

NIS2-RICHTLINIE

Erhöhte Cybersicherheitsanforderungen und deren Auswirkungen in der EU

Wir machen **DIGITALISIERUNG** – aber **SICHER!**

INHALT

1. EINFÜHRUNG	3
2. HISTORISCHER HINTERGRUND	3
3. ENTWICKLUNG DER NIS2	4
4. INHALTE DER NIS2	4
5. STRENGERE SICHERHEITSANFORDERUNGEN	5
7. SANKTIONEN BEI NICHTEINHALTUNG	6
8. BESONDERE UND WICHTIGE EINRICHTUNGEN	7
9. VERSCHÄRFUNG DER HAFTUNG UND SANKTIONEN	7
10. MASSNAHMEN ZUM RISIKOMANAGEMENT FÜR CYBERSICHERHEIT GEMÄSS NIS2 (ART. 21)	8
11. NIS2-RICHTLINIE: HERAUSFORDERUNGEN FÜR GESUNDHEITSEIN- RICHTUNGEN	10
12. FAZIT	11
13. QUELLEN	12

1. EINFÜHRUNG

Die Digitalisierung hat in den letzten Jahren in nahezu allen Lebensbereichen Einzug gehalten und die Art und Weise, wie wir arbeiten, kommunizieren und unsere Geschäfte abwickeln, grundlegend verändert. Gleichzeitig sind mit der wachsenden Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) auch die Risiken gestiegen. Cyberangriffe auf kritische Infrastrukturen, Unternehmen und staatliche Einrichtungen sind häufiger und komplexer geworden, was erhebliche wirtschaftliche und gesellschaftliche Schäden verursachen kann. In diesem Kontext spielt die NIS2-Richtlinie eine zentrale Rolle. Sie zielt darauf ab, die Cybersicherheit in der Europäischen Union zu verbessern, indem sie strengere Sicherheitsanforderungen und Meldepflichten für eine breite Palette von Sektoren und Unternehmen einführt. Dieser Beitrag beleuchtet die Entstehung, Entwicklung und Inhalte der NIS2-Richtlinie und zeigt ihre Bedeutung für Unternehmen und Institutionen auf.

2. HISTORISCHER HINTERGRUND

Die erste NIS-Richtlinie wurde 2016 als Reaktion auf die zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) und die damit verbundenen Bedrohungen durch Cyberangriffe eingeführt. Sie zielte darauf ab, ein hohes gemeinsames Sicherheitsniveau für Netz und Informationssysteme in der EU zu gewährleisten. Diese Richtlinie war ein Meilenstein, da sie erstmals spezifische Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste (Operators of Essential Services, OES) und Anbieter digitaler Dienste (Digital Service Providers, DSP) festlegte. Mit der rasanten Weiterentwicklung der digitalen Technologien und der zunehmenden Komplexität der Bedrohungslandschaft wurde jedoch deutlich, dass die ursprüngliche NIS-Richtlinie nicht ausreichte, um die Cybersicherheit effektiv zu gewährleisten. Cyberangriffe wurden häufiger und ausgeklügelter, was eine verstärkte und umfassendere regulatorische Antwort erforderte. Deshalb begann die Europäische Kommission im Jahr 2020 mit der Überarbeitung der NIS-Richtlinie, um den neuen Herausforderungen gerecht zu werden.

NIS2-Richtlinie

Anwendungsbereiche

BISHER

- Energie
- Transport
- Banken
- Finanzmarktinfrastrukturen
- Gesundheit
- Trinkwasserversorgung
- digitale Infrastruktur



NEU

- Öffentliche Verwaltung
- Raumfahrt
- Abfallwirtschaft
- Lebensmittelversorgung
- Chemische Industrie

sepp.med

3. ENTWICKLUNG DER NIS2

Die Überarbeitung der NIS-Richtlinie umfasste mehrere Phasen, einschließlich umfangreicher Konsultationen mit Mitgliedstaaten, Industrievertretern und anderen Interessengruppen. Ziel war es, die Schwachstellen der ursprünglichen Richtlinie zu identifizieren und Lösungen zu entwickeln, die eine bessere Resilienz und Sicherheit der Netz- und Informationssysteme gewährleisten.

Nach intensiven Diskussionen und Verhandlungen legte die Europäische Kommission im Dezember 2020 ihren Vorschlag für die NIS2-Richtlinie vor. Dieser Vorschlag wurde vom Europäischen Parlament und dem Rat der Europäischen Union geprüft und im Dezember 2022 offiziell angenommen. Die NIS2-Richtlinie tritt somit an die Stelle der ursprünglichen NIS-Richtlinie und erweitert deren Geltungsbereich und Anforderungen erheblich.

4. INHALTE DER NIS2

Die NIS2-Richtlinie umfasst mehrere zentrale Komponenten, die darauf abzielen, die Cybersicherheit in der EU umfassend zu verbessern. Diese werden im Folgenden detailliert erläutert.

Die NIS2-Richtlinie erweitert den Anwendungsbereich der ursprünglichen NIS-Richtlinie erheblich. Während die ursprüngliche Richtlinie nur bestimmte kritische Sektoren wie Energie, Transport, Banken, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasserversorgung und digitale Infrastruktur umfasste, erweitert die NIS2 diesen Geltungsbereich auf weitere Sektoren, darunter:

- Öffentliche Verwaltung
- Raumfahrt
- Abfallwirtschaft

- Lebensmittelversorgung
- Chemische Industrie

Durch diese Erweiterung wird sichergestellt, dass eine breitere Palette von Unternehmen und Organisationen, die für das Funktionieren der Gesellschaft und Wirtschaft wesentlich sind, den Cybersicherheitsanforderungen unterliegt.

5. STRENGERE SICHERHEITSANFORDERUNGEN

Unternehmen, die unter die NIS2 fallen, sind verpflichtet, umfassende technische und organisatorische Maßnahmen zu ergreifen, um ihr Netz- und Informationssysteme gegen Cyberangriffe zu schützen. Diese Maßnahmen umfassen unter anderem:

- Risikomanagement: Durchführung regelmäßiger Risikoanalysen zur Identifizierung und Bewertung von Bedrohungen und Schwachstellen.
- Sicherheitsrichtlinien: Implementierung und kontinuierliche Aktualisierung von Sicherheitsrichtlinien und deren Verfahren.
- Schulungen: Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter, um das Sicherheitsbewusstsein zu stärken.
- Technische Schutzmaßnahmen: Einsatz fortschrittlicher Technologien wie Firewalls, Intrusion Detection Systems (IDS), und Verschlüsselung zur Sicherung der IT-Infrastruktur.



NIS2-Richtlinie Betroffene Sektoren



Sektoren mit hoher Kritikalität

- Energie
- Abwasser
- Trinkwasser
- Verkehr
- Gesundheitswesen
- digitale Infrastruktur
- Bankwesen
- Verwaltung von IKT-Diensten (B2B)
- Finanzmarktinfrastrukturen
- Öffentliche Verwaltung
- Raumfahrt

Sonstige kritische Sektoren

- Post- und Kurierdienste
- Abfallwirtschaft
- Forschung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Herstellung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/ Herstellung von Waren
- Anbieter digitaler Dienste

6. ERWEITERTE MELDEPFLICHTEN

Die NIS2 verschärft die Meldepflichten für Sicherheitsvorfälle erheblich. Unternehmen müssen sicherstellen, dass alle Vorfälle, die erhebliche Auswirkungen auf die Bereitstellung ihrer Dienste haben, unverzüglich den zuständigen nationalen Behörden gemeldet werden. Die Meldepflichten sind klarer definiert und beinhalten spezifische Zeitrahmen für die Berichterstattung:

- **Erstmeldung:** Innerhalb von 24 Stunden nach dem Erkennen eines Vorfalls.
- **Zwischenbericht:** Innerhalb von 72 Stunden mit detaillierteren Informationen.
- **Abschlussbericht:** Innerhalb eines Monats nach dem Vorfall, einschließlich einer vollständigen Analyse und einer Beschreibung der ergriffenen Gegenmaßnahmen.

7. SANKTIONEN BEI NICHTEINHALTUNG

Die NIS2 sieht strengere Strafen für Unternehmen vor, die ihre Cybersicherheitsverpflichtungen nicht erfüllen. Diese Sanktionen können erhebliche Geldstrafen umfassen, die je nach Schwere des Verstoßes und der Größe des Unternehmens variieren. Ziel dieser Sanktionen ist es, die Einhaltung der Richtlinie sicherzustellen und Unternehmen zu motivieren, angemessene Sicherheitsmaßnahmen zu implementieren.

NIS2-Richtlinie

Umsetzung und Anforderungen



↓ 50



↓ 10 Mio. €

- **Kleine Unternehmen:**
Weniger als 50 Mitarbeitende oder Jahresumsatz unter 10 Mio. Euro (nicht relevant)



→ 250



↓ 50 Mio. €

- **Mittlere Unternehmen:**
Bis zu 250 Mitarbeitende oder Jahresumsatz bis 50 Mio. Euro (relevant)



↑ 250



↑ 50 Mio. €

↑ 43 Mio. €

- **Große Unternehmen:**
Über 250 Mitarbeitende oder Jahresumsatz über 50 Mio. Euro und Bilanzsumme von mind. 43 Mio. Euro (relevant)

8. BESONDERE UND WICHTIGE EINRICHTUNGEN

Die NIS2-Richtlinie unterscheidet zwischen „besonders wichtigen Einrichtungen“ und „wichtigen Einrichtungen“. Der Hauptunterschied besteht darin, dass für „wichtige Einrichtungen“ geringere Geldstrafen vorgesehen sind und sie einer reaktiven Aufsicht durch die Behörden unterliegen, im Gegensatz zur proaktiven Aufsicht, die der „besonders wichtigen Einrichtung“ vorbehalten ist.

In der EU soll es keine unterschiedlichen Mindestschwellenwerte mehr geben, sondern die Betroffenheit nach „uniformen Kriterien“ ermittelt werden. Unter die Regulierung fallen mittlere und große Unternehmen:

- Mittel (medium): 50-249 Beschäftigte oder 10-50 Mio. Euro Umsatz, < 43 Mio. Euro Bilanzsumme
- Groß (large): mindestens 250 Mitarbeitende oder mindestens 50 Mio. Euro Umsatz

Dadurch wird der Anwendungsbereich in Deutschland erheblich ausgeweitet.

9. VERSCHÄRFUNG DER HAFTUNG UND SANKTIONEN

Die NIS2-Richtlinie sieht ein differenziertes System für Bußgelder und Haftung vor, um die Einhaltung der Sicherheitsanforderungen sicherzustellen. Es wird zwischen fahrlässigem und vorsätzlichem Verschulden unterschieden, was sich auf die Höhe der Bußgelder auswirkt. Für wichtige Einrichtungen können Bußgelder verhängt werden, die entweder bis zu sieben Millionen Euro oder 1,4 Prozent des gesamten weltweiten Jahresumsatzes betragen, je nachdem, welcher Betrag höher ist. Besonders wichtige Einrichtungen müssen mit noch höheren Bußgeldern rechnen, die bis zu zehn Millionen Euro oder zwei Prozent des gesamten weltweiten Jahresumsatzes betragen können. Insgesamt können Bußgelder im Rahmen der NIS2-Richtlinie bis zu zwanzig Millionen Euro erreichen. Diese Regelungen sollen Organisationen dazu bewegen, angemessene Sicherheitsmaßnahmen zu ergreifen und die Meldepflichten bei Sicherheitsvorfällen ernst zu nehmen. Die betroffenen Unternehmen und Organisationen müssen angemessene Maßnahmen in Bereichen wie Cyber-Risikomanagement, Sicherheit in der Lieferkette, Business Continuity Management, Verschlüsselung, Zutrittsbeschränkungen sowie Berichterstattung an die Behörde und Abhilfemaßnahmen ergreifen.

Ein wichtiger Hinweis ist, dass gemäß dem Entwurf des Bundesinnenministeriums die Leitungsorgane von Unternehmen für die Einhaltung der Risikomanagementmaßnahmen mit ihrem Privatvermögen haften. Die Obergrenze für diese Haftung entspricht zwei Prozent des globalen Jahresumsatzes des Unternehmens.

Beispiel: Ein Cyberangriff mit betriebseinschränkenden Auswirkungen aufgrund eines mangelhaft überwachten Risikomanagementprozesses in einer besonders wichtigen Einrichtung könnte zu erheblichen Lösegeldzahlungen, Kosten für externe Dienstleister und Bußgeldern infolge von DSGVO- oder BSIG-Verstößen führen.

Bei Verletzung der Überwachungspflichten haftet ein Geschäftsleiter für die entstandenen Schäden. Ein Verzicht der Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung

oder ein Vergleich über diese Ansprüche ist unwirksam, außer bei Zahlungsunfähigkeit der Leitungsperson kann ein Vergleich mit ihren Gläubigern erfolgen oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

10. MASSNAHMEN ZUM RISIKOMANAGEMENT FÜR CYBERSICHERHEIT GEMÄSS NIS2 (ART. 21)

Unternehmen und Organisationen, die von der NIS2-Richtlinie betroffen sind, müssen spezifische Maßnahmen zur Cybersecurity ergreifen, um Risiken für ihre Netz- und Informationssysteme zu minimieren und die Auswirkungen von Sicherheitsvorfällen zu begrenzen. Diese Maßnahmen sollten sowohl die IT-Systeme als auch deren physische Umgebung schützen und auf einem risikobasierten Ansatz basieren. Das Sicherheitsniveau muss „dem bestehenden Risiko angemessen“ sein, wobei aktuelle Technikstandards, europäische und internationale Normen sowie die Kosten der Umsetzung berücksichtigt werden müssen.

10.1 Faktoren zur Bestimmung angemessener Maßnahmen:

- Risikoexposition
- Größe der Einrichtung
- Wahrscheinlichkeit und Schwere von Sicherheitsvorfällen

10.2 Umzusetzende Maßnahmen:

1. Richtlinien und Verfahren: Organisationen müssen umfassende Richtlinien zur Informationssicherheit entwickeln, die alle Aspekte der IT-Infrastruktur abdecken. Dies beinhaltet die Durchführung von Risikoanalysen, um potenzielle Bedrohungen zu identifizieren und deren Auswirkungen zu bewerten. Zudem ist es wichtig, klare Verantwortlichkeiten und Zuständigkeiten für die Umsetzung und Überwachung der Sicherheitsmaßnahmen festzulegen.
2. Vorfallmanagement: Es ist erforderlich, ein Incident-Response-Team zu etablieren, das für die Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen zuständig ist. Darüber hinaus müssen Organisationen einen detaillierten Vorfallreaktionsplan erstellen, der Schritte zur schnellen Reaktion und Wiederherstellung nach einem Vorfall enthält. Regelmäßige Übungen und Tests der Vorfallreaktionspläne sind notwendig, um ihre Wirksamkeit zu überprüfen und sicherzustellen, dass alle Mitarbeiter vorbereitet sind.
3. Kontinuitätsmanagement: Organisationen sollten Backup-Management-Systeme implementieren, die regelmäßige und sichere Backups aller kritischen Daten gewährleisten. Zudem müssen sie Wiederherstellungspläne entwickeln, die sicherstellen, dass die Organisation nach einem Ausfall schnell wieder betriebsfähig ist. Krisenmanagementpläne, die spezifische Maßnahmen für verschiedene Krisenszenarien, einschließlich Cyberangriffen, enthalten, sind ebenfalls erforderlich.
4. Lieferkettensicherheit: Es ist wichtig, Sicherheitsüberprüfungen und Audits bei Lieferanten und Partnern durchzuführen, um sicherzustellen, dass sie die Sicherheitsstandards einhalten. Sicherheitsanforderungen sollten in Verträge mit Lieferanten und Dienstleistern aufgenommen werden. Die Überwachung und Bewertung der Sicherheitspraktiken in der gesamten Lieferkette sind notwendig, um Schwachstellen zu identifizieren und zu beheben.

-
5. Sicherer Einkauf und Wartung: Organisationen müssen Sicherheitsanforderungen für den Erwerb neuer IT-Systeme und Software festlegen. Es sollten Sicherheitsvorkehrungen während der Entwicklung und Wartung von IT-Systemen implementiert werden, einschließlich regelmäßiger Updates und Patches. Sicherheitsüberprüfungen und Tests sind durchzuführen, um sicherzustellen, dass alle Systeme den Sicherheitsanforderungen entsprechen.
 6. Evaluierung der Maßnahmen: Es ist notwendig, die Wirksamkeit der implementierten Sicherheitsmaßnahmen regelmäßig zu überprüfen und zu bewerten. Dies beinhaltet die Durchführung von internen und externen Audits, um die Einhaltung der Sicherheitsrichtlinien zu überprüfen. Basierend auf den Ergebnissen der Bewertungen und Audits sollten die Maßnahmen angepasst und verbessert werden.
 7. Sicherheit und Schulungen: Organisationen sollten regelmäßige Schulungen und Sensibilisierungsprogramme für alle Mitarbeiter durchführen, um das Bewusstsein für Cybersicherheitsrisiken zu erhöhen. Spezialisierte Schulungen für IT- und Sicherheitspersonal sind ebenfalls bereitzustellen. Die Schulungsinhalte müssen regelmäßig aktualisiert werden, um mit den neuesten Bedrohungen und Best Practices Schritt zu halten.
 8. Einsatz von Kryptografie: Organisationen sollten Verschlüsselungstechnologien nutzen, um die Vertraulichkeit und Integrität sensibler Daten zu gewährleisten. Es sollten sichere Kommunikationsprotokolle für den Datenaustausch implementiert werden. Kryptografie sollte bei der Speicherung und Übertragung von Daten angewendet werden, um unbefugten Zugriff zu verhindern.
 9. Personalsicherheit und Zugangskontrollen: Es müssen strenge Zugangskontrollen eingeführt werden, um den Zugang zu kritischen Systemen und Daten auf autorisierte Personen zu beschränken. Hintergrundüberprüfungen bei neuen Mitarbeitern und regelmäßige Überprüfungen bei bestehenden Mitarbeitern sind durchzuführen. Asset-Management-Systeme zur Überwachung und Verwaltung aller IT-Ressourcen sollten implementiert werden.
 10. Authentifizierungsmethoden: Organisationen sollten Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit beim Zugriff auf Systeme und Daten einführen. Kontinuierliche Authentifizierungsmethoden sollten genutzt werden, um die Identität der Benutzer während ihrer gesamten Sitzung zu überprüfen. Sichere Authentifizierungsprotokolle und -verfahren sind zu implementieren.
 11. Sichere Kommunikation: Es ist notwendig, sichere Kommunikationsmethoden für Sprache, Video und Text zu gewährleisten, insbesondere in Notfallsituationen. Ende-zu-Ende-Verschlüsselung sollte für alle Kommunikationskanäle genutzt werden. Sichere Kommunikationsprotokolle und -plattformen sollten implementiert werden, um die Vertraulichkeit und Integrität der Kommunikation zu schützen.

Der deutsche Entwurf zur Umsetzung der NIS2-Richtlinie verlangt, dass nur zertifizierte IKT-Produkte und Dienste genutzt werden dürfen, um die Sicherheit der Netz- und Informationssysteme weiter zu erhöhen.

11. NIS2-RICHTLINIE: HERAUSFORDERUNGEN FÜR GESUNDHEITSEINRICHTUNGEN

Die NIS2-Richtlinie stellt Gesundheitseinrichtungen vor erhebliche Herausforderungen im Bereich der Cybersicherheit. Krankenhäuser und andere medizinische Einrichtungen müssen umfassende Maßnahmen zur Risikoanalyse, Vorfallsbewältigung und Sicherstellung der Betriebsfortführung umsetzen. Dabei muss die Sicherheit der gesamten Lieferkette medizinischer Produkte und Dienstleistungen gewährleistet sein, und die Mitarbeiter müssen regelmäßig geschult werden. Proaktive Sicherheitsmaßnahmen und strikte Zugangskontrollen sind unerlässlich, da diese Einrichtungen unter strenger Aufsicht stehen und hohe Geldstrafen bei Nichteinhaltung drohen. Wie bereits erwähnt haften Führungskräfte persönlich für die Einhaltung der Risikomanagementmaßnahmen.

Gesundheitseinrichtungen müssen eine detaillierte Risikoanalyse durchführen, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Diese Analyse umfasst sowohl IT-Systeme als auch vernetzte medizinische Geräte und Infrastrukturen. Ein effektiver Plan zur Vorfallsbewältigung ist essenziell, um schnell auf Cyberangriffe reagieren zu können, einschließlich der Einrichtung eines spezialisierten Notfallteams. Der Plan zur Betriebsfortführung stellt sicher, dass kritische Dienstleistungen auch im Falle eines Angriffs aufrechterhalten werden können, was besonders wichtig ist, da Ausfälle die Patientenversorgung direkt beeinträchtigen können.

Die Lieferkette medizinischer Produkte und Dienstleistungen muss streng überwacht werden, da Cyberangriffe auf Lieferanten erhebliche Auswirkungen auf Gesundheitseinrichtungen haben können. Daher ist es wichtig, dass alle Partner in der Lieferkette hohe Sicherheitsstandards einhalten, einschließlich regelmäßiger Sicherheitsüberprüfungen und der Integration von Sicherheitsanforderungen in Verträge mit Drittanbietern. Regelmäßige Schulungen der Mitarbeiter sind unerlässlich, um das Bewusstsein für Cyberbedrohungen zu schärfen und sichere Verhaltensweisen zu fördern. Dies umfasst Schulungen zur Erkennung von Phishing-Versuchen und zum sicheren Umgang mit sensiblen Daten.

Gesundheitseinrichtungen müssen zudem proaktive Sicherheitsmaßnahmen ergreifen, wie z.B. regelmäßige Sicherheitsüberprüfungen und Penetrationstests, um Schwachstellen zu identifizieren und zu beheben. Strikte Zugangskontrollen sind notwendig, um sicherzustellen, dass nur autorisiertes Personal Zugriff auf sensible Bereiche und Daten hat. Dies umfasst sowohl physische Sicherheitsmaßnahmen als auch IT-basierte Zugriffskontrollen wie Multi-Faktor-Authentifizierung und die Segmentierung von Netzwerken, um den Schaden im Falle eines Angriffs zu minimieren.

Durch die Umsetzung dieser umfassenden Maßnahmen können Gesundheitseinrichtungen die Anforderungen der NIS2-Richtlinie erfüllen und ihre Cybersicherheit erheblich verbessern, was letztendlich zur besseren Patientensicherheit und -versorgung beiträgt.



12. FAZIT

Die NIS2-Richtlinie markiert einen entscheidenden Schritt zur Stärkung der Cybersicherheit in der EU. Durch die Ausweitung des Anwendungsbereichs, verschärfte Sicherheitsanforderungen sowie strengere Meldepflichten und Sanktionen werden die Resilienz und Sicherheit der Netz- und Informationssysteme maßgeblich verbessert. Unternehmen und Mitgliedstaaten sind nun in der Pflicht, diese neuen Vorgaben konsequent umzusetzen, um die Stabilität der digitalen Infrastruktur Europas zu gewährleisten. Die NIS2-Richtlinie spielt eine zentrale Rolle in den fortlaufenden Bemühungen, die Cybersicherheit zu erhöhen und die Widerstandsfähigkeit gegen ständig wachsende Cyberbedrohungen zu stärken. In einer zunehmend vernetzten Welt ist die NIS2-Richtlinie ein unverzichtbares Instrument, um den Schutz kritischer Infrastrukturen sicherzustellen und das Vertrauen in digitale Dienste zu festigen. Wie der renommierte Sicherheitsexperte Bruce Schneier einmal sagte: „Sicherheit ist ein Prozess, kein Produkt.“ Diese Worte erinnern uns daran, dass Cybersicherheit ein fortlaufender, gemeinschaftlicher Aufwand ist, der ständige Wachsamkeit und Anpassung erfordert. Nur durch kontinuierliche Anstrengungen, Investitionen in innovative Sicherheitslösungen und enge Zusammenarbeit zwischen Staat und Wirtschaft können wir eine sicherere digitale Zukunft gestalten. Unternehmen müssen nicht nur technologisch aufrüsten, sondern auch eine Kultur der Sicherheit fördern, in der jeder Mitarbeiter seinen Beitrag zum Schutz der digitalen Infrastruktur leistet. Letztlich liegt es in unserer gemeinsamen Verantwortung, die notwendigen Maßnahmen zu ergreifen, um die Widerstandsfähigkeit gegen Cyberbedrohungen nachhaltig zu stärken und die digitale Souveränität Europas zu sichern.

NIS2-Richtlinie

Erforderliche Maßnahmen

- Risikomanagement
- Prozess zur Bewältigung von Sicherheitsvorfällen
- Sicherheit der Lieferketten
- Schulungen zur Cybersicherheit
- Kryptografie, Multi-Faktor-Authentifizierung
- Business Continuity Management
- Registrierung beim BSI
- Meldepflicht bei erheblichen Sicherheitsvorfällen

13. QUELLEN

Die Norm:

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

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinie_node.html

<https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/>

[Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html](#)

<https://www.pwc.de/de/cyber-security/europaeische-nis-2-richtlinie-implikationen-fuer-unternehmen-und-institutionen.html>