



## NIS-2-Richtlinie: Wie Endian Sie bei der Umsetzung unterstützt

Die globale Wirtschaft ist immer stärker von digitalen Lösungen abhängig. Unterschiedliche Dienstleistungen und Sektoren sind zunehmend untereinander vernetzt und auf eine reibungslose Zusammenarbeit angewiesen. Diese Situation begünstigt eine schnell wachsende Bedrohungslandschaft für die Cybersicherheit: Jeder einzelne IT-Sicherheitsvorfall, selbst wenn er vorerst nur eine einzige Organisation betrifft, kann kaskadenartig auf andere Bereiche und Unternehmen übergreifen und damit negative Auswirkungen auf den gesamten EU-Binnenmarkt haben.

Die Europäische Union sah deshalb Handlungsbedarf und hat die NIS-2-Richtlinie (Directive on security of network and information systems) verabschiedet. Diese baut auf der ursprünglichen NIS-Richtlinie aus dem Jahr 2016 auf und verfolgt zwei wichtige Ziele: Zum einen soll sie für höhere Standards in der Netzwerk- und Informationssicherheit sorgen und zum anderen das Sicherheitsniveau in den EU-Mitgliedsstaaten angleichen, um die Cyber-Resilienz Europas insgesamt zu stärken.

Bis zum 17. Oktober 2024 haben die EU-Länder Zeit, die Richtlinie in nationales Recht zu überführen. In der EU tätige Unternehmen sollten sich daher schon jetzt mit der NIS2 auseinandersetzen, um zu klären, ob sie betroffen sind. Die EU schreibt nicht nur technische Maßnahmen vor, sondern einen Risikomanagementansatz, für dessen Implementierung ausreichend Zeit benötigt wird.

Dieser Beitrag bietet einen Überblick über die wichtigsten Eckpunkte der NIS2 und zeigt, wie Endian bei der Umsetzung der Anforderungen unterstützen kann.

Mit Endian haben Sie den idealen Partner für NIS2 an Ihrer Seite: Als IT-Security-Hersteller arbeitet Endian nach dem Prinzip "Security by Design" und verfügt über langjährige Erfahrung bei Digitalisierungsprojekten. Endian ist unabhängig, inhabergeführt und hat seinen Sitz im Herzen Europas.

## Wer ist betroffen?



**Wichtig:** Die Behörden teilen Ihnen nicht mit, ob Ihr Unternehmen zu den kritischen Sektoren nach NIS2 gehört. Sie müssen also selbst aktiv werden und anhand der Vorgaben beurteilen, ob die Richtlinie für Ihr Unternehmen oder Ihre Organisation relevant ist.

**Die NIS2 erweitert den Kreis der betroffenen Unternehmen:** Waren es bei der ersten NIS-Richtlinie nur acht Sektoren, sind es bei NIS2 bereits 18. Es wird unterschieden in "wesentliche" (Essential entities) und "wichtige" (Important entities) Sektoren:

### Essential entities: Wesentliche Sektoren



**Energie** (Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff)



**Gesundheitswesen** (Gesundheitsdienstleister, EU-Labore, Medizinforschung, Pharmazeutik, Medizingeräte)



**Transport** (Luft-, Schienen- und Straßenverkehr sowie Schifffahrt)



**Banken** (Kreditinstitute)



**Finanzwesen** (Handelsplätze und zentrale Gegenparteien)



**Trinkwasser** (Lieferanten und Versorger)



**Abwasser**



**Weltraumsektor**



**IKT-Dienstleistungsmanagement**



**Öffentliche Verwaltung** (Zentral und regional)



**Digitale Infrastruktur** (Internet-Knoten, DNS-Dienstanbieter, TLD-Namensregister, Cloud-Provider, Rechenzentren, Content Delivery Networks, Vertrauensdienste, Kommunikationsnetze und Kommunikationsdienste)

## Important Entities: Wichtige Sektoren

-  **Post- und Kurierdienste**
-  **Abfallwirtschaft**
-  **Chemikalien** (Produktion, Herstellung und Handel)
-  **Lebensmittel** (Produktion, Verarbeitung und Großhandel)
-  **Hersteller** (Medizinprodukte und In-vitro-Diagnostika, Computer, elektrische Ausrüstung, Optik, Maschinenbau, Kfz und Teile, Fahrzeugbau)
-  **Digitale Anbieter** (Online-Marktplätzen, Suchmaschinen, soziale Plattformen)
-  **Forschung**

## Größenregelung

Die NIS2 führt auch eine neue Größenregelung ein: Alle mittleren und großen Unternehmen in den genannten Sektoren fallen in den Anwendungsbereich. Das betrifft Unternehmen ab 50 Mitarbeitern oder 10 Millionen Euro Umsatz und zwar unabhängig von Leistung oder Schwellenwerten ihrer Anlagen. Gleichzeitig lässt die EU den Mitgliedstaaten einen gewissen Ermessensspielraum, kleinere Unternehmen mit einer besonders hohen Kritikalität ebenfalls zu den kritischen Sektoren zuordnen zu können.



## Maßnahmen

Die NIS2 beinhaltet strengere Vorschriften beim Risikomanagement. Unternehmen müssen ein angemessenes Sicherheitsniveau etablieren und nachweisen, dass sie Sicherheitsvorfälle verhindern, ermitteln und im Notfall darauf reagieren können.

Die umfangreichen Anforderungen lassen sich nicht nur über die Implementierung von technischen Lösungen erfüllen, sondern erfordern ebenso einen genauen Blick auf die Prozesse im Unternehmen.

Deshalb stellen wir an dieser Stelle vor, wie die Cybersecurity-Lösungen von Endian durch Leistungen von Beratungsunternehmen ergänzt werden können, um in allen Punkten der NIS2 zu entsprechen.

## Konzepte zur Risikoanalyse und der Sicherheit von Informationssystemen

Ausgangspunkt für alle weiteren Schritte ist die Erfassung des Ist-Zustandes. Richten Sie eine Task-Force ein, die den Status-quo ermittelt und den Handlungsbedarf herausarbeitet.

### Wie kann Endian hier helfen?

Bei Bedarf können hier unsere Systemintegratoren und Consultants unterstützen.

### Wie können Consultants hier helfen?

Um die aktuelle Situation zu bewerten und eine Zielvorstellung zu definieren, wird eine Soll-Ist-Analyse durchgeführt. Anschließend lassen sich anhand einer detaillierten Dokumentation geeignete Maßnahmen planen und umsetzen.

## Incident-Management

Mit einem strukturierten Incident-Management lassen sich die Auswirkungen einer Cyberattacke minimieren, um die Daten und Systeme Ihres Unternehmens zu schützen. Voraussetzung für ein erfolgreiches Incident-Management ist es, den Angriff überhaupt als solchen zu identifizieren.

### Wie kann Endian hier helfen?

Die Endian IoT-Security-Gateways sind mit mehreren Sicherheitsfunktionen ausgestattet, die Cyberangriffe erkennen und stoppen können: Die Deep Packet Inspection (DPI) analysiert die Datenpakete, die über ein Netzwerk verschickt werden. Anders als bei herkömmlichen Analysemethoden, die sich nur auf die Metadaten beschränken, findet bei DPI eine Analyse bis in die Anwenderebene statt und erkennt über 300 IT/OT Protokolle und 2000 Applikationen. Damit lässt sich der Normalzustand des Netzwerks ermitteln. Sollte sich eine Anomalie im Datenverkehr ergeben, wird dies mithilfe des Intrusion Detection Systems (IDS) erkannt. Falls es sich um einen Angriff handelt, greift das Intrusion Prevention System (IPS) ein, um ihn zu stoppen.

### Wie können Consultants hier helfen?

Consultants unterstützen dabei, geeignete Prozesse zu implementieren, um ein Incident-Management einzuführen. Dies umfasst den gesamten Lebenszyklus eines Vorfalls, beginnend mit präventiven Maßnahmen zur Vermeidung von Vorfällen, über die Erkennung und Reaktion bis hin zur Wiederherstellung der Systeme nach einem Vorfall. Die Schulung und Sensibilisierung von Mitarbeitern in der IT sowie in den Fachabteilungen ist ebenfalls ratsam.

## Geschäftskontinuität, Backup-Management und Notfallwiederherstellung, sowie Krisenmanagement

Unternehmen müssen Maßnahmen ergreifen, mit denen sich Geschäftsunterbrechungen verhindern lassen, die beispielsweise durch einen Systemausfall entstehen können.

### Wie kann Endian hier helfen?

Endian bietet mehrere Funktionen, mit denen sich Geschäftsunterbrechungen und Datenverlust verhindern lassen: Firewall sowie Deep Packet Inspection (DPI) ermöglichen die Abwehr von Cyberangriffen. Die Hochverfügbarkeitsfunktion (HA-System) stärkt die Resilienz, da hier ein zusätzliches EndianOS im Stand-by Modus zur Verfügung steht, das den Betrieb bei einem Systemausfall sofort übernehmen kann. Sollte es dennoch zu einer Kompromittierung der Systeme kommen, ermöglicht die Backup-Funktion eine schnelle Wiederherstellung.

### Wie können Consultants hier helfen?

Der Aufbau optimaler Prozesse und Geschäftsabläufe ist ein wichtiger Punkt, um die Resilienz zu stärken. Es gilt, Risiken zu identifizieren und geeignete Maßnahmen zur Risikominderung umzusetzen, damit der Geschäftsbetrieb stabil bleibt. Gemeinsam mit dem Unternehmen wird eine Business Impact Analyse durchgeführt, um die Auswirkungen von potenziellen Störungen auf den Betrieb zu bewerten. Die Einführung eines Business Continuity Managements sorgt dafür, dass ein Unternehmen auch in Krisensituationen handlungsfähig bleibt.

## Sichere Lieferkette

NIS2 bezieht auch die Sicherheit von Lieferketten und Lieferantenbeziehungen mit ein, denn ohne sichere Zulieferer lässt sich keine umfassende IT-Sicherheit herstellen. Mit der NIS-2-Richtlinie sind einzelne Unternehmen dazu aufgefordert, die IT-Sicherheitsrisiken in den Lieferketten und Lieferantenbeziehungen anzugehen.

### Wie kann Endian hier helfen?

EndianOS schützt die Netzwerke vor Sicherheitsbedrohungen, die von externen Zulieferern ausgehen. Die Endian Firewall sowie die DPI verhindern das Eindringen von Malware über Lieferanten und können Cyberangriffe damit abblocken. Dank des integrierten Virenschutzes sind die Netzwerke auch vor weiterer Schadsoftware geschützt.

### Wie können Consultants hier helfen?

Das Sicherheitsniveau der Zulieferer lässt sich über verschiedene Methoden verifizieren. Gezielte Überprüfungen und Self-Assessments stellen sicher, dass die Lieferanten angemessene Sicherheitsvorkehrungen treffen und den Anforderungen der Kunden entsprechen. Eine strukturierte und effiziente Verwaltung aller Dokumente und Verträge ist eine wertvolle Unterstützung, um die getroffenen Vereinbarungen im Blick zu behalten. Der Aufbau eines effektiven Dokumenten- und Vertragsmanagements sowie der damit verbundenen Prozesse hilft, einen reibungslosen Ablauf zu gewährleisten.

## Beschaffung

Die NIS-2-Richtlinie schreibt vor, dass Unternehmen für Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzen und Informationssystemen sorgen müssen. Die Behandlung und Offenlegung von Schwachstellen sind hier mit eingeschlossen. Es wird also noch wichtiger, zuverlässige Lieferanten für die IT-Infrastruktur und Netzwerksysteme zu wählen.

### Wie kann Endian hier helfen?

Endian entwickelt seine Produkte nach dem Prinzip „Security by Design“, d.h. Sicherheit wird von Anfang an mitgedacht und eingeplant. Die Endian Secure Digital Platform entspricht den Vorgaben der IEC 62443, der Norm für industrielle Cybersicherheit. Zudem ist Endian ein unabhängiger, europäischer Hersteller.

### Wie können Consultants hier helfen?

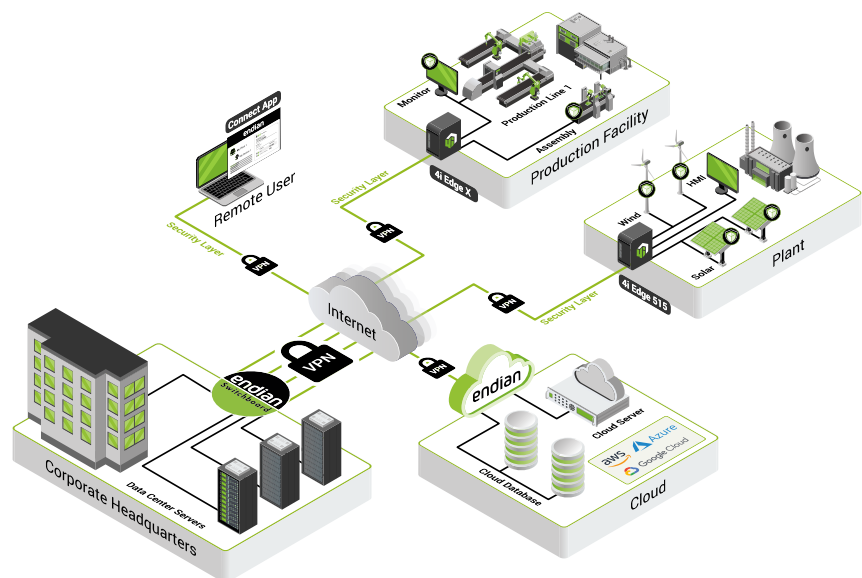
Alle Systeme müssen permanent aktualisiert werden, um vor Cyberattacken sicher zu sein. Für die regelmäßige Aktualisierung und das Patching der Systeme, Anwendungen und Infrastruktur ist eine strukturierte und gut koordinierte Vorgehