Eine Tabelle, die die Entsprechungen zwischen den Artikeln der alten NIS-Richtlinie und der neuen NIS2-Richtlinie aufzeigt.

Hier finden Sie den vollständigen Text von NIS2:

nis2law.deudat.de

DIE WICHTIGSTEN CYBERSICHERHEITSANFORDERUNGEN DER NIS2

Überraschenderweise definiert die NIS2-Richtlinie die spezifischen Anforderungen an wesentliche und wichtige Einrichtungen hauptsächlich in Kapitel IV, das "Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit" behandelt. Alle anderen Kapitel richten sich vorwiegend an die Mitgliedstaaten und deren Verpflichtungen sowie an die Maßnahmen der Regierungsbehörden zur Durchsetzung der Richtlinie.

KAPITEL IV: WESENTLICHE ARTIKEL

Artikel 20 - Governance: Regelt die Anforderungen an die Unternehmensführung bezüglich der Cybersicherheit und verlangt, dass die Geschäftsleitung die Cybersicherheitsstrategie und deren Umsetzung überwacht.

Artikel 21 - Risikomanagementmaßnahmen im Bereich der Cybersicherheit: Beschreibt die spezifischen technischen und organisatorischen Maßnahmen, die Unternehmen zur Bewältigung von Cybersicherheitsrisiken ergreifen müssen.

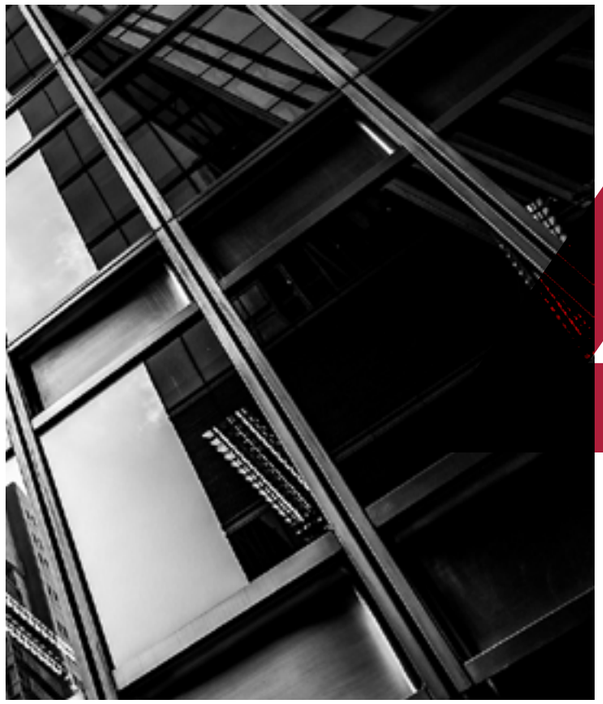
Artikel 22 - Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union: Behandelt die Bewertung und das Management von Risiken, die mit kritischen Lieferketten verbunden sind.

Artikel 23 - Berichtspflichten: Legt fest, wie und wann Unternehmen Cybersicherheitsvorfälle melden müssen, einschließlich Frühwarnungen und detaillierter Berichte.

Artikel 24 - Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung: Fördert die Verwendung von EU-weit anerkannten Cybersicherheitszertifizierungen zur Erhöhung der Sicherheitsstandards.

Artikel 25 - Normung: Stellt sicher, dass Unternehmen anerkannte Standards und Normen zur Cybersicherheit einhalten.

Diese Artikel bilden den Kern der Anforderungen für wesentliche und wichtige Einrichtungen und sind entscheidend für die Einhaltung der NIS2-Richtlinie. Die Unternehmen müssen sicherstellen, dass sie diese Anforderungen vollständig und fristgerecht umsetzen.



4

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

WELCHE UNTERNEHMEN SIND VON DER NEUEN NIS - RICHTLINIE BETROFFEN?

Die NIS2-Richtlinie erweitert den Geltungsbereich erheblich im Vergleich zur vorherigen Version und umfasst nun eine breitere Palette von Sektoren und Unternehmen. Diese Erweiterung zielt darauf ab, die Cybersicherheit in einer Vielzahl von kritischen und nicht kritischen Sektoren zu stärken, indem sie spezifische Anforderungen an Sicherheitsmaßnahmen und Risikomanagement setzt. Die betroffenen Unternehmen und Sektoren werden in zwei Hauptkategorien eingeteilt: Sektoren mit hoher Kritikalität und sonstige kritische Sektoren.

