



WHITEPAPER

Pflichten, Fristen & Maßnahmen für Unternehmen

NIS2-Umsetzungsgesetz Deutschland

Inhalt

1 Was ist NIS2?	03
2 Was ist neu bei NIS2?	04
2.1 NIS2 betrifft nun mehr Unternehmen und Organisationen	04
2.2 Fehlende Compliance wird teuer	05
2.3 Maßnahmenkatalog in NIS2 erweitert	05
2.4 Management haftet bei Verstößen	06
Schutz vor Cyberbedrohungen – NIS2-Vorgaben im Überblick	06
3 NIS2-Umsetzung in Deutschland	07
3.1 NIS2-Umsetzungs- & Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	08
3.2 NIS2UmsuCG verschärft Maßnahmen und Meldepflicht	08
4 Wen betrifft NIS2?	09
5 Verpflichtende Maßnahmen nach NIS2	11
5.1 Strenge Registrierungspflicht	11
5.2 Meldepflicht von Sicherheitsvorfällen	11
6 Im Fokus von NIS2: Risikomanagement	13
Welche Maßnahmen des Risikomanagements regelt die NIS2-Richtlinie?	14
7 Mit baramundi zur NIS2-Compliance	15
8 Die nächsten Schritte zur NIS2-Compliance	17



1 Was ist NIS2?

Die wachsende Bedeutung von Cybersecurity

Die weltweite Bedrohung im digitalen Raum nimmt zu, auch in der EU. Besonders gefährdet sind kritische Infrastrukturen, die unverzichtbar für das reibungslose Funktionieren einer Gesellschaft sind. Ein eindrückliches Beispiel: Der Ausfall des Stromnetzes könnte zu einem Stillstand von lebenswichtigen Dienstleistungen wie Krankenhäusern, Kommunikationssystemen und Wasseraufbereitungsanlagen führen.

Von NIS zu NIS2

Die Klassifizierung solcher kritischen Infrastrukturen unterscheidet sich zwar zum Teil in den verschiedenen EU-Ländern, doch bereits seit 2016 setzt sich der Staatenverbund dafür ein, die Sicherheit in diesem besonders sensiblen Bereich durch einheitliche Standards zu erhöhen. Dafür entstand mit „NIS“ eine neue Richtlinie zur Netzwerk- und Informationssicherheit als Bestandteil der europäischen Cybersecurity-Strategie. NIS verpflichtete Organisationen der kritischen Infrastruktur – egal ob KRITIS oder den vergleichbaren EU-Pendants – eine Reihe von Mindeststandards einzuhalten, um die Sicherheit ihrer Netzwerke und Systeme zu gewährleisten. Die NIS-Richtlinie enthält gemeinsame Grundsätze und Mindestanforderungen, lässt jedoch den Mitgliedstaaten einen gewissen Spielraum bei der Umsetzung.

Nun wurde im Januar 2023 die NIS2-Richtlinie beschlossen. NIS2 zielt darauf ab, die Sicherheitsanforderungen für kritische Infrastrukturen weiter zu erhöhen und den Anwendungsbereich der ersten Richtlinie deutlich zu erweitern.¹

Höhere Anforderungen für Unternehmen

Von transparenter IT-Infrastruktur bis zu konkreten Maßnahmen im Cyberrisikomanagement: Die meisten betroffenen Unternehmen werden nicht umhinkommen, zusätzliche Ressourcen zu mobilisieren, um NIS2 gerecht zu werden. Insbesondere das Risikomanagement nehmen wir in Kapitel 6 in den Blick.

Cybersecurity als Managementaufgabe

Die NIS2-Regelungen betreffen jedoch längst nicht mehr nur den praktischen Alltag von IT-Fachkräften. An verlässlicher Cybersecurity kommen mittlerweile verschiedene Führungsebenen wie der Chief Information Security Officer (CISO), die Geschäftsführung und Finance nicht mehr vorbei. Das heißt, Netzwerk- und Informationssicherheit wird immer mehr zu einem strategischen und unternehmenskulturellen Thema. Um dieses Interessenfeld auch in Zeit des Fachkräftemangels und einer immer komplexer werdenden IT dann jedoch realistisch, effizient und beispielsweise automatisiert umzusetzen, kann Unified Endpoint Management eine wertvolle Unterstützung bieten.

¹ Die gesamte Richtlinie findet sich zum Nachlesen unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555>.

2 Was ist neu bei NIS2?

In diesem Kapitel erfahren Sie, wie NIS2 die bisherigen Sicherheitsregeln verschärft, mehr Unternehmen einbezieht und Geschäftsleitungen stärker in die Verantwortung nimmt, um Cybersicherheit und Risikomanagement verbindlich zu stärken.

Seit 6. Dezember 2025 verbindlich

Im Vergleich zur NIS-Richtlinie von 2016 hat die EU mit NIS2 die bestehenden Regeln in fünf Kernbereichen verschärft. Diese Änderungen gelten in Deutschland seit dem 6. Dezember 2025 mit dem Inkrafttreten des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) und der Neufassung des BSI-Gesetzes und sind seitdem verbindlich umzusetzen, inkl. laufender BSI-Aufsicht.

Die 5 wichtigsten Änderungen

- 1 **Erweiterte Sektoren mit Unterscheidung zwischen Betreibern kritischer Anlagen (KRITIS), „besonders wichtigen“ und „wichtigen“ Einrichtungen**
- 2 **Höhere Geldstrafen bei Nichteinhaltung und strengere Aufsichtsmaßnahmen**
- 3 **Direkte Verantwortung und Beteiligung der Geschäftsleitung**
- 4 **Erweiterte Informations- und Meldepflichten**
- 5 **Detaillierte Anforderungen an verpflichtende Sicherheitsmaßnahmen, insbesondere im Risikomanagement, das regelmäßig dokumentiert werden muss**

2.1 NIS2 betrifft nun mehr Unternehmen und Organisationen

NIS2 erweitert die relevanten Sektoren auf elf besonders kritische und sieben weitere wichtige Bereiche. In Deutschland sind nach aktuellen Schätzungen rund 29.500 Einrichtungen betroffen – ein deutlicher Anstieg gegenüber den bisher etwa 4.500 regulierten KRITIS-Betreibern. Die Einstufung als Betreibender kritischer Anlagen, besonders wichtige oder wichtige Einrichtung hängt vom Sektor und der Unternehmensgröße ab (siehe Kapitel 4).

2.2 Fehlende Compliance wird teuer

Unternehmen in Deutschland riskieren bei NIS2-Verstößen erhebliche Geldbußen nach dem NIS2-Umsetzungsgesetz (§ 65 BSIg). Die EU-Richtlinie legt verbindliche Mindeststandards fest: Besonders wichtige Einrichtungen (z. B. Betreiber kritischer Anlagen und große Unternehmen in hochkritischen Sektoren) drohen bis zu 10 Millionen € oder 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Wichtige Einrichtungen können mit bis zu 7 Millionen € oder 1,4 % des weltweiten Jahresumsatzes belegt werden.

In Deutschland sind die Bußgelder staffelartig geregelt und reichen je nach Schwere des Verstoßes (z. B. bei Meldepflicht- oder Risikomanagementverstößen) von 100.000 € für leichtere Verstöße wie eine fehlende Registrierung bis zu den genannten Höchstbeträgen.

Für die Einstufung der Unternehmensgröße gelten die in der NIS2 definierten Schwellenwerte:



Mittlere Unternehmen:

mehr als 50 Mitarbeitende
oder Umsatz > 10 Mio. Euro UND
Bilanzsumme > 10 Mio. Euro



Große Unternehmen:

mehr als 250 Mitarbeitende
oder Umsatz ≤ 50 Mio. Euro UND
Bilanzsumme ≤ 43 Mio. Euro



Entscheidend ist, dass in den betroffenen Sektoren in der Regel zwei von drei Kriterien (Anzahl Mitarbeitende, Umsatz, Bilanzsumme) erfüllt sein müssen, um als betroffen im Sinne der NIS2-Richtlinie zu gelten.

2.3 Maßnahmenkatalog in NIS2 erweitert

Von NIS2 betroffene Unternehmen müssen außerdem ein klares Sicherheitsprofil einhalten mit Fokus auf Risikomanagement und Lieferkettensicherheit. Erforderlich sind ebenso Penetrationstests, Incident-Reporting-Systeme und aktive Maßnahmen zur Absicherung von Netzwerken. Vorfälle müssen je nach Schwere des Vorfalls nicht nur national, sondern gegebenenfalls auch EU-weit kommuniziert werden.

2.4 Management haftet bei Verstößen



Enorm wichtig: NIS2 nimmt die Leitungsebene in besondere Verantwortung, wenn gegen Sicherheitsstandards verstoßen wird!

Die Geschäftsführung trägt persönliche Verantwortung für Cybersecurity und muss die Umsetzung geeigneter Cybersicherheitsmaßnahmen aktiv überwachen – ähnlich wie bei der DSGVO Haftungslogik.

Darüber hinaus besteht für Geschäftsführende NIS2 betroffener Unternehmen die Pflicht, regelmäßig Schulungen im Cybersicherheits Risikomanagement zu absolvieren und entsprechende Kenntnisse und Fähigkeiten nachzuweisen. Wird diesen Pflichten nicht nachgekommen, kann eine persönliche Binnenhaftung gegenüber der Einrichtung entstehen.

Schutz vor Cyberbedrohungen – NIS2-Vorgaben im Überblick

- ➔ Richtlinien („Policies“) für Risiken und Informationssicherheit
- ➔ Incident Management zur Vorbeugung und Bewältigung von Sicherheitsverletzungen
- ➔ Business Continuity (Backup, Disaster Recovery, Krisenmanagement)
- ➔ Schutz der Lieferkette und sichere IT-Beschaffung
- ➔ Messung der Wirksamkeit von Maßnahmen
- ➔ Kryptographie und Verschlüsselung
- ➔ Zugangskontrollen mittels Multi-Faktor-Authentifizierung und Single-Sign-On
- ➔ Maßnahmen zum Einsatz sicherer Sprach-, Video- und Text-Kommunikation

3 NIS2-Umsetzung in Deutschland

In diesem Kapitel erfahren Sie, wie Deutschland die EU-Richtlinie NIS2 mit dem NIS2UmsuCG umgesetzt hat, welche neuen Sicherheits- und Meldepflichten gelten und warum Unternehmen seit dem 6. Dezember 2025 ohne Übergangsfrist umfassende Cybermaßnahmen nachweisen müssen.

Bisherige Regelungen

Bisher wurde Cybersecurity in Deutschland durch das BSI-Gesetz (BSIG) und die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-KritisV) geregelt. Zusätzlich gab es auch spezialgesetzliche Anforderungen im Telekommunikationsgesetz (TKG) und im Gesetz über die Elektrizitäts- und Gasversorgung (EnWG).

IT-Sicherheitsgesetz 2.0 (2021)

Darüber hinaus wurde 2021 in Deutschland das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) eingeführt, das Cybersicherheit als Teil des flächendeckenden Wirtschaftsschutzes betonte und die Kategorisierung „Unternehmen im besonderen öffentlichen Interesse“ (UBI) einführte. Das IT-SiG 2.0 gilt als einer der Wegbereiter für die neue europäische Regulierung (kritischer) Cybersicherheit.

Umsetzung ohne Übergangsfrist

Die Bundesrepublik hat die NIS2-Richtlinie und die europäische Resilienz-Richtlinie (CER-RL) in das nationale Recht integriert. Die EU-Umsetzungsfrist lag bei 17. Oktober 2024; Deutschland hat beide Richtlinien mit dem NIS2UmsuCG zum 6. Dezember 2025 umgesetzt – ohne Übergangsfristen. Das bedeutet, dass alle betroffenen Unternehmen und Einrichtungen unmittelbar ab dem 6. Dezember 2025 den neuen gesetzlichen Pflichten unterliegen. Eine Übergangsphase wurde vom Gesetzgeber ausdrücklich ausgeschlossen.



Die Aufsicht durch das BSI beginnt damit sofort – Unternehmen können sich nicht auf Schonfristen berufen und müssen Maßnahmen nachweisen, selbst wenn diese erst unter Aufsicht finalisiert werden.

3.1 NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

In Deutschland wurden die NIS2-Vorgaben mit dem „NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG) in nationales Recht überführt. Das seit dem 6. Dezember 2025 geltende Gesetz ergänzt das BSI-Gesetz. Die CER-Richtlinie ist im „KRITIS-Dachgesetz“ (Entwurf vom 3. November 2025) verankert und gilt nur für Betreibende kritischer Anlagen. Das NIS2UmsuCG stärkt den Schutz kritischer Anlagen und großer Teile der Wirtschaft deutlich umfassender als zuvor.

So ist die in NIS2 benannte Unterteilung in „wesentliche“ und „wichtige“ Einrichtungen im deutschen Änderungs-gesetz sehr viel genauer differenziert: Es wird zwischen Betreibern kritischer Anlagen (KRITIS), besonders wichtigen Einrichtungen und wichtigen Einrichtungen unterschieden. KRITIS-Betreibende stellen dabei die höchste Qualifikationsstufe dar. Die im IT-SiG 2.0 noch als „UBI“ bezeichneten Unternehmen gehen in den besonders wichtigen und wichtigen Einrichtungen auf und sind damit in die neue Einordnung der NIS2-Regulierung integriert.

3.2 NIS2UmsuCG verschärft Maßnahmen und Meldepflicht

Das deutsche Umsetzungsgesetz erweitert bestehende Vorgaben für Cybersecurity und den Umgang mit tatsächlichen Sicherheitsvorfällen. Nach einer Erstmeldung eines Incidents innerhalb von 24 Stunden sind betroffene Einrichtungen nun auch zu Folge-, Zwischen- und Abschlussmeldungen verpflichtet.

Besonders wichtige und wichtige Einrichtungen müssen außerdem ein umfassendes Risikomanagement vorhalten. Hinzu kommen erforderliche technische und organisatorische Maßnahmen (TOM), um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme und Prozesse zu vermeiden. Auch die Auswirkungen von Sicherheitsvorfällen auf eigene oder andere Dienste sollen verhindert oder möglichst geringgehalten werden.

Um unverhältnismäßige Bürden zu vermeiden, werden bei der Bewertung verschiedene Faktoren berücksichtigt, ob getroffene Sicherheitsmaßnahmen dem bestehenden Risiko angemessen sind. Darunter fallen zum Beispiel das Ausmaß der Risikoexposition, die Größe der Einrichtung, wie wahrscheinlich Sicherheitsvorfälle sind und wie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen ausfallen.

Für KRITIS-Betreibende gelten allerdings erhöhte Anforderungen: Nach NIS2UmsuCG müssen sie bei ihren Maßnahmen z.B. auch aktuelle Lageberichte und Bewertungen des BSI zu Bedrohungsszenarien für die Versorgungssicherheit berücksichtigen.



Meldepflicht

Erstmeldung innerhalb 24 Stunden, sowie Folge-, Zwischen- und Abschlussmeldungen



Risikomanagement

Umfassendes Risikomanagement für besonders wichtige und wichtige Einrichtungen



Technische und organisatorische Maßnahmen (TOM)

Schutz von Verfügbarkeit, Integrität, Authentizität & Vertraulichkeit



Verhältnismäßigkeit

Bewertung anhand relevanter Faktoren zur Angemessenheit der Maßnahmen und des bestehenden Risikos

4 Wen betrifft NIS2?

In diesem Kapitel erfahren Sie, welche Unternehmen unter NIS2 fallen und warum auch mittlere Betriebe und ihre Lieferketten betroffen sind. Die Richtlinie erweitert den Kreis der verpflichteten Organisationen weit über klassische KRITIS-Betreiber hinaus.

Drei Kategorien betroffener Einrichtungen

NIS2 weitet die Anzahl der Organisationen, die von den erweiterten Cybersicherheitsmaßnahmen künftig betroffen sind, auf eine deutlich größere Gruppe aus. Die Richtlinie unterscheidet Sektoren nach zwei Anhängen (besonders kritische und weitere wichtige Sektoren); in Deutschland werden daraus drei Kategorien von Einrichtungen:

- ➔ **Betreibende kritischer Anlagen (KRITIS)**
- ➔ **Besonders wichtige Einrichtungen**
- ➔ **Wichtige Einrichtungen**

Zu den besonders kritischen Sektoren zählen u. a. Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (mit Ausnahme des Verbraucherbereichs), öffentliche Verwaltung sowie Weltraum. Unter den weiteren wichtigen Sektoren versteht man künftig u.a. Post und Kurier, Abfallwirtschaft, Chemikalien, Ernährung, Industrie sowie Bildung und Forschung.

Doch NIS2 geht bestehende Klassifizierungen kritischer Infrastruktur hinaus.

Künftig werden auch folgende Unternehmenskategorien von der NIS2-Richtlinie erfasst:

Mittlere Unternehmen: mindestens 50 und höchstens 249 Beschäftigte / Jahresumsatz von mehr als 10 Millionen Euro und eine Jahresbilanzsumme von mehr als 10 Millionen Euro

Großunternehmen: mindestens 250 Beschäftigte / Jahresumsatz von mindestens 50 Millionen Euro und zugleich einer Jahresbilanzsumme von mehr als 43 Millionen Euro



Viele betroffenen Unternehmen übersehen allerdings, dass NIS2 auch Lieferketten umfasst. Unternehmen, die also NIS2-relevante Organisationen unter ihren Kundinnen und Kunden haben, werden also ebenfalls dokumentieren müssen, dass sie NIS2-konform zu agieren – jenseits der genannten NIS2-Sektoren und -Kategorien.

Betroffenheit prüfen

Schätzungen deuten darauf hin, dass in Europa zusätzlich mehr als 100.000 Unternehmen von diesen neuen Vorschriften betroffen sein werden. Ob eine Einrichtung betroffen ist, lässt sich über den sogenannten NACE-Code überprüfen. Anhand der ermittelten Kategorisierung gilt es, die entsprechenden Pflichten zu identifizieren. Eine Betroffenheitsanalyse ist der erste Schritt, um Rolle und Pflichten des Unternehmens nach NIS2 und NIS2UmsuCG zu bestimmen.

Erfüllung von zwei der drei Merkmale:

Ein Unternehmen kann in eine der KMU-Klassen eingeordnet werden, sofern es die Anzahl der Mitarbeitenden (50 JAE) erreicht und lediglich eins der beiden finanziellen Merkmale erfüllt.

Kategorie des Unternehmens	Mitarbeiterzahl: Jahresarbeits Einheit (JAE)	Jahresumsatz	Jahresbilanzsumme
Mittelgroß	≤ 250	≤ 50 Mio. EUR	≤ 43 Mio. EUR
Klein	≤ 50	≤ 10 Mio. EUR	≤ 10 Mio. EUR
Kleinst	≤ 10	≤ 2 Mio. EUR	≤ 2 Mio. EUR



Beispiel:

Ein rechtlich selbständiges Unternehmen mit 49 Vollzeitmitarbeitenden (49 JAE), 11 Millionen Jahresumsatz und 9 Millionen Bilanzsumme darf sich als Kleinunternehmen einordnen, da es unter 50 Mitarbeitenden hat und eins der zwei finanziellen Merkmale erfüllt. Würde dieses Unternehmen nun wachsen auf 49 Vollzeitmitarbeitenden (49 JAE), 11 Millionen Jahresumsatz und 10 Millionen Bilanzsumme, so würde es als mittleres Unternehmen gelten und damit in den Anwendungsbereich der NIS2 fallen.

5 Verpflichtende Maßnahmen nach NIS2

In diesem Kapitel erfahren Sie, welche neuen Registrierungs- und Meldepflichten Unternehmen durch das NIS2UmsuCG erfüllen müssen und warum insbesondere die fristgerechte Registrierung beim BSI sowie schnelle Meldungen von Sicherheitsvorfällen entscheidend für die Compliance sind.

NIS2 legt zwei entscheidende Anforderungen für betroffene Unternehmen fest: die strenge Registrierungspflicht und die Meldepflicht von Sicherheitsvorfällen. Diese sind zwingend zu erfüllen bzw. gegebenenfalls umgehend umzusetzen.

5.1 Strenge Registrierungspflicht

Wichtige und besonders wichtige Einrichtungen müssen sich auf nationaler Ebene spätestens drei Monate nach ihrer erstmaligen oder erneuten Einstufung nach NIS2 registrieren und folgende Informationen an die verantwortliche Behörde übermitteln: Unternehmensname, Rechtsform, Handelsregisternummer, Adresse, Kontaktdaten (einschließlich E-Mail, Telefon, IP-Adressbereiche), relevanter Sektor oder Teilsektor, gegebenenfalls Liste der Mitgliedsstaaten, in denen das Unternehmen tätig ist. In Deutschland ist das BSI zuständig; die Registrierung erfolgt über ein zweistufiges Verfahren mit „Mein Unternehmenskonto“ (MUK) und dem neuen BSI-Portal, das seit 6. Januar 2026 live ist – erste Deadlines für viele Einrichtungen laufen zum 6. März 2026. Für jede Person, die Zugriff auf das Portal benötigt, ist ein eigenes ELSTER Organisationszertifikat erforderlich; pro Einrichtung können bis zu 500 Zertifikate beantragt werden. Änderungen dieser Angaben müssen unverzüglich, spätestens innerhalb von zwei Wochen, gemeldet werden. Die Nicht-registrierung oder verspätete Registrierung sowie die verspätete Übermittlung von Änderungen gelten als Ordnungswidrigkeit.²

5.2 Meldepflicht von Sicherheitsvorfällen

Von NIS2 betroffene Unternehmen sind verpflichtet, das BSI zeitnah über einen „erheblichen Sicherheitsvorfall“ zu informieren. Ein so definiertes Ereignis hat bereits schwere Betriebsstörungen oder finanzielle Verluste für die betroffene Einrichtung verursacht oder könnte diese verursachen. Oder das Ereignis hat andere Personen durch bedeutende materielle oder immaterielle Schäden beeinträchtigt oder könnte diese beeinträchtigen. In Deutschland gilt eine besonders detaillierte Regelung mit gestuften Fristen (24 Stunden, 72 Stunden, Zwischenmeldung, Abschlussmeldung), wie sie im NIS2UmsuCG und im BSIG festgelegt ist.

² Das Melde- und Informationsportal des BSI ist unter <https://mip2.bsi.bund.de/> erreichbar.



Beispiel:

24 h

Innerhalb von 24 Stunden nach Feststellen muss eine frühe Erstmeldung erfolgen. Dabei ist zu prüfen, ob ein Verdacht auf rechtswidrige Handlungen oder grenz-überschreitende Auswirkungen besteht.

72 h

Spätestens nach 72 Stunden muss eine Meldung mit einer ersten Bewertung von Schweregrad, befürchteten Auswirkungen und ggf. Kompromittierungsindikatoren (IoC) erfolgen.

auf
Anfrage

Auf Anfrage des Bundesamtes muss eine Zwischenmeldung erfolgen.

1 Monat

Spätestens einen Monat nach der ersten Meldung muss eine Abschlussmeldung erfolgen. Bestandteile sind eine ausführliche Beschreibung des Sicherheitsvorfalls, Art der Bedrohung bzw. zugrunde liegenden Ursache, getroffene und laufende Abhilfemaßnahmen, ggf. grenzüberschreitende Auswirkungen.

6 Im Fokus von NIS2: Risikomanagement

In diesem Kapitel erfahren Sie, wie NIS2 umfassendes Risikomanagement vorschreibt und warum Unified Endpoint Management (UEM) sowie klassische Cyberhygiene-Maßnahmen die Kernanforderungen effizient erfüllen.

Risikomanagement als Kernanforderung

Im Mittelpunkt der neuen NIS2-Direktive steht umfassendes Risikomanagement. Im Allgemeinen beinhalten die NIS2-Vorgaben, dass die Risikomanagement-Maßnahmen dem aktuellen Stand der Technik entsprechen. Sie beziehen relevante Standards, das Ausmaß der Risikobelastung, die Größe der Institution, die Wahrscheinlichkeit und Schwere von Sicherheitsvorfällen ein. Außerdem berücksichtigen sie die sozialen und wirtschaftlichen Auswirkungen. Wer seine Risikomanagement-Maßnahmen gar nicht, nicht richtig oder nicht rechtzeitig umsetzt, handelt ordnungswidrig.



Technische Umsetzung in der Praxis

Die Umsetzung der NIS2-Richtlinie erfordert von vielen Unternehmen zunächst eine Vielzahl an technischen und organisatorischen Maßnahmen. Es gibt kein einzelnes Werkzeug, das alle NIS2-Anforderungen vollständig erfüllt. Stattdessen setzen die meisten Unternehmen bereits eine Reihe von IT-Sicherheitslösungen ein, die nun auch zur Einhaltung der NIS2-Richtlinie beitragen. Dazu gehören neben Network Access Control und Monitoring auch Lösungen für das Client Management beziehungsweise Unified Endpoint Management (UEM).



Transparenz durch Asset Management

Der Prozess beginnt mit einer umfassenden Inventarisierung der Hardware- und Softwareinformationen. Dabei ist es wichtig, alle Gerätetypen zu berücksichtigen, einschließlich Steuerungen und Netzwerkgeräte sowie Windows-Rechner und Mobilgeräte. Dieses Asset Management bildet die Grundlage für einige Anforderungen der NIS2-Richtlinie, wie Transparenz, Risikoanalyse und allgemeine Informationssicherheit.



Cyberhygiene durch UEM

NIS2 hebt außerdem Cyberhygiene und Incident Prevention hervor, was Schwachstellen- und Update-Management, Festplattenverschlüsselung (Defense Control), Allow- oder Blocklisting von Software und ein Ticketsystem zur schnellen Reaktion umfasst – allesamt klassische UEM-Disziplinen. Unternehmen können also mit automatisiertem Endpoint-Management eine breite Palette der NIS2-Vorgaben effizient erfüllen, ohne wichtige Ressourcen zu vergeuden.



Welche Maßnahmen des Risikomanagements regelt die NIS2-Richtlinie?

- | | | | |
|----------|---|-----------|--|
| 1 | Policies:
Einführung von Leitlinien für alle Risiken und die Umsetzung der Informationssicherheit | 8 | Personal:
Sicherheit personenbezogener Daten in Human Resources |
| 2 | Incident Management:
Erkennung und Bewältigung von Sicherheitsvorfällen | 9 | Asset Management (ISMS):
Ein Informationssicherheits-Managementsystem umfasst Regeln, Verfahren, Methoden und Werkzeuge zur Erhöhung der IT-Security.
ISO 27001 gilt als der Goldstandard |
| 3 | Business Continuity:
Backup-Management, Disaster Recovery und Krisenmanagement | 10 | Zugangskontrolle:
Überwachung und Protokollierung aller Zugriffe |
| 4 | Lieferkette:
Sicherheit der Lieferkette und Sicherheitsmaßnahmen bei der Beschaffung und Wartung von IT- und Netzwerksystemen | 11 | Authentifizierung:
Einsatz von Multifaktor-Authentifizierung (MFA) und Single Sign-On (SSO) |
| 5 | Wirksamkeit:
Spezifikationen für die Messung von Cyber- und Risikomaßnahmen | 12 | Kommunikation:
Verwendung von verschlüsselter Sprach-, Video- & Textkommunikation |
| 6 | Schulungen:
Trainings für Mitarbeitende im Bereich Cybersecurity | 13 | Emergency Response:
Einsatz von sicheren Notfall-Kommunikationssystemen |
| 7 | Datensicherheit:
Spezifikationen für Verschlüsselung in alle wesentlichen Bereiche | | |

7 Mit baramundi zur NIS2-Compliance

In diesem Kapitel erfahren Sie, wie die baramundi Management Suite Anforderungen der NIS2-Richtlinie zu Risikoanalyse, Patch-Management, Verschlüsselung und Zugriffskontrolle abdeckt.

Sind Sie für die IT in einem von NIS2 betroffenen Unternehmen verantwortlich? Dann kann baramundi Ihnen helfen, die neuen Anforderungen für die Cybersicherheit Ihres Unternehmens zu erfüllen. Die baramundi Management Suite deckt dabei folgende Bereiche der NIS2-Richtlinie über die unten genannten Funktionen ab:



Artikel 21 Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Die Mitgliedstaaten stellen sicher, dass [...] Einrichtungen geeignete [...] Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme [...] zu beherrschen und die Auswirkungen von Sicherheitsvorfällen [...] möglichst gering zu halten.

a)

Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

- **Vulnerability Scanner:** Finden Sie automatisiert bekannte Schwachstellen in Ihrem gesamten Netzwerk.
- **Inventory & Network Devices:** Hilft Ihnen vorhandene IT-Geräte in Ihrem Netzwerk zu entdecken und zu inventarisieren.
- **Update Management & Managed Software:** Verteilen Sie Updates und Patches in Form von getesteten, einsatzbereiten Paketen.

c)

Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

- **OS-Deployment & Configuration:** Löschen Sie kompromittierte Systeme und reinstallieren Sie Systeme und Konfigurationen automatisiert über ihr gesamtes Netzwerk.





f)

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

- **Vulnerability Scanner:** Identifizieren Sie automatisch die neuesten CVE
- **Update Management & Managed Software:** Installieren Sie automatisiert Sicherheitspatches und -updates aus vertrauenswürdigen Quellen

h)

Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

- **Endpoint Security:** Konfigurieren und verwalten Sie Verschlüsselung zentral – auf der Basis von MS Bitlocker Technologie – einschließlich PIN- und Recovery Key Management.
- **Device Control (powered by Drivelock):** Beschränken und kontrollieren Sie zuverlässig Zugang und Zugriff auf Daten und Informationen in Ihrem Netzwerk.

i)

Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

- **Endpoint Security:** Verwalten Sie zuverlässig lokale Admin-Passwörter und stellen Sie sicher, dass Passwörter nach Benutzung sofort geändert werden können.
- **Device Control (powered by Drivelock):** Kontrollieren Sie zuverlässig den Datenfluss zwischen Geräten und Zugriffe auf Datenträger.



Effektives UEM wie die baramundi Management Suite bietet nicht nur Schutz vor Strafen, sondern verhindert auch kostspielige Ausfälle. Die Beachtung von NIS2-Richtlinien ist somit nicht nur eine gesetzliche Pflicht, sondern auch ein zentraler Beitrag zur unternehmensweiten Sicherheit und Resilienz.

8 Die nächsten Schritte zur NIS2-Compliance

In diesem Kapitel erfahren Sie, welche Schritte zur NIS2-Compliance nötig sind – von der Analyse über Risikomanagement bis zu Schulungen – und wie eine konsequente Umsetzung die Cyberresilienz und Unternehmenssicherheit stärkt.

Sind Sie für die IT in einem von NIS2 betroffenen Unternehmen verantwortlich? Dann drängt die Zeit und Sie sollten so schnell wie möglich einen Plan erstellen, wie Sie die neuen Anforderungen für die Cybersicherheit Ihres Unternehmens umsetzen. Wir empfehlen Ihnen folgende nächste Schritte:

- 1 Starten Sie mit der Betroffenheitsanalyse:**
Führen Sie zeitnah die Betroffenheitsanalyse durch, um Ihr Unternehmen entsprechend der neuen NIS2-Richtlinie und auf der Basis der NACE-Klassifizierung einzuordnen. Auf dieser Grundlage können Sie dann Sicherheitsmaßnahmen planen.
- 2 Integrieren Sie das Management aktiv in den NIS2-Prozess**
Erläutern Sie Ihrer Geschäftsleitung die potenziellen Auswirkungen, wenn die NIS2-Anforderungen nicht oder nicht rechtzeitig erfüllt werden. Informieren Sie aber auch über die Vorteile einer proaktiven Umsetzung der im Rahmen der NIS2-Richtlinie geforderten Maßnahmen und zeigen Sie auf, wie NIS2 langfristig die Resilienz und Reputation Ihres Unternehmens stärken kann.
- 3 Planen Sie Ihre Risikomanagement-Maßnahmen:**
Führen Sie eine umfassende GAP-Analyse durch, um festzustellen, wo Handlungsbedarf besteht. Dies bildet die Grundlage für gezielte Schritte zur verbesserten Cybersecurity. Identifizieren Sie in diesem Zusammenhang auch, ob geeignete Automatisierungslösungen zur Verfügung stehen. Mit ihnen können Sie sich wertvolle Ressourcen für andere IT-Aufgaben freihalten.
- 4 Setzen Sie einen konkreten Plan für Ihr NIS2-Umsetzungsprojekt in Gang:**
Starten Sie ein dezidiertes Umsetzungsprojekt, um die Maßnahmen Schritt für Schritt zu implementieren. Bedenken Sie dies unbedingt in der Budget- und Personalplanung.
- 5 Führen Sie die Registrierung und Meldung an die Behörden durch:**
Legen Sie die notwendigen Prozesse zur Registrierung fest und bereiten Sie sich darauf vor, einen erheblichen Sicherheitsvorfall zu melden. Üben Sie diesen Ablauf, um im Ernstfall schnell und effizient handeln zu können.
- 6 Richten Sie ein regulatorisches Monitoring ein:**
Etablieren Sie ein Monitoring-System, das aktuelle Gesetzgebungen frühzeitig erkennt. Analysieren Sie neue Regularien gründlich und bewerten Sie ihre Auswirkungen auf Ihr Unternehmen.
- 7 Kümmern Sie sich um die nötigen Schulungen**
Seit 2026 laufen in Deutschland Schulungen für Geschäftsleiter und Mitarbeitende zu NIS2. BSI-FAQs und Webinare sind auf bsi.bund.de verfügbar.

UEM als Schlüssel zur NIS2-Compliance

In Zusammenfassung zeigt sich, dass NIS2 eine konsequente Umsetzung von Cybersecurity-Maßnahmen fordert. Verstöße oder Nachlässigkeit werden geahndet. Ein effektives UEM inklusive Endpoint Protection bietet nicht nur Schutz vor Strafen, sondern verhindert auch kostspielige Ausfälle. Diese Kombination gewährleistet die reibungslose Business Continuity in allen Unternehmensbereichen, sei es im Umgang mit Mitarbeitenden, in entscheidenden Terminen mit Kundinnen und Kunden oder in der Produktionshalle. Die Beachtung von NIS2-Richtlinien ist somit nicht nur eine gesetzliche Pflicht, sondern auch ein zentraler Beitrag zur unternehmensweiten Sicherheit und Resilienz.

Es lässt sich nicht leugnen: NIS2 fordert zum Teil strenges Vorgehen bei Cybersecurity-Maßnahmen und fordert konsequente Umsetzung. Verstöße oder Nachlässigkeit werden geahndet. NIS2-Compliance ist also ein Thema, das Geschäftsführung und IT-Abteilung nicht auf die leichte Schulter nehmen dürfen. Wer Ressourcen in die eigenen IT-Sicherheit investiert, beugt jedoch auch abseits von EU-Richtlinien kostenintensiven Ausfällen vor – egal, ob bei der Produktivität der Mitarbeitenden, in entscheidenden Terminen mit Kundinnen und Kunden oder in der Produktionshalle.

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an! Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

<https://www.baramundi.com/de-de/it-training/webinare/>

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com

