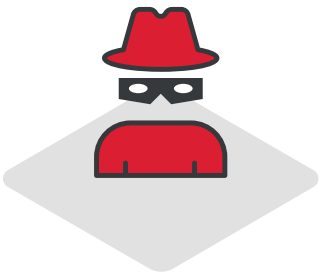
xantaro
connecting the world.

ALLES, WAS SIE ÜBER NIS2 WISSEN MÜSSEN

Whitepaper

Verschärfte Cybersecurity-Pflichten für mehr als 30.000 Unternehmen in Deutschland ab Oktober 2024



In einer zunehmend digitalisierten Welt sind Cyber-Bedrohungen allgegenwärtig. Kritische Infrastrukturen und Unternehmen geraten verstärkt ins Visier von Cyberkriminellen und politisch motivierten Angriffen. Damit gewinnt der Schutz dieser Systeme immer größere Bedeutung.

Die EU hat bereits 2016 mit der ersten NIS-Richtlinie (NIS1) darauf reagiert, um die Cybersecurity-Standards in Europa zu stärken und zu harmonisieren.

Doch die Bedrohungslage hat sich drastisch verschärft, sodass 2023 die NIS2-Richtlinie verabschiedet wurde, um Sicherheitsstandards noch umfassender und verpflichtender zu gestalten.

Laut der Digital Trust Studie von PwC von 2024 erlitten 70% der befragten Unternehmen in den vergangenen drei Jahren Verluste in Höhe von bis zu 20 Millionen US-Dollar durch Sicherheitslücken.

Das ist ein Beleg, dass die Cyber-Attacken immer effektiver werden - offensichtlich unterschätzen Unternehmen noch immer die Risiken und schützen ihre IT-Infrastruktur nur unzureichend gegen Angriffe von außen.

Die Mitgliedstaaten waren verpflichtet, die NIS2-Richtlinie bis Oktober 2024 in nationales Recht zu überführen. In Deutschland wurde die gesetzliche Umsetzung jedoch verzögert und es existiert bisher nur ein Referentenentwurf des Bundesinnenministeriums (BMI), der weitreichende Auswirkungen auf Unternehmen und deren Führungsebene haben wird. Besonders hervorzuheben ist die persönliche Haftung von Geschäftsführer*innen für unzureichende Cybersecurity-Maßnahmen. Erst nach der Bildung einer neuen Bundesregierung kann das NIS2-Umsetzungsgesetz final verabschiedet werden.

NIS2: Fakten im Überblick

Die Abkürzung „NIS“ steht für „Network and Information Security“. Die NIS2-Richtlinie wurde am 7. Dezember 2022 im EU-Amtsblatt veröffentlicht und trat am 16. Januar 2023 in Kraft.

Ein zentrales Ziel dieser Richtlinie ist es, die Cyber- und Informationssicherheit von Unternehmen und Institutionen der EU-Mitgliedsstaaten zu regulieren und so die Sicherheit im digitalen Raum zu verbessern. Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese Richtlinie in nationales Recht umsetzen.

Die NIS2-Richtlinie erweitert im Vergleich zur NIS1 die Anforderungen an die Cybersicherheit und die damit verbundenen Sanktionen, um das Sicherheitsniveau in den Mitgliedstaaten zu vereinheitlichen und zu verbessern. Sie enthält strengere Vorschriften für verschiedene Sektoren.

Unternehmen und Organisationen werden unter anderem verpflichtet, sich mit Themen wie Cyber-Risikomanagement, Kontrolle und Überwachung sowie Umgang mit Zwischenfällen und Geschäftskontinuität nachweisbar auseinanderzusetzen.

Endgültige Umsetzung und Auswirkungen auf Unternehmen

Nach der Bundestagswahl 2025 laufen noch die Koalitionsverhandlungen, wodurch die endgültige Umsetzung von NIS2 als nationales Gesetz weiterhin offen ist. Die möglichen Konsequenzen für Unternehmen, je nach Ausgang der Verhandlungen:

Strengere behördliche Kontrollen und Sanktionen:

- Das BSI erhielt erweiterte Prüfkompetenzen zur Durchsetzung der Vorschriften.
- Die Sanktionen für Verstöße wurden erhöht, mit besonderem Fokus auf personenbezogene Haftung der Unternehmensleitung.

Verlängerte Übergangsfristen für kleinere Unternehmen:

- Unternehmen mit weniger als 250 Mitarbeitern erhielten eine Übergangsfrist bis 2026 zur vollständigen Implementierung.

Erweiterung auf neue Technologien:

- Die Richtlinie wurde auf Cloud-Dienste, IoT-Sicherheit und KI-basierte Systeme ausgeweitet.

Fazit: Verschärfte Anforderungen und regulatorische Entwicklungen

Die NIS2-Richtlinie betrifft eine Vielzahl von Unternehmen in kritischen und essenziellen Sektoren. Sie definiert umfassendere Anforderungen und legt neue Berichtspflichten sowie drastischere Sanktionen fest.

Trotz der Verzögerungen auf nationaler Ebene ist die NIS2-Umsetzung verbindlich und endgültig in Kraft. Unternehmen, die sich auf eine spätere Umsetzung verlassen, müssen unter hohem Zeitdruck Maßnahmen umsetzen, um Bußgelder, Haftungsrisiken und operative Risiken zu vermeiden.

Wer frühzeitig Sicherheitsmaßnahmen implementiert, profitiert von einer besseren Position gegenüber regulatorischen Anforderungen und Cyber-Bedrohungen.

„Wesentliche Einrichtungen" gemäß NIS2-Richtlinie

NIS2-Sektoren	Inhalt	KRITIS
Energie	Elektrizität Fernwärme Erdöl Erdgas Wasserstoff	Energie
Transport	Luftverkehr Schienenverkehr Schifffahrt Straßenverkehr	Transport/Verkehr
Bankwesen	Kreditinstitute	Finanzwesen
Finanzmärkte	Handelsplätze Zentrale Gegenpartien	Finanzwesen
Gesundheit	Gesundheitsdienstleister EU Labore Medizinforschung Pharmazeutik Medizingeräte	Gesundheit
Trinkwasser	Wasserversorgung	Wasser
Abwasser	Abwasserentsorgung	Wasser
Digitale Infrastruktur	Internet-Knoten (IXP) DNS (ohne Root) TLD Registries Cloud Provider Rechenzentren CDNs Vertrauensdienste (TSP) Elektronische Kommunikation	IT tw. TKG
IKT-Dienstleitungs-management	Managed Service Providers Managed Secrurity Service Providers (B2B)	-
Öffentliche Verwaltung	Zentralregierung Regionale Regierung	-
Weltraum	Boden-Infrastruktur	tw. Transport

„Wichtige Einrichtungen" gemäß NIS2-Richtlinie

NIS2-Sektoren	Inhalt	KRITIS
Post und Kurier	Postdienste	tw. Transport
Abfall	Abfallbewirtschaftung	Entsorgung
Chemikalien	Produktion, Herstellung und Handel	UBI (3)
Lebensmittel	Produktion, Verarbeitung und Vertrieb	Ernährung
Industrie (Herstellung) *NACE-Kategorien*	Medizinprodukte und In-vitro DV (Computer) Elektronik, Optik Elektrische Ausrüstung Maschinenbau Kraftwagen und Teile Fahrzeugbau	tw. UBI (2)
Digitale Dienste	Marktplätze Suchmaschinen Soziale Netzwerke	tw. TMG
Forschung	Forschungsinstitute	-

NIS2 stellt sicher, dass die Stärkung der Cybersicherheit für eine Vielzahl von Unternehmen in ganz Europa zur Pflicht wird.

Ausnahmen von NIS2 betreffen auch kleinere Unternehmen

Unabhängig von der Firmengröße oder dem Umsatz können bestimmte Ausnahmen gelten. Dies betrifft Unternehmen, die kritische Tätigkeiten ausüben, Bedeutung für die öffentliche Ordnung haben oder bei einem Ausfall Systemrisiken bzw. grenzüberschreitende Folgen verursachen.

Solche Unternehmen unterliegen auch dann den NIS2-Vorschriften, wenn sie weniger als 50 Mitarbeiter beschäftigen oder einen Jahresumsatz von unter 10 Millionen Euro erzielen.

Unter bestimmten Ausnahmen kann ein Unternehmen andererseits vollständig von den Anforderungen der NIS2 befreit sein.

Welche Unternehmen fallen nicht unter NIS2?

Unternehmen und Institutionen, die in sensiblen Bereichen wie Verteidigung, nationale Sicherheit, öffentliche Sicherheit und Strafverfolgung tätig sind, unterliegen nicht den Bestimmungen der NIS2-Richtlinie.

Diese Ausnahmeregelung gilt ebenfalls für Justizbehörden, Parlamente und Zentralbanken. Diese Einrichtungen haben spezifische Sicherheitsanforderungen und -richtlinien, die in der Regel separat geregelt sind und daher nicht in den Anwendungsbereich der NIS2 fallen.

Dieser Ausschluss berücksichtigt die besondere Rolle und die spezifischen Sicherheitsanforderungen dieser Institutionen, die oft mit nationalen Sicherheitsinteressen und rechtlichen Kompetenzen verbunden sind.

Welche Anforderungen stellt die NIS2 an Unternehmen?

Die von NIS2 betroffenen Unternehmen müssen eine Reihe von Anforderungen erfüllen und umfangreiche Maßnahmen ergreifen, um mit der Richtlinie konform zu sein.

Dies umfasst die Implementierung geeigneter Sicherheitsmaßnahmen, die nachfolgend kurz beschrieben werden:

Unternehmensrichtlinien für Informationssicherheit aufsetzen

Unternehmen sind verpflichtet, Richtlinien für Risiken und Informationssicherheit zu entwickeln und umzusetzen. Diese Richtlinien dienen als Leitfaden für den Umgang mit Cyber-Sicherheitsrisiken und gewährleisten, dass angemessene Schutzmaßnahmen ergriffen werden.

Interne Trainings für Cybersecurity-Hygiene durchführen

Die NIS2-Richtlinie schreibt auch vor, dass Unternehmen ihre Mitarbeiter in Sachen „Cybersicherheits-Hygiene" schulen müssen. Die Cybersicherheits-Hygiene Maßnahmen zielen darauf ab, Cyber-Bedrohungen zu minimieren und das Risiko von Sicherheitsvorfällen zu reduzieren.

Typische Beispiele hierfür sind die Erkennung von Phishing-E-Mails, das sichere Passwortmanagement, sichere Authentifizierungsverfahren und das Bewusstsein für weitere Cyberbedrohungen oder Social-Engineering-Techniken zu schärfen. Generell werden in solchen Schulungen bewährte Verfahren im Umgang mit sensiblen Daten und der sicheren Nutzung von IT-Systemen vermittelt.

Risikomanagement auf- und ausbauen

Unternehmen, die als wesentliche oder wichtige Einrichtungen eingestuft werden, müssen angemessene technische, operative und organisatorische Maßnahmen ergreifen, um Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu kontrollieren und die Auswirkungen von Sicherheitsvorfällen zu minimieren, wie es in der NIS2-Richtlinie gefordert ist.

Das Ziel eines einheitlichen Risikomanagements besteht darin, dass Unternehmen potenzielle Bedrohungen und Schwachstellen in ihren Netz- und Informationssystemen frühzeitig erkennen können. Dies umfasst interne und externe Bedrohungen wie Cyberangriffe, Datenschutzverletzungen, Systemausfälle und menschliches Versagen.

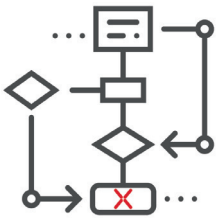
Sichere Authentifizierungsverfahren installieren

In der Informationssicherheit steht die Wahrung der Vertraulichkeit im Mittelpunkt. Es ist unerlässlich, dass ausschließlich autorisierte Personen Zugriff auf sensible Informationen wie Projektdaten haben.

Unternehmen sollten daher nach Möglichkeit auf Multi-Faktor-Authentifizierung und Single-Sign-On (SSO) zurückgreifen, um die Sicherheit ihrer Zugangsmechanismen zu erhöhen und unbefugten Zugriff zu vermeiden.

Business Continuity sicherstellen

Business Continuity bezieht sich auf die Fähigkeit eines Unternehmens, seine kritischen Geschäftsprozesse aufrechtzuerhalten oder schnell wiederherzustellen, selbst wenn unvorhergesehene Ereignisse oder Katastrophen eintreten. Die Unternehmen sind verpflichtet, geeignete Maßnahmen im Bereich Business Continuity Management (BCM) einzuführen, um die Funktionsfähigkeit der essenziellen Dienstleistungen selbst bei einem Cyber-Sicherheitsvorfall gewährleisten zu können.



Zum Business Continuity Management (BCM) gehören verschiedene Maßnahmen und Prozesse, die darauf abzielen, die Geschäftskontinuität eines Unternehmens sicherzustellen.

Dazu gehören unter anderem:

- Risikoanalyse und Risikomanagement
- Business Impact Analysis (BIA): Bewertung der Auswirkungen von Störungen oder Ausfällen auf die kritischen Geschäftsprozesse und -aktivitäten.
- Entwicklung von Notfallplänen und -verfahren
- Implementierung von Backups und Datensicherungen
- Schulungen und Awareness-Programme der Mitarbeiter über Notfallverfahren, Krisenmanagement und deren Rollen und Verantwortlichkeiten im Business Continuity Management.
- Regelmäßige Überprüfung der Notfallpläne und -verfahren durch Tests, Übungen und Audits.

Informations-Sicherheitsstandards in Kunde-Lieferant-Beziehungen gewährleisten

Ein wesentlicher Aspekt der NIS2-Anforderungen betrifft die Sicherheit entlang der Lieferkette. Unternehmen sind dazu verpflichtet zu gewährleisten, dass ihre Geschäftspartner und Dienstleister angemessene Sicherheitsvorkehrungen für ihre Informationssysteme treffen.

Hierbei kann die Festlegung von Sicherheitsanforderungen in vertraglichen Vereinbarungen eine Rolle spielen. Zudem sind Zertifizierungen von großer Bedeutung, um die Einhaltung von Standards nachzuweisen.

Ein Beispiel dafür wäre das TISAX®-Label als ein grundlegendes Erfordernis für Zulieferer in der Automobilbranche. Das Ziel dieses Standards besteht darin, zu verhindern, dass bösartige Interessenten durch Angriffe auf die Informationssysteme von Zulieferern Zugriff auf sensible Informationen großer Automobilhersteller erlangen.

Verschlüsselte Kommunikation intern und extern nutzen

Gemäß der NIS2-Richtlinie ist es entscheidend, dass die betroffenen Unternehmen verschlüsselte Sprach-, Video- und Textkommunikation implementieren, um die Vertraulichkeit und Integrität von Kommunikationsinhalten zu sichern.

Notfall-Kommunikationssystem aufbauen

Unternehmen gesicherte Notfall-Kommunikationssysteme implementieren, um im Falle eines Sicherheitsvorfalls oder einer Krise eine effektive Kommunikation und Koordination sicherzustellen.

Hier sind einige Beispiele für Notfallkommunikationssysteme:

- Massenbenachrichtigungssysteme
- Krisenkommunikations-Apps
- Virtuelle Befehlszentren zur Koordination von Reaktionen auf Notfälle
- Web-basierte Kollaborationsplattformen wie Microsoft Teams oder Slack

Diese Systeme ermöglichen eine effektive Kommunikation und Koordination während eines Notfalls, um schnell auf die Situation zu reagieren und die Sicherheit von Mitarbeitern und anderen Beteiligten zu gewährleisten.

Ihre Checkliste – unsere Kompetenz

Die wesentlichen und wichtigen Unternehmen sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden.

Was ändert sich durch NIS2 an der Meldepflicht?

Zuerst muss ein Unternehmen seine Einordnung in die verschiedenen Kategorien (siehe oben „wesentliche Einrichtungen“ oder „wichtige Einrichtungen“) vornehmen und sich innerhalb von drei Monaten nach der Identifizierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren lassen.

„Besonders wichtige Einrichtungen“ sind zudem verpflichtet, sich am Informationsaustausch über die zentrale Austauschplattform des BSI (BISP) zu beteiligen. Oft übernehmen Datenschutzbeauftragte diese Meldepflichten.

Zusätzlich zur Registrierung bei der zuständigen Behörde müssen die Unternehmen, die als Akteure kritischer Infrastrukturen zugeordnet werden, unverzüglich ihre nationale Cybersecurity-Behörde über signifikante Störungen, Vorfälle und Bedrohungen ihrer kritischen Dienstleistungen informieren.

Für den Meldevorgang ist ein dreistufiger Prozess vorgesehen:

1 Innerhalb von 24 Stunden, nachdem ein Vorfall aufgetreten ist, muss ein vorläufiger Bericht übermittelt werden.

2 Innerhalb von 72 Stunden muss ein vollständiger Bericht mit der ersten Bewertung des Vorfalls erstellt werden.

3 Innerhalb eines Monats soll ein Abschlussbericht vorliegen, der den Vorfall, Art der Bedrohung und alle Auswirkungen detailliert beschreibt.

Um diesen Prozess zu gewährleisten, sollen die Unternehmen intern geeignete Informationssicherheits-Managementsysteme (ISMS) betreiben. ISO 27001 ist ein international anerkannter Standard für Informationssicherheitsmanagement (ISMS). Er legt Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems fest.

Sanktionsmaßnahmen bei NIS2 auf bis zu 10 Mio. Euro gestiegen

NIS2 sieht auch eine Verschärfung der Sanktionen bei Verstößen vor. Bei „wesentlichen Einrichtungen“ können Bußgelder bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes betragen.

Für „wichtige Einrichtungen“ beträgt das maximale Bußgeld 7 Millionen Euro oder 1,4 Prozent des weltweiten Jahresumsatzes.

Management haftet mit Privatvermögen

Im Referentenentwurf des Bundesinnenministeriums ist auch vorgesehen, dass Geschäftsführer und andere leitende Organe von Unternehmen persönlich mit ihrem Privatvermögen haften, um die Einhaltung der Risikomanagement-Maßnahmen sicherzustellen.

MIT NIS2 BETRETEN UNTERNEHMEN KEIN TRIVIALES TERRAIN.

Gehört Ihr Unternehmen zu den betroffenen Einrichtungen?

Verlassen Sie sich auf das Know-how von Xantaro, um Ihre Sicherheitsstrategie zu optimieren und Ihr Unternehmen erfolgreich auf die neuen Herausforderungen vorzubereiten.

Ihr Kontakt bei Xantaro

Oliver M. Meißner-Gutberlet
Senior Named Account Manager Enterprise Sales
+49 (0)89 1891 71 345
+49 (0)160 49 14 723
omg@xantaro.net

Die Xantaro Gruppe

Die Xantaro-Gruppe mit den Mitgliedsunternehmen NetDescribe und nicos ist ein international führender Solution Provider in den Bereichen High-Performance-Netzwerke, IT-Sicherheitslösungen und Managed Services für Carrier, Service Provider und Industriekunden.

Xantaro Deutschland GmbH
T +49 (0)40 413 4980 I contact@xantaro.net I www.xantaro.net

xantaro
connecting the world.