Sektoren mit hoher Kritikalität

Zu den Sektoren mit hoher Kritikalität gehören:

- **Energie:** Strom, Öl und Gas.
- **Verkehr:** Straßen-, Schienen-, Luft- und Seeverkehr.
- **Bankwesen:** Finanzinstitute und Banken.
- **Finanzmarktinfrastrukturen:** Börsen und andere zentrale Finanzdienstleister.
- **Gesundheitswesen:** Krankenhäuser und andere medizinische Einrichtungen.
- **Trinkwasser:** Wasserversorgung und -aufbereitung.
- **Abwasser:** Entsorgung und Behandlung von Abwasser.
- **Digitale Infrastruktur:** Internetknotenpunkte, DNS-Dienste und Datenzentren.
- **Verwaltung von IKT-Diensten:** IT-Service-Provider und Managed Services.
- **Öffentliche Verwaltung:** Regierungs- und Verwaltungsstellen.
- **Weltraum:** Satelliten und andere weltraumbezogene Dienste

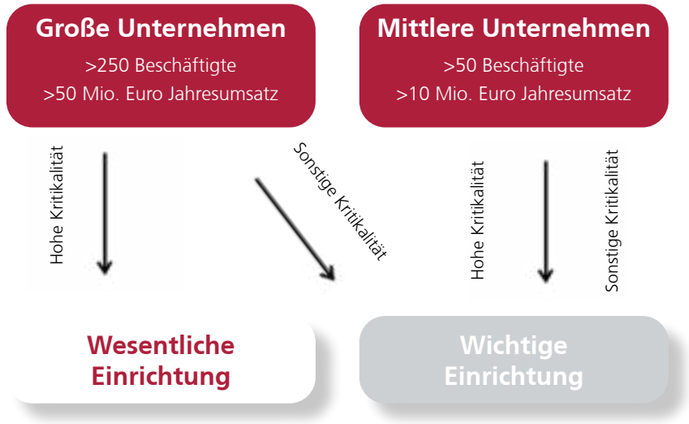
Sonstige kritische Sektoren umfassen:

- **Post- und Kurierdienste**
- **Abfallbewirtschaftung**
- **Produktion, Herstellung und Handel mit chemischen Stoffen**
- **Produktion, Verarbeitung und Vertrieb von Lebensmitteln**
- **Verarbeitendes Gewerbe**
- **Herstellung von Medizinprodukten**
- **Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen**
- **Herstellung von elektrischen Ausrüstungen**
- **Maschinenbau**
- **Herstellung von Kraftwagen und Kraftwagenteilen**

WESENTLICHE UND WICHTIGE EINRICHTUNGEN

Die NIS2-Richtlinie unterscheidet zwischen wesentlichen und wichtigen Einrichtungen. Diese Klassifizierung bestimmt die spezifischen Anforderungen und Aufsichtsmechanismen:

1. Wesentliche Einrichtungen: Unternehmen in Sektoren mit hoher Kritikalität, die mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von mehr als 50 Millionen Euro erzielen.
2. Wichtige Einrichtungen: Unternehmen, die mindestens 50 Mitarbeiter haben oder einen Jahresumsatz von mehr als 10 Millionen Euro erzielen, jedoch nicht als wesentliche Einrichtungen gelten.



Erweiterung des Anwendungsbereichs

Ein wesentlicher Aspekt der NIS2-Richtlinie ist die Erweiterung des Anwendungsbereichs, der nun auch kleinere Unternehmen und zusätzliche Sektoren umfasst. Zum Beispiel müssen nun auch Maschinenbauer, verschiedene Produktionsunternehmen, sowie alle Hersteller von medizinischen Geräten, einschließlich Wearables wie Fitness-Tracker, die Vorgaben der NIS2-Richtlinie einhalten. Dies bedeutet, dass Unternehmen, die bisher nicht unter die NIS1-Richtlinie fielen, nun Maßnahmen zur Cybersicherheit ergreifen müssen.

Diese umfassende Erweiterung stellt sicher, dass ein höheres Maß an Sicherheit und Resilienz in den betroffenen Sektoren erreicht wird, was letztlich dazu beiträgt, die gesamte EU widerstandsfähiger gegen Cyberangriffe zu machen. Unternehmen sind gut beraten, frühzeitig die notwendigen Schritte zu unternehmen, um die Anforderungen der NIS2-Richtlinie zu erfüllen und so ihre Betriebskontinuität und Sicherheit zu gewährleisten.

Resilienz bedeutet hierbei, sich schnell und effektiv von Cyberangriffen und anderen sicherheitsrelevanten Zwischenfällen zu erholen und ihre normalen Betriebsabläufe fortzusetzen. Resilienz umfasst sowohl präventive Maßnahmen als auch die Fähigkeit, im Ernstfall adäquat zu reagieren, Schäden zu begrenzen und sich wieder zu stabilisieren. Die NIS2-Richtlinie zielt darauf ab, genau diese Resilienz zu stärken, indem sie Unternehmen dazu anleitet, die notwendigen Sicherheitsvorkehrungen zu treffen.

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

BEISPIELE FÜR WESENTLICHE EINRICHTUNGEN

Krankenhaus	500 Beschäftige 500 Mio. Jahresumsatz	**Wesentliche Einrichtung**
Energieversorger	1.500 Beschäftige 800 Mio. Jahresumsatz	**Wesentliche Einrichtung**
Bank	4.000 Beschäftige 1,5 Mrd. Jahresumsatz	**Wesentliche Einrichtung**
IT-Dienstleister	800 Beschäftige 600 Mio. Jahresumsatz	**Wesentliche Einrichtung**

BEISPIELE FÜR WICHTIGE EINRICHTUNGEN

Maschinenbau-unternehmen	200 Beschäftige 35 Mio. Jahresumsatz	**Wichtige Einrichtung**
Produktion von medizini-schen Geräten	120 Beschäftige 25 Mio. Jahresumsatz	**Wichtige Einrichtung**
Wasserwerk	25 Beschäftige 30 Mio. Jahresumsatz	**Wichtige Einrichtung**
Produktion von Lebensmitteln	400 Beschäftige 40 Mio. Jahresumsatz	**Wichtige Einrichtung**

VERGLEICH KRITIS UND NIS2 (KRITIS)

BISHERIGE KRITIS-SEKTOREN

- Energie
- Transport/Verkehr
- Banken/Versicherung
- Medien & Kultur
- Gesundheit
- Wasser
- IT & TK
- Öffentliche Verwaltung
- Entsorgung
- Ernährung

UBI - KATEGORIEN

- Chemie
- Rüstung
- Volkswirtschaft

VERGLEICH KRITIS UND NIS2 (NIS2)

NEUE HOHE KRITISCHE SEKOTREN NACH NIS2

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum

NEUE SONSTIGE KRITISCHE SEKOTREN NACH NIS2

- Post- & Kurierdienste
- Entsorgung
- Chemie
- Ernährung
- Industrie
- Anbieter digitaler Dienste
- Forschung

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

KERNZIELE DER NIS2 - RICHTLINIE

Die NIS2-Richtlinie verfolgt mehrere wesentliche Ziele, die sich auf die Verbesserung der Cybersicherheit und die Schaffung eines einheitlichen Sicherheitsniveaus in der EU konzentrieren:

1. **Erweiterung des Geltungsbereichs:** Mehr Sektoren und Unternehmen fallen unter die Richtlinie, einschließlich digitaler Dienste und Lieferkettenmanagement.
2. **Stärkung der nationalen und EU-weiten Zusammenarbeit:** Förderung einer besseren Koordination und Informationsaustausch zwischen den Mitgliedstaaten.
3. **Verbesserte Risikomanagementmaßnahmen:** Einführung umfassenderer und detaillierterer Anforderungen an Sicherheitsmaßnahmen.
4. **Erhöhung der Verantwortlichkeit des Managements:** Leitungsorgane müssen aktiv in die Cybersicherheitsstrategie und deren Umsetzung eingebunden werden.
5. **Strengere Durchsetzungs- und Sanktionsmechanismen:** Einführung von klar definierten Sanktionen und Bußgeldern bei Nichteinhaltung.

MASSNAHMEN ZUM RISIKOMANAGEMENT

Die NIS2-Richtlinie fordert von wesentlichen und wichtigen Einrichtungen, geeignete technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen. Zu diesen Maßnahmen gehören:

1. **Risikoanalyse und Sicherheitsrichtlinien**: Regelmäßige Bewertung und Dokumentation der Sicherheitsrisiken.
2. **Incident Management**: Systeme und Prozesse zur Prävention, Erkennung und Reaktion auf Sicherheitsvorfälle.
3. **Geschäftskontinuität und Krisenmanagement**: Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Bewältigung von Krisensituationen.
4. **Sicherheit der Lieferkette**: Sicherstellung der Sicherheitsstandards bei Zulieferern und Dienstleistern.
5. **Schulung und Sensibilisierung**: Regelmäßige Schulungen für Mitarbeiter und Management in Bezug auf Cybersicherheitsrisiken und -praktiken.

ZENTRALE NIS2 - ANFORDERUNGEN

Von den 46 Artikeln der NIS2-Richtlinie betreffen nur die Artikel 20 bis 25 direkt Unternehmen, die NIS2-konform sein müssen. Die meisten anderen Artikel richten sich an staatliche Stellen, die für die Regulierung der Cybersicherheit verantwortlich sind. Diese zentralen Anforderungen sind in Kapitel IV zusammengefasst und konzentrieren sich auf die beiden Hauptbereiche Risikomanagement und Berichtspflichten. Hier sind die wichtigsten Punkte, die Unternehmen beachten müssen:

Verantwortlichkeit des Managements

Ein zentrales Element der NIS2-Richtlinie ist die gesteigerte Verantwortung des Managements. Leitungsorgane müssen sicherstellen, dass alle Risikomanagementmaßnahmen umgesetzt und überwacht werden. Bei Verstößen können sie persönlich haftbar gemacht werden, was die Bedeutung einer starken Führungsverantwortung im Bereich der Cybersicherheit unterstreicht.

Umsetzungsmechanismen

Die Umsetzung der NIS2-Richtlinie erfolgt durch nationale Behörden, die für die Überwachung und Durchsetzung der Maßnahmen zuständig sind. Diese Behörden haben das Recht, Audits durchzuführen, Sicherheitsüberprüfungen anzufordern und bei Nichteinhaltung Sanktionen zu verhängen.

Unternehmen müssen zudem regelmäßige Berichte über ihre Sicherheitsmaßnahmen und Vorfälle an die nationalen Behörden übermitteln.

ZENTRALE NIS2 - ANFORDERUNGEN

Lieferkettensicherheit

Artikel 21 betont die Notwendigkeit, Risiken in der Lieferkette zu managen. Unternehmen müssen die Sicherheit ihrer Lieferanten und Dienstleister bewerten, einschließlich deren Produktqualität und Sicherheitspraktiken, sowie sichere Entwicklungsverfahren sicherstellen.

Vorfallmeldung

Artikel 23 verpflichtet Unternehmen, erhebliche Sicherheitsvorfälle an die Computer Security Incident Response Teams (CSIRTs) und die Nutzer ihrer Dienste zu melden. Dies umfasst Frühwarnungen, detaillierte Zwischenberichte und Abschlussberichte über die Vorfälle.

Nutzung zertifizierter IT-Produkte und -Dienstleistungen

Obwohl die NIS2-Richtlinie keine Zertifizierung für wesentliche und wichtige Einrichtungen vorschreibt, können die Mitgliedstaaten oder die EU-Kommission verlangen, dass diese Einrichtungen zertifizierte IT-Produkte oder -Dienstleistungen verwenden. Diese Produkte und Dienstleistungen müssen den europäischen Zertifizierungsstandards für Cybersicherheit entsprechen.

Sanktionen und Strafen

Die NIS2-Richtlinie sieht erhebliche Strafen für die Nichteinhaltung vor. Wesentliche Einrichtungen können mit Bußgeldern von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes bestraft werden, je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen liegen die Höchststrafen bei 7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes. Diese strengen Sanktionen sollen sicherstellen, dass Unternehmen die Cybersicherheitsanforderungen ernst nehmen.

UMSETZUNGSSCHRITTE FÜR MASSNAHMEN ZUM MANAGEMENT VON CYBERSICHERHEITSRISIKEN

Die Einhaltung der NIS2-Richtlinie kann komplex sein, aber ein klarer Plan erleichtert das gesamte Projekt erheblich. Hier sind bewährte Vorgehensweisen, um die Anforderungen von Kapitel IV der NIS2-Richtlinie zu erfüllen, dass die Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit umfasst. Diese Schritte konzentrieren sich auf wesentliche und wichtige Einrichtungen, die die Hauptziele der NIS2-Richtlinie umsetzen müssen.

1. Unterstützung durch die Geschäftsleitung einholen

Die Einhaltung der NIS2-Richtlinie erfordert das Engagement der obersten Führungsebene. Ohne aktive Unterstützung kann das Projekt ins Stocken geraten, unterfinanziert sein und auf zahlreiche Hindernisse stoßen. Daher ist es wichtig, die Führungskräfte von der Bedeutung und den Vorteilen der Cybersicherheitsmaßnahmen zu überzeugen.

2. Projektmanagement einrichten

Aufgrund der Komplexität der NIS2-Richtlinie ist ein strukturiertes Projektmanagement unerlässlich. Dies beinhaltet die Definition von Implementierungsschritten, die Festlegung von Meilensteinen und die Zuweisung von Verantwortlichkeiten. Ein formeller Projektansatz hilft, den Fortschritt zu überwachen und sicherzustellen, dass alle Anforderungen termingerecht erfüllt werden.

3. Anfangsschulung durchführen

Frühzeitige Schulungen sind entscheidend, um alle Beteiligten mit den Anforderungen der NIS2-Richtlinie vertraut zu machen. Diese Schulungen schaffen ein gemeinsames Verständnis für die notwendigen Maßnahmen und erleichtern den Projektstart erheblich.

4. Top-Level-Politik zur Sicherheit von Informationssystemen verfassen

Auch wenn die NIS2-Richtlinie kein übergeordnetes Dokument explizit verlangt, ist es nach internationalen Standards eine bewährte Praxis, eine solche Richtlinie zu erstellen. Dieses Dokument legt die strategischen Ziele der Cybersicherheit fest, definiert Rollen und Verantwortlichkeiten und beschreibt, wie der Erfolg gemessen wird.

5. Risikomanagement-Methodik festlegen

Ein klar definierter Risikomanagementprozess ist entscheidend für die Einhaltung der NIS2-Richtlinie. Diese Methodik stellt sicher, dass alle im Unternehmen verstehen, wie Risiken identifiziert, bewertet und gemanagt werden. Ein entsprechendes Dokument legt die Regeln und Verfahren für das Risikomanagement fest.

6. Risikobewertung und -behandlung durchführen

Bei der Risikobewertung identifizieren Sie potenzielle Bedrohungen und Schwachstellen Ihrer Informationssysteme. Anschließend bewerten Sie die Wahrscheinlichkeit und die Auswirkungen dieser Risiken. Auf dieser Grundlage entwickeln Sie Maßnahmen zur Risikominderung, die in Artikel 21 der NIS2-Richtlinie beschrieben sind.

7. Risikobehandlungsplan erstellen und genehmigen

Ein detaillierter Risikobehandlungsplan dokumentiert die spezifischen Maßnahmen zur Risikominderung. Dieser Plan muss von der Unternehmensleitung genehmigt werden und enthält Informationen zu Verantwortlichkeiten, Zeitrahmen und den erforderlichen Ressourcen.

8. Cybersicherheitsmaßnahmen umsetzen

Die NIS2-Richtlinie erfordert die Umsetzung verschiedener Cybersicherheitsmaßnahmen, die auf den Ergebnissen der Risikobewertung basieren. Dies umfasst die Einführung neuer Sicherheitsprozesse, Aktivitäten und Technologien sowie die Erstellung von Richtlinien und Verfahren, um klare Anweisungen für die neuen Maßnahmen zu geben.

9. Sicherheit der Lieferkette festlegen

Eine zunehmende Zahl von Sicherheitsvorfällen ist auf Schwachstellen bei Lieferanten zurückzuführen. Daher müssen Unternehmen ihre Lieferanten sorgfältig bewerten, Sicherheitsklauseln in Verträgen aufnehmen und die Sicherheitslage ihrer Lieferanten überwachen.

10. Wirksamkeit der Cybersicherheit bewerten

Die Unternehmensleitung muss die Cybersicherheitsmaßnahmen kontinuierlich überwachen. Dies erfolgt durch regelmäßige Messungen, interne Audits und formelle Managementbewertungen. Diese Aktivitäten helfen, Abweichungen zu identifizieren und notwendige Korrekturmaßnahmen zu ergreifen.

11. Vorfallmanagement etablieren

Ein effektives Vorfallmanagement ist unerlässlich. Unternehmen müssen sicherstellen, dass bedeutende Vorfälle schnell und effektiv an die zuständigen Computer Security Incident Response Teams (CSIRTs) und die betroffenen Dienstleistungsempfänger gemeldet werden. Dies umfasst Frühwarnungen, Zwischenberichte und Abschlussberichte.

12. Kontinuierliche Cybersicherheitsschulung gestalten

Regelmäßige Schulungen für alle Mitarbeiter, einschließlich der Führungskräfte, sind notwendig, um die Cybersicherheitskultur im Unternehmen zu stärken. Die Schulungen sollten aktuelle Bedrohungen, neue Sicherheitspraktiken und die Bedeutung der NIS2-Richtlinie thematisieren.

13. Regelmäßige interne Audits

Obwohl interne Audits nicht explizit in der NIS2-Richtlinie erwähnt werden, gelten sie nach internationalen Standards als bewährte Praxis. Interne Audits helfen, Nichtkonformitäten zu identifizieren und bieten eine Grundlage für kontinuierliche Verbesserungen.

14. Regelmäßige Managementbewertungen

Managementbewertungen sind formelle Sitzungen, bei denen die Unternehmensleitung alle relevanten Informationen zur Cybersicherheit erhält, um wichtige Entscheidungen zu treffen. Diese Bewertungen können Korrekturmaßnahmen, Änderungen von Verantwortlichkeiten, neue Sicherheitsziele und Budgetfestlegungen umfassen.

15. Durchführung von Korrekturmaßnahmen

Korrekturmaßnahmen sind ein systematischer Ansatz zur Behebung von Nichtkonformitäten. Sie beinhalten die Analyse der Ursachen von Sicherheitslücken und die Umsetzung von Maßnahmen zur Beseitigung dieser Ursachen, um sicherzustellen, dass ähnliche Probleme in Zukunft nicht mehr auftreten.

ERFORDERLICHE DOKUMENTE FÜR NIS2

Notwendige Dokumentation

Die NIS2-Richtlinie verlangt eine Vielzahl von Dokumenten, um die Einhaltung der Cybersicherheits- und Berichtspflichten sicherzustellen. Dies umfasst:

- Risikobehandlungspläne: Dokumentation der identifizierten Risiken und der Maßnahmen zu deren Minderung.
- Schulungspläne: Pläne für die Schulung und Sensibilisierung der Mitarbeiter.
- Sicherheitsrichtlinien: Unternehmensweite Richtlinien, die die Cybersicherheitsstandards und -verfahren festlegen.
- Verfahrensdokumente: Dokumentation von Prozessen und Verfahren zur Umsetzung der Sicherheitsmaßnahmen und zur Reaktion auf Sicherheitsvorfälle.

Empfohlene zusätzliche Dokumente

Zusätzlich zu den erforderlichen Dokumenten sind weitere Richtlinien und Dokumente empfehlenswert, um die Cybersicherheit zu stärken:

- Informationsklassifizierung: Richtlinien zur Klassifizierung und zum Schutz sensibler Informationen.
- Mobilgerätenutzung: Richtlinien zur sicheren Nutzung von mobilen Geräten innerhalb des Unternehmens.
- Änderungsmanagement: Prozesse zur Verwaltung und Kontrolle von Änderungen in der IT-Infrastruktur.
- Sichere Kommunikation: Verfahren zur Sicherstellung der Vertraulichkeit und Integrität der Kommunikation innerhalb des Unternehmens.

Diese umfassende Dokumentation hilft, die Einhaltung der NIS2-Richtlinie nachzuweisen und die Cybersicherheitspraktiken im Unternehmen zu standardisieren.

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

NIS2 ZERTIFIZIERUNG

Die Einhaltung der NIS2-Anforderungen ist ein fortlaufender Prozess, der von Unternehmen verlangt, kontinuierlich ihre Sicherheitsmaßnahmen zu überwachen und gegebenenfalls anzupassen. Während die NIS2-Richtlinie selbst keine direkte Zertifizierung anbietet, fordert sie Unternehmen auf, anerkannte Sicherheitsstandards einzuhalten, die durch bestehende Zertifizierungen nachgewiesen werden können.

Es ist wichtig zu betonen, dass die NIS2-Richtlinie nicht die Umsetzung der ISO/IEC 27001 vorschreibt, jedoch in der Präambel die ISO/IEC 27000-Reihe als eine Möglichkeit zur Umsetzung von Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit erwähnt. Bei einem Vergleich von NIS2 und ISO/IEC 27001 wird deutlich, dass ISO/IEC 27001 einen ausgezeichneten Rahmen für die Einhaltung der in NIS2 geforderten Maßnahmen bietet. ISO/IEC 27001 bietet klare Leitlinien für den Risikomanagementprozess, die technische Umsetzung, Schulungen und die Einbeziehung der obersten Führungsebene.

Zusätzlich haben die Mitgliedstaaten oder die EU-Kommission die Möglichkeit, von wesentlichen und wichtigen Einrichtungen zu verlangen, bestimmte IT-Produkte oder Dienstleistungen zu verwenden, die nach den europäischen Zertifizierungsschemata für Cybersicherheit zertifiziert sind. Diese Zertifizierung erfolgt gemäß dem Cybersicherheitsgesetz (EU-Verordnung 2019/881), um sicherzustellen, dass die eingesetzten IT-Produkte und Dienstleistungen hohen Sicherheitsstandards entsprechen. Zu den spezifischen Zertifizierungen, die Einrichtungen erwerben können, gehören unter anderem die Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), die europäische Cloud-Zertifizierung (ENISA) und das EU Cybersecurity Certification Framework. Diese Zertifizierungen gewährleisten, dass IT-Produkte und Dienstleistungen robusten Sicherheitsanforderungen gerecht werden.

ZUSAMMENFASSUNG

Die NIS2-Richtlinie stellt eine erhebliche Erweiterung und Verschärfung der bisherigen Cybersicherheitsanforderungen dar. Unternehmen müssen proaktiv Maßnahmen ergreifen, um den neuen Anforderungen gerecht zu werden und die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten. Durch die frühzeitige Implementierung geeigneter Maßnahmen können Unternehmen nicht nur gesetzliche Anforderungen erfüllen, sondern auch ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen erheblich verbessern.

Wesentliche Einrichtungen, wie große Energieversorger, Banken und Gesundheitsdienste, sowie wichtige Einrichtungen, wie mittelständische IT-Dienstleister und digitale Plattformen, müssen nun strengere Sicherheitsmaßnahmen einhalten und regelmäßige Risikobewertungen durchführen. Ein Beispiel aus dem Gesundheitssektor zeigt, dass nun auch alle Hersteller von medizinischen Geräten den Vorgaben der NIS2-Richtlinie unterliegen, nicht nur jene, die bestimmte Schwellenwerte überschreiten. Dies umfasst auch Hersteller von Wearables wie Fitness-Tracker, die nun ebenfalls Maßnahmen zur Cybersicherheit umsetzen müssen.

Ein weiteres Beispiel ist der Automobilsektor, wo Hersteller nicht nur interne Sicherheitsmaßnahmen einführen, sondern auch sicherstellen müssen, dass ihre Zulieferer bestimmte Cybersicherheits-Standards einhalten. Diese erweiterte Verantwortung erstreckt sich entlang der gesamten Lieferkette und erfordert eine enge Zusammenarbeit zwischen den verschiedenen Akteuren, um die Sicherheitsanforderungen zu erfüllen.

Die NIS2-Richtlinie betont zudem die persönliche Haftung des Managements für die Einhaltung der Sicherheitsvorgaben. Dieser Aspekt ist von enormer Bedeutung, da er Entscheidungsträger direkt in die Verantwortung nimmt und sie dazu motiviert, die erforderlichen Sicherheitsmaßnahmen konsequent umzusetzen. Die persönliche Haftung bedeutet, dass Manager persönlich für Verstöße und mangelnde Sicherheitsvorkehrungen zur Rechenschaft gezogen werden können, was die Dringlichkeit und Wichtigkeit der Einhaltung der Richtlinie zusätzlich unterstreicht.

Damit wird die Implementierung der NIS2-Richtlinie nicht nur zu einer organisatorischen, sondern auch zu einer persönlichen Priorität für das Management. Führungskräfte müssen sich aktiv an der Umsetzung und Überwachung von Cybersicherheitsmaßnahmen beteiligen. Versäumnisse können zu erheblichen Strafen führen, die bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes betragen können. Diese strengeren Durchsetzungsmechanismen sollen sicherstellen, dass Cybersicherheit als zentrale Managementaufgabe wahrgenommen wird.

ZUSAMMENFASSUNG

Insgesamt ist die NIS2-Richtlinie ein entscheidender Schritt zur Stärkung der Cybersicherheit in der EU. Unternehmen, die frühzeitig die notwendigen Maßnahmen ergreifen und ihre Sicherheitsstrategien an die neuen Anforderungen anpassen, werden nicht nur den gesetzlichen Vorgaben gerecht, sondern auch ihre Resilienz gegenüber Cyberbedrohungen deutlich erhöhen. Dies trägt nicht nur zum Schutz der eigenen Infrastruktur bei, sondern auch zur Stabilität und Sicherheit der europäischen Wirtschaft und Gesellschaft insgesamt.

Unser Expertenteam der DEUDAT freut sich auf Sie!

WWW.DEUDAT.DE

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

UNSER NIS2-WORKSHOP FÜR IHR UNTERNEHMEN

Möchten Sie sicherstellen, dass Ihr Unternehmen optimal auf die Anforderungen der NIS2-Richtlinie vorbereitet ist? Nehmen Sie an unserem umfassenden Workshop teil, der speziell entwickelt wurde, um Ihnen die notwendigen Kenntnisse und Fähigkeiten zu vermitteln.

Das erwartet Sie in unserem Workshop:

1. Einführung
2. NIS2 Grundlagen
3. Welche Unternehmen müssen die Vorschriften einhalten
4. Die wichtigsten NIS2-Anforderungen
5. Umsetzungsschritte für Maßnahmen
6. Erforderliche Unterlagen für NIS2
7. Meldung von Vorfällen
8. Durchführung von Schulungen und Sensibilisierung gemäß NIS2
9. Beziehung zu anderen Rahmenwerken
10. 1Die Rolle der Registrierung und Umsetzung in lokale Gesetze
11. NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
12. Matching NIS2 Anforderungen zu ISO/IEC 27001

DEUDAT

Die Informationssicherheit dient in der Organisation der Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Dabei hat sie zum Ziel, Informationen vor Verlust, Diebstahl, Manipulation oder Missbrauch zu schützen. Grundlegend ist dafür eine geeignete Organisationsstruktur mit klar geregelten Abläufen, Verhaltensweisen und Zuständigkeiten, die mögliche Bedrohungsszenarien identifiziert und ihnen wirksame Abwehrstrategien entgegenstellt.

In unserer heutigen modernen Industriegesellschaft ist Informationssicherheit eine der wichtigsten Aufgaben einer Organisation und bildet die Basis für Qualität und Vertrauen von Kunden und Partnern. Mit unserem langjährigen Know-how und den passenden Werkzeugen bringen wir Ihre Organisationen in Sachen Informationssicherheit einfach und sicher auf den richtigen Weg!

Wir sind mit der DEUDAT spezialisiert auf die Bereiche Datenschutz, Informationssicherheit, Qualitäts- und Umweltmanagement. Wir betreuen eine Vielzahl an Kunden aus verschiedenen Branchen, von Start-ups bis hin zu internationalen Konzernen. Dabei ist uns eine pragmatische und zielführende Arbeitsweise mit unseren Kunden wichtig.

Wünschen Sie nähere Informationen?
Kontaktieren Sie uns – wir beraten Sie gerne.

DEUDAT

Sie wünschen weitere Beratung zum Thema der NIS2-Richtlinie?

Die DEUDAT GmbH unterstützt Sie gerne bei der Zertifizierung und Umsetzung der Cybersicherheitsmaßnahmen.

Wenden Sie sich bei Interesse jederzeit gerne an:

kontakt@deudat.de

oder **+49 611 950008-40**

Ihr DEUDAT Team

WEITERE ANGEBOTE

Auch über das Thema der neuen NIS2-Richtlinie hinaus haben wir Firmen und Organisationen viel zu bieten. Hier ein Ausschnitt aus dem DEUDAT-Portfolio im Überblick:

Beratungen
- Datenschutz
- Informationssicherheitsmanagement (z.B. auf der Bais der DIN EN ISO/IEC 27001)
- Qualitätsmanagement (z.B. auf der Basis der DIN EN ISO 9001)
- Business Continuity Management und Notfallmanagement (z.B. auf Basis der DIN EN ISO 22301, BSI 200-4)
- Risikoanalysen
- DIN SPEC 27076
- KRITIS
- VDA-ISA TISAX
- Prüfungen nach BSI C5-Katalog

Rechtsberatungen
- Datenschutzrecht
- IT-Recht
- Vertragsrecht

Externe Bestellungen
- Datenschutzbeauftragter
- Informationssicherheitsmanagement-Beauftragter
- Qualitätsmanagement-Beauftragter
- Umweltmanagement-Beauftragter

Audits
- Rund um Datenschutz, Informationssicherheit, Qualitätsmanagement & Umweltmanagement

Schulungen
- Online-Schulungsplattform
- Inhouse Schulungen

Sind Ihre Themen dabei? Wünschen Sie nähere Informationen?
Sprechen Sie uns an – wir beraten Sie gerne.

DEUDAT GmbH
Zehntenhofstraße 5b I 65201 Wiesbaden I +49 611 95 00 08 -40
Gotzkowskystraße 20/21 I 10555 Berlin I +49 30 81 4 50 01-40
Oberalleestraße 3 I 56338 Braubach I +49 2627 26 49 99 -40
www.deudat.de

DEUDAT
Datenschutz und Informationssicherheit