rubrik

NIS2-LEITFADEN

NIS2-Richtlinie

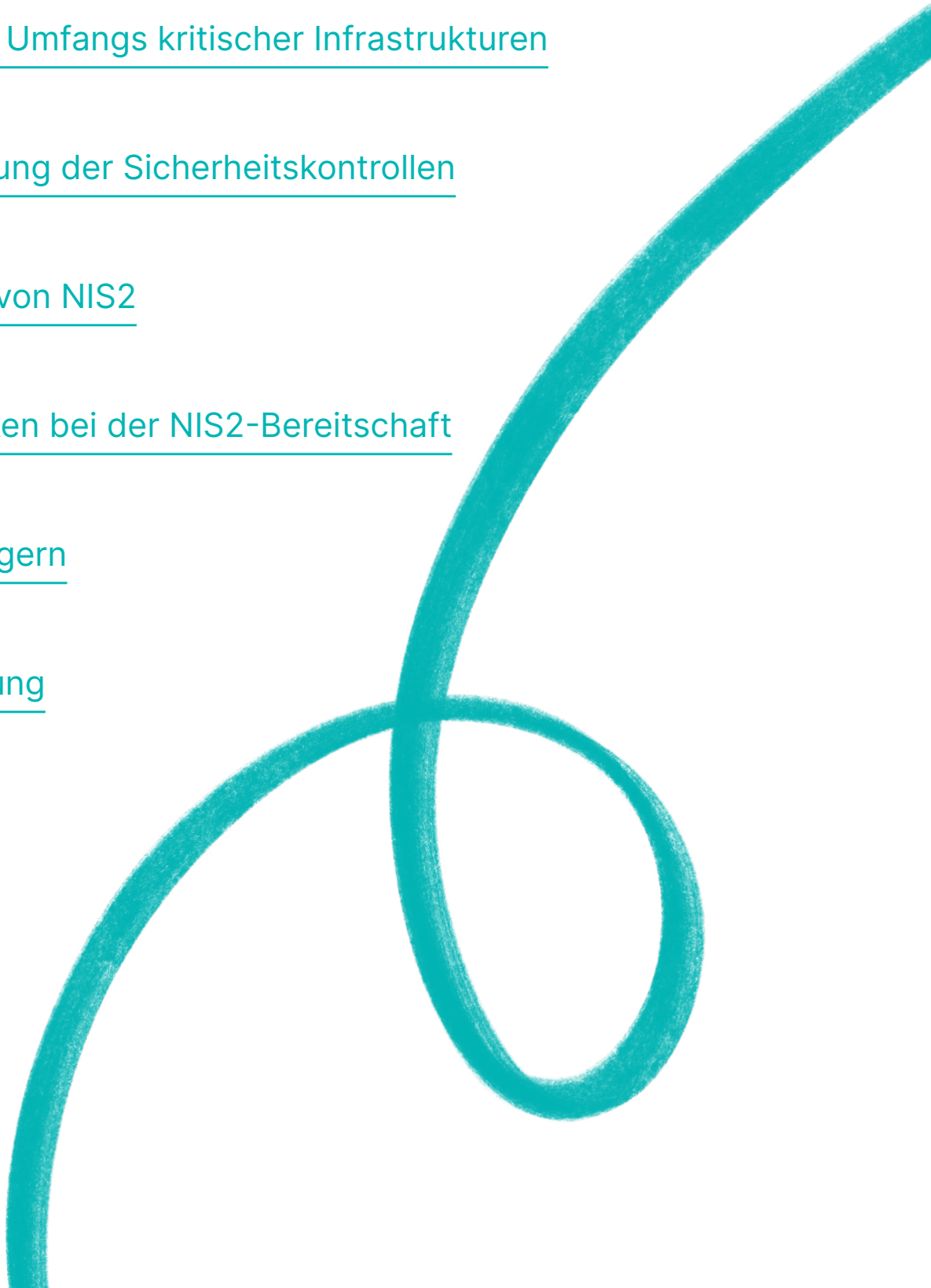
rubrik

Angesichts der rasanten Zunahme von Cyber-Bedrohungen, technologischen Entwicklungen, globalen Pandemien und Naturkatastrophen stehen unsere lebenswichtigen kritischen Infrastruktursysteme unter extremem Druck.

Die Aktualisierung der Richtlinien zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (Security of Networks & Information Systems Regulations, NIS2) ist die jüngste in einer Reihe von Datenschutzverordnungen, die speziell für Unternehmen gelten, die Geschäfte mit Unternehmen in der Europäischen Union (EU) und im Vereinigten Königreich tätigen, die als Bestandteil der kritischen Infrastruktur eines Landes gelten.

Dieser Leitfaden für den schnellen Einstieg in NIS2 hilft Ihnen dabei, das Framework zu nutzen, um Ihre Cyber-Resilienz zu verbessern.

Inhaltsverzeichnis



NIS2 ersetzt NIS

Die NIS-Richtlinie war das erste EU-weite Gesetz zur Cyber-Sicherheit. Sie verfolgte das Ziel, für ein hohes allgemeines Cyber-Sicherheitsniveau für Unternehmen, die in der Europäischen Union tätig sind, zu sorgen. Sie hat zwar die Cyber-Sicherheitskapazitäten in Unternehmen erhöht, ihre Umsetzung erwies sich jedoch als schwierig, was zu einer Fragmentierung auf verschiedenen Ebenen unter den in der EU ansässigen Unternehmen führte.

Die EU-Kommission stellte Mängel in der NIS-Richtlinie fest, darunter:

- Unzureichende Cyber-Resilienz von EU-Unternehmen
- Uneinheitliche Resilienz in den EU-Mitgliedstaaten und Sektoren
- Mangelndes gemeinsames Verständnis von Bedrohungen
- Fehlende gemeinsame Reaktion auf Krisen

Als Reaktion auf die wachsende Bedrohung durch die Digitalisierung und die Zunahme von Cyber-Angriffen, hat die EU die NIS-Richtlinie durch die NIS2-Richtlinie ersetzt, um die Sicherheitsanforderungen zu verschärfen, die Sicherheit von Lieferketten zu verbessern, Meldepflichten zu straffen und strengere Aufsichtsmaßnahmen und Durchsetzungsanforderungen einzuführen, einschließlich vereinheitlichter Sanktionen für in der EU tätige Unternehmen. [Quelle]

„Die NIS2-Richtlinie ist für die europäische Cyber-Sicherheit das, was die DSGVO für den europäischen Datenschutz ist.“

RICHARD CASSIDY, FIELD CISO RUBRIK

Ausweitung des Umfangs kritischer Infrastrukturen

Die NIS2-Richtlinie legt strengere Cyber-Sicherheitsverpflichtungen für Risikomanagement, Meldepflichten und den Informationsaustausch fest. Die Anforderungen betreffen unter anderem die Reaktion auf Vorfälle, die Sicherheit der Lieferkette, Verschlüsselung und die Offenlegung von Schwachstellen. Mit der NIS2-Richtlinie wird auch die Zahl der abgedeckten Branchen von 7 auf 15 Sektoren erweitert und die Kategorien „Wesentliche Einrichtungen“ (Essential Entities) und „Wichtige Einrichtungen (Important Entities) werden eingeführt.

„ Die NIS2-Richtlinie betrifft ein breiteres Spektrum an Einrichtungen, die in kritischen Infrastrukturen tätig sind.“

RICHARD CASSIDY, FIELD CISO RUBRIK

	Wesentliche Einrichtungen	Wichtig
Unternehmensgröße	• 250+ Mitarbeiter ODER • Jahresumsatz von 50 Mio. € oder Bilanz von 43 Mio. €	• 50+ Mitarbeiter ODER • Jahresumsatz von 10 Mio. € oder Bilanz von 10 Mio. €
Branche	• Energie • Transport • Bankensektor • Finanzmarktinfrastrukturen • Gesundheitswesen • Trinkwasser • Abwasser • Digitale Infrastruktur • ICT-Service-Management • Einrichtungen der öffentlichen Verwaltung (ohne Justiz, Parlament und Zentralbanken)	• Post- und Kurierdienste • Abfallwirtschaft • Herstellung, Produktion und Vertrieb von Chemikalien • Lebensmittelproduktion, -verarbeitung und -vertrieb • Fertigung von medizinischen Geräten und elektronischen Produkten sowie Transport • Digitale Dienstleister • Forschung

Jede Vorschrift birgt das Risiko von Sanktionen, wenn sie nicht eingehalten wird. Auch wenn die Höhe der Geldstrafen einschüchternd wirken kann, sollten Unternehmen bei der Ausrichtung an NIS2 die Kosten und Auswirkungen beim Einhalten der Vorschriften gegen die Kosten abwägen, die mit einer Nichteinhaltung einhergehen würden. Die Höhe der Geldstrafe ist von der jeweiligen Kategorie abhängig.

	Wesentliche Einrichtungen	Wichtig
Bußgeldhöhe	• Mindestens 10.000.000 € oder 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.	• Eine maximale Geldstrafe von mindestens 7.000.000 € oder mindestens 1,4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.

NIS2: Verschärfung der Sicherheitskontrollen

Viele Regelungen und Rahmenwerke können schwerfällig und umständlich erscheinen und ihre Einhaltung kann ressourcenintensiv sein. Dabei liefern sie nicht unbedingt den Mehrwert, den sich Unternehmen erhoffen. Durch NIS2 können Unternehmen ihre Sicherheitskontrollen verschärfen.

> „Diese europäische Richtlinie wird rund 160.000 Einrichtungen dabei helfen, ihre Sicherheitsmaßnahmen zu verschärfen.“

BART GROOTHUIS, MITGLIED DES EUROPÄISCHEN PARLAMENTS

Der Schwerpunkt bei NIS2 besteht nicht nur darin, die bestehende NIS-Richtlinie zu verbessern. NIS2 legt zudem den Fokus auf einige sehr spezifische Elemente, die wir uns etwas genauer ansehen sollten. Nehmen wir als Beispiel den Umgang mit Bedrohungen und Vorfällen. Je schneller Sie im Falle einer Datenschutzverletzung Informationen mit Ihren Kollegen und anderen Organisationen austauschen können, um eine behördenübergreifende Reaktion auf einen Vorfall zu ermöglichen, desto besser ist Ihre Cyber-Resilienz. Für den sektorübergreifenden Informationsaustausch ist dies ein großer Fortschritt. Zuvor betrafen viele Rechtsvorschriften den FinTech- und Finanzbereich oder waren zu weit gefasst und zu schwer zu definieren. Mit NIS2 wird der Schwerpunkt auf Schlüsselbereiche gelegt, die Unternehmen greifbare Vorteile bringen werden. [Quelle]

NIS2 ist ein praxisorientiertes, prägnantes und konvergentes Regelwerk, das Unternehmen in die Lage versetzt, ihre Daten in Schlüsselbereichen umfassend zu verwalten, sich wesentlich effektiver gegen Cyber-Bedrohungen zu verteidigen und nach einem größeren Cyber-Vorfall schnell zur betrieblichen Effizienz zurückzukehren.

Die fünf Säulen von NIS2

NIS2 unterteilt Branchen in bestimmte Kategorien: Wesentliche und wichtige Einrichtungen. Dies ändert nichts an den Punkten, denen Sie entsprechen müssen, um NIS2 zu erfüllen, es gibt jedoch Schwerpunktbereiche, je nachdem, welcher Kategorie Sie angehören.

NIS2 enthält mehr als 46 Artikel (die Sie hier finden). Im Großen und Ganzen lassen sie sich zu fünf Hauptsäulen zusammenfassen:

NIS2				
Sicherheits-anforderungen	Umgang mit Vorfällen	Geschäfts-kontinuität	Überwachung, Prüfung und Tests	Einhaltung internationaler Standards

Die größte Schwerpunktverlagerung für Unternehmen aus technologischer und prozessualer Sicht sehen wir bei den folgenden Säulen: Umgang mit Vorfällen, Überwachung, Prüfung und Tests sowie Servicekontinuität. Allein diese drei Säulen enthalten viele neue Funktionen und Aspekte, die Unternehmen zwingen werden, ihre Strategien in Bezug auf Cyber-Sicherheit und Cyber-Resilienz sowie die Art und Weise zu überarbeiten, wie sie Daten nach außen weitergeben.

Im Bereich Cyber-Sicherheit verfügen Unternehmen typischerweise oft über sehr komplexe und weitreichende Sicherheits-Ökosysteme, aber diese Ökosysteme sind isoliert und auf die Geschäftsabläufe abgestimmt. Mit NIS2 müssen Unternehmen die Art und Weise, wie sie Daten mit europäischen Aufsichtsbehörden und anderen Organisationen austauschen, die Teil von NIS2 sind, wesentlich verbessern. Dieses Maß an Informationsaustausch wird die Stärkung der operativen Resilienz und der operativen Wiederherstellung unterstützen.

„Ransomware und andere Cyber-Bedrohungen plagen Europa schon viel zu lange. Wir müssen handeln, um unsere Unternehmen und Regierungen sowie die Gesellschaft widerstandsfähiger gegen Cyber-Angriffe zu machen."

BART GROOTHUIS,
MITGLIED DES EUROPÄISCHEN PARLAMENTS

Die großen Lücken bei der NIS2-Bereitschaft

Wo bestehen in Unternehmen die größten Lücken im Hinblick auf ihre NIS2-Bereitschaft?

Bei der Betrachtung der fünf Säulen der NIS2-Richtlinie stellen wir fest, dass die meisten Unternehmen – wenn nicht sogar alle – über ein sehr uneinheitliches Ökosystem verfügen, wenn es darum geht, wie sie Sicherheitsanforderungen handhaben, von der Erstmeldung von Vorfällen über den Umgang mit diesen bis hin zum Informationsaustausch mit anderen Unternehmen.

Säule 1: Die Sicherheitsanforderungen sind die erste Säule. Die meisten Unternehmen erfüllen diese Anforderungen zu einem hohen Grad.

Säule 2: Der Umgang mit Vorfällen ist die zweite Säule. Auch diese Anforderungen erfüllen viele Unternehmen bereits. Unabhängig davon, ob die Handhabung von Vorfällen intern erfolgt oder ob ein externer Dienstleister damit betraut wird: Die meisten Unternehmen haben in diesem Bereich bereits viel Erfahrung gesammelt. Sie werden feststellen, dass Sie Ihre Tools und Richtlinien für die Handhabung von Vorfällen an die Anforderungen der NIS2-Richtlinie anpassen müssen, doch die meisten Unternehmen sollten bereits jetzt in der Lage sein, diese Anforderungen zu erfüllen.

Bei Säule 3, der Geschäftskontinuität, weist Ihr Unternehmen wahrscheinlich große Lücken auf. Sie werden Zeit und Ressourcen aufwenden müssen, um diese zu schließen. Viele Unternehmen verfügen aktuell noch nicht über alle erforderlichen Cyber-Resilienz-Kapazitäten. Dies liegt in den meisten Fällen daran, dass sie meinen, Daten-Backups seien gleichbedeutend mit Cyber-Resilienz, oder dass sie darauf vertrauen, dass ein Cloud-Service-Anbieter genügend Sicherheit bietet. Bei echter Cyber-Resilienz geht es darum, die eigene betriebliche Resilienz und den eigenen Wiederherstellungsplan zu testen und zu optimieren.

Bei Säule 4, Überwachung, Prüfung und Tests.

Bei Säule 5, der Einhaltung internationaler Standards, müssen Unternehmen den Fokus darauf legen, wie sie ihre Daten erfassen, woher die Daten stammen und wie diese Daten gemäß den Vorgaben des NIS2-Rahmens effektiv weitergegeben werden können.

„Wir müssen die kollektive Resilienz der kritischen Systeme stärken, die die Grundlage für unsere moderne Lebensweise bilden.“

MICHAEL ŠIMEČKA, MITGLIED DES EUROPÄISCHEN PARLAMENTS

Keine Zeit zu zögern

Am 17. Oktober 2024 endet die Frist, bis zu der Unternehmen die NIS2-Vorschriften einhalten müssen. Und machen Sie sich nichts vor: Jetzt ist die Zeit, Ihr Unternehmen auf Vordermann zu bringen. Bringt NIS2 also eine Generalüberholung Ihrer gesamten Cyber-Sicherheitsstruktur mit sich? Nicht unbedingt.

> „Müssen Sie zeitnah konform werden? Ja. Sie haben bis Oktober 2024 Zeit, um Ihr Unternehmen auf den neuesten Stand zu bringen“.

RICHARD CASSIDY, FIELD CISO RUBRIK

Die größte Herausforderung bei NIS2? Sie müssen sich daran halten. NIS2 ist nicht optional. Und Compliance beginnt auf Vorstandsebene. Der Vorstand muss die für die nächsten 12 bis 18 Monate geplanten Projekte sorgfältig prüfen und diese mit der NIS2-Richtlinie in Einklang bringen. Die Umsetzung von NIS2 kann als ein weiteres Projekt angesehen werden, das jedoch von entscheidender Bedeutung ist und sofort in Angriff genommen werden muss. Verstöße gegen diese Vorschriften werden mit Geldbußen, nicht monetären Rechtsbehelfen oder strafrechtlichen Sanktionen geahndet und können die Fähigkeit eines Unternehmens beeinträchtigen, mit anderen NIS2 -Einrichtungen in der Europäischen Union Geschäfte zu tätigen.

Die gute Nachricht? Viele bestehende und geplante IT-Projekte, die bereits angestoßen wurden, verfügen über integrierte Funktionen, um im Falle eines größeren Ausfalls oder eines Disaster-Recovery-Szenarios den gesamten Geschäftsbetrieb von Grund auf neu aufzubauen. Sie werden feststellen, dass Sie mit diesen Voraussetzungen viele Anforderungen in Verbindung mit NIS2 abdecken können. Um Ihre NIS2-Bereitschaft zu ermitteln, empfehlen wir die folgenden drei Schritte:

1. **NIS2-Geltungsbereich:** Bestimmen Sie, in welchen NIS2-Geltungsbereich und in welche Kategorie Ihr Unternehmen fällt und welche Geschäftsbereiche davon betroffen sind.
2. **NIS2-Abdeckung:** Bewerten Sie Ihre Sicherheitsmaßnahmen und -richtlinien und ändern Sie sie gegebenenfalls, um sie an die Anforderungen der NIS2-Richtlinie anzupassen.
3. **Gap-Analyse:** Analysieren und identifizieren Sie die Sicherheitsmaßnahmen und -richtlinien, die Sie noch benötigen, um NIS2-Konformität zu erreichen. Die Meldepflichten für Vorfälle in Bezug auf die Lieferkette sind ein Aspekt, mit dem man sich frühzeitig auseinandersetzen sollte, um bei der Anpassung an die Richtlinie nicht ins Hintertreffen zu geraten.

Tipp: Legen Sie den Fokus auf Anbieter in der Lieferkette – ein Bereich, der leicht übersehen wird und oft Zielscheibe von Angreifern ist.

Schlussbemerkung

Wichtig ist: Machen Sie sich bewusst, dass Sie die Anforderungen der NIS2-Richtlinie vielleicht schon heute weitgehend erfüllen. Und für diejenigen, die es noch nicht sind, werden die richtige Gap-Analyse und die Partnerschaften mit Technologie- und Serviceanbietern helfen, die Anforderungen relativ leicht zu erfüllen. Vergessen Sie nicht, dass die NIS2-Richtlinie als Hilfe gedacht ist. Machen Sie sie sich zunutze!

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com