Neue Anforderungen für KMU – NIS-2-Richtlinie

INFO BLATT

NIS2 Directive
Netzwerk- und Informations-sicherheit Richtlinie

17.10.2024
Umsetzung in nationales Recht

18.10.2024
Maßnahmen müssen ergriffen sein

Neue Normen für digitaler Infrastruktur

Bereits im Jahr 2016 führte die Europäische Union mit der Netzwerk- und Informationssicherheit-1-Richtlinie Vorschriften zur Cybersicherheit ein. Die neu beschlossene Netzwerk- und Informationssicherheit-2-Richtlinie erweitert und aktualisiert den Anwendungsbereich auf Unternehmen und Organisationen.

Die Netzwerk- und Informationssicherheit-2-Richtlinie wurde auf EU-Ebene im Jahr 2023 verabschiedet, mit dem Ziel, den Schutz kritischer Infrastrukturen vor potenziellen Cyberangriffen zu verbessern. NIS steht für "Netzwerk- und Informationssicherheit" und entspricht der deutschen Übersetzung von "Network and Information Security".

Ziel der NIS-2-Richtlinie der EU ist es, Unternehmen zu verpflichten, ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken. Dies beinhaltet Maßnahmen zur Erhöhung des Schutzes vor Cyberangriffen, die Einhaltung von Sicherheitsstandards sowie die kontinuierliche Aktualisierung von Systemen. Die Mitgliedsstaaten sind verpflichtet, diese Richtlinie bis zum **17.10.2024** in nationales Recht umzusetzen.

Dieses Infoblatt gibt einen Überblick über die NIS-2-Richtlinie der EU. Erfahren Sie, welche Sektoren betroffen sind, welche Pflichten & Maßnahmen ab dem 18.10.2024 gelten und was das Nichteinhalten der neuen Anforderungen mit sich bringt.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Welche Unternehmen/Organisationen sind von der NIS-2-Richtlinie betroffen?

Die Anzahl der von der NIS-2-Richtlinie betroffenen Unternehmen steigt deutlich an, da die betroffenen Branchen erweitert wurden. Betroffen sind große und mittlere Unternehmen aus Sektoren mit hoher Kritikalität sowie aus anderen kritischen Sektoren.

ACHTUNG Die Unternehmen sind selbst dafür verantwortlich, festzustellen, ob die NIS-2-Richtlinie auf sie zutrifft, indem sie die vorgegebenen Kriterien prüfen. Eine behördliche Benachrichtigung darüber, dass die NIS-2-Vorgaben für sie gelten, erfolgt nicht.

Innerhalb der Sektoren unterscheidet man wesentliche und wichtige Einrichtungen. Die Unternehmen selbst werden noch in Größenklassen kategorisiert. Die NIS-2-Richtlinie gilt für Unternehmen, der nachfolgenden Sektoren, mit mind. 50 Mitarbeitenden **und** mindestens 10 Millionen Euro Jahresumsatz und Jahresbilanzsumme.

Große Unternehmen sind Unternehmen mit mehr als 250 Mitarbeitenden oder mehr als 50 Millionen Euro Jahresumsatz und 43 Millionen Euro Jahresbilanzsumme. Unabhängig von der Größe der Einrichtung gilt diese Richtlinie auch für Einrichtungen und deren Lieferanten, die nach der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden. Diese zählen zu den wesentlichen Einrichtungen.

Beispiel: Ein Unternehmen mit 39 Mitarbeitern und 11 Millionen Euro Umsatz gilt als mittleres Unternehmen. Bietet dieses Unternehmen z.B. „Digitale Dienste“ an, so handelt es sich um eine wichtige Einrichtung.

Sowohl wesentliche als auch wichtige Einrichtungen sind verpflichtet, die Auflagen der NIS-2-Richtlinie umzusetzen. **Unterschiede** bestehen jedoch bei der **Überprüfung durch Behörden** und den **Sanktionen.**

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Unternehmen aus diesen Sektoren mit hoher Kritikalität sind von der NIS-2-Richtlinie betroffen:

Die Größe eines Unternehmens spielt hier in der Zuordnung zu wesentlichen oder wichtigen Einrichtungen eine Rolle. **Große Unternehmen** aus den genannten Sektoren gelten als **wesentliche Einrichtungen** und **mittelgroße Unternehmen** werden als **wichtige Einrichtungen** eingestuft.

Mittlere und große Unternehmen zählen zu wichtigen Einrichtungen wenn Sie in den folgenden Sektoren tätig sind:

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Pflichten und Maßnahmen

Die NIS-2-Richtlinie der Europäischen Union legt eine Reihe von Pflichten fest, die Unternehmen im Bereich der Netzwerk- und Informationssicherheit erfüllen müssen, um den Schutz kritischer Infrastrukturen zu gewährleisten.

PFLICHTEN

- Risikomanagement
- Meldepflicht von Sicherheitsvorfällen
- Eigenständige Identifikation und Registrierung
- Dokumentationspflicht
- Organisationsleitung
- Angriffserkennung

1. Risikomanagement:

Die Implementierung eines umfassenden Risikomanagementsystems, das Unternehmen dabei unterstützt, potenzielle Cyberbedrohungen zu identifizieren, zu bewerten und angemessen darauf zu reagieren.

2. Meldepflicht:

Die Richtlinie eine Meldepflicht mit inhaltlichen Vorgaben für Unternehmen vor. Betroffene Unternehmen sind verpflichtet, Sicherheitsvorfälle zu melden. Die vorgesehenen Fristen können im deutschen Umsetzungsgesetz noch angepasst werden.

a. **Erstmeldung:** innerhalb von 24 Stunden ab Kenntnis des Vorfalls
b. **Technische Erweiterungsmeldung:** innerhalb von 72 Stunden ab Kenntnis des Vorfalls
c. **Zwischenbericht:** dauert der Sicherheitsvorfall länger als 30 Tage an, muss ein Zwischenbericht nach spätestens 30 Tagen erfolgen
d. **Abschlussmeldung:** spätestens nach 30 Tagen nach Beendigung des Sicherheitsvorfalls

3. Eigenständige Identifikation und Registrierung:

Unternehmen sind verpflichtet, eigenständig Sicherheitsrisiken zu identifizieren und zu registrieren, ohne auf externe Hinweise zu warten.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

4. Dokumentationspflichten:

Unternehmen werden verpflichtet, umfassende Dokumentationspflichten zu erfüllen. Sie müssen Nachweise über ihre Sicherheitsmaßnahmen führen und diese bei Bedarf den zuständigen Behörden vorlegen.

5. Verantwortung der Organisationsleitung

Führungskräfte in Unternehmen werden in die Pflicht genommen. Die Organisationsleitung muss die vom Unternehmen ergriffenen Risikomanagementmaßnahmen billigen und sich aktiv an Pflichtschulungen beteiligen, um ein angemessenes Verständnis für die Sicherheitsanforderungen zu gewährleisten. Darüber hinaus kann die Führungskraft unter bestimmten Umständen persönlich haftbar gemacht werden, wenn Sicherheitsvorfälle auftreten und Schäden entstehen.

6. Angriffserkennung:

Die Angriffserkennung für Betreiber kritischer Infrastrukturen ist verpflichtend. Diese Unternehmen müssen Mechanismen implementieren, um Cyberangriffe frühzeitig zu erkennen und angemessen darauf zu reagieren, um potenzielle Schäden zu minimieren. Dies trägt dazu bei, die Widerstandsfähigkeit kritischer Infrastrukturen gegen Cyberbedrohungen zu stärken und die Auswirkungen von Sicherheitsvorfällen zu begrenzen.

Maßnahmen

Von der NIS-2-Richtlinie betroffene Unternehmen sind verpflichtet, Maßnahmen bis zum **18.10.2024** zu ergreifen, um Sicherheitsrisiken zu kontrollieren und die Auswirkungen von Vorfällen zu minimieren oder zu verhindern. Die Angemessenheit dieser Maßnahmen wird durch eine Risikobewertung festgestellt. Zu den von der Richtlinie geforderten Maßnahmen gehören mindestens:

1. Risikoanalyse und Sicherheit für Informationssysteme:

Eine gründliche Risikoanalyse bildet die Grundlage für ein effektives Sicherheitsmanagement. Dabei werden potenzielle Bedrohungen identifiziert, bewertet und Maßnahmen zur Minimierung der Risiken implementiert. Dies umfasst sowohl die technischen Systeme als auch organisatorische Prozesse.

2. Bewältigung von Sicherheitsvorfällen:

Ein klar definierter Prozess zur Bewältigung von Sicherheitsvorfällen ist unerlässlich. Dies beinhaltet die schnelle Erkennung, Reaktion und Aufklärung von Vorfällen sowie die Implementierung von Maßnahmen zur Vermeidung zukünftiger Vorfälle.

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

3. Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisenmanagement:

Die kontinuierliche Aufrechterhaltung des Geschäftsbetriebs und die schnelle Wiederherstellung nach Störungen sind entscheidend. Ein effektives Backup-Management und umfassende Krisenmanagementstrategien stellen sicher, dass Daten und Systeme schnell wiederhergestellt werden können.

4. Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit:

Die Sicherheit erstreckt sich auch auf die gesamte Lieferkette. Sicherheitsvorkehrungen müssen sowohl für die Zusammenarbeit zwischen verschiedenen Einrichtungen als auch für externe Dienstleister getroffen werden, um Schwachstellen an diesen Schnittstellen zu minimieren.

Die Umsetzung dieser Maßnahmen ist erforderlich, um die Konformität nachzuweisen.

5. Sicherheit in der Entwicklung, Beschaffung und Wartung:

Sicherheitsaspekte müssen von Anfang an in den Entwicklungsprozess integriert werden. Dies umfasst sichere Entwicklungspraktiken, sorgfältige Beschaffung und regelmäßige Wartung der Systeme, um Sicherheitslücken zu schließen.

6. Management und Offenlegung von Schwachstellen:

Ein proaktives Management und die transparente Offenlegung von Schwachstellen sind entscheidend. Durch regelmäßige Sicherheitsüberprüfungen und zeitnahe Updates können bekannte Schwachstellen schnell behoben werden.

7. Bewertung der Wirksamkeit von Cybersicherheit und Risiko-Management:

Die kontinuierliche Bewertung der Wirksamkeit der implementierten Sicherheitsmaßnahmen ist unerlässlich. Dies hilft, Schwachstellen zu identifizieren und die Strategien kontinuierlich zu verbessern.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

8. Schulungen zu Cybersicherheit und Cyberhygiene:

Regelmäßige Schulungen und Sensibilisierungskampagnen für Mitarbeiter:innen stärken das Bewusstsein und die Kompetenzen im Umgang mit Sicherheitsrisiken. Cyberhygiene umfasst dabei grundlegende Praktiken zur Sicherung des täglichen Umgangs mit IT-Systemen.

9. Kryptografie:

Der Einsatz von Kryptografie ist ein wesentlicher Bestandteil der Informationssicherheit. Verschlüsselungstechniken schützen vertrauliche Daten sowohl während der Übertragung als auch bei der Speicherung.

10. Personalsicherheit, Zugriffskontrolle und Anlagen-Management:

Personalsicherheit und effektive Zugriffskontrollen sind entscheidend, um unbefugten Zugriff auf sensible Informationen zu verhindern. Ein umfassendes Anlagen-Management unterstützt dabei die Sicherung physischer und digitaler Ressourcen.

11. Multi-Faktor-Authentifizierung und kontinuierliche Authentisierung:

Die Implementierung von Multi-Faktor-Authentifizierung erhöht die Sicherheit erheblich. Kontinuierliche Authentisierungsmethoden, inklusive gesicherter Video-, Text- und Notfallkommunikation, gewährleisten eine robuste Zugangskontrolle und Überwachung.

Unterstützung finden Sie auch bei CYBERsicher, der Transferstelle Cybersicherheit im Mittelstand.
https://transferstelle-cybersicherheit.de/

SCAN ME

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Sanktionen

Bei Nichteinhaltung der geforderten Maßnahmen oder Verstoß gegen Meldepflichten besteht die Möglichkeit, dass auf das Unternehmen hohe Geldstrafen zukommen.

Die jeweiligen Aufsichtsbehörden haben die Befugnis, Vor-Ort-Kontrollen durchzuführen, Nachweise anzufordern und Anweisungen mit festgelegten Fristen zu erteilen. Dies erfolgt bei **wichtigen Einrichtungen** in der Regel reaktiv, beispielsweise nach Hinweisen auf Verstöße. Hingegen erfolgt die Überwachung **wesentlicher Einrichtungen** proaktiv durch zusätzliche regelmäßige Sicherheitsprüfungen, einschließlich Ad-hoc-Prüfungen.

Es existieren eine Bußgeldtabelle sowie entsprechende Bußgeldtatbestände gemäß der NIS-2-Richtlinie für die Umsetzung und die Verstöße in Bezug auf nicht umgesetzte Themen.

Die Sanktionen sind ähnlich zu Verstößen gegen die DSGVO.

Als Höchstbeträge für mögliche Geldbußen wurden 10 Millionen Euro oder 2 Prozent des weltweiten Gesamtumsatzes im Vorjahr für wesentliche Einrichtungen festgesetzt. Für **wichtige Einrichtungen** sind es 7 Millionen Euro oder 1,7 Prozent des weltweiten Gesamtumsatzes im Vorjahr.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Quellen und weiterführende Informationen

Weiterführende Links:

Richtlinie (EU) 2022/2557:

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2557

CYBERsicher Transferstelle Cybersicherheit im Mittelstand:

https://transferstelle-cybersicherheit.de/

Risk Inventory:

https://auditpbl3.wordpress.com/2019/03/13/task-1-risk-inventory/

Geldbußen für DSGVO-Verstöße:

https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

Vollständige NIS-2-Richtlinie:

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1687253036177

Das Mittelstand-Digital Zentrum Handel gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Infoblatt: Neue Anforderungen für KMU – NIS-2-Richtlinie – 05 2024
Herausgeber: ©Mittelstand-Digital Zentrum Handel
Partner: ibi research an der Universität Regensburg GmbH
Galgenbergstraße 25, 93053 Regensburg

digitalzentrumhandel.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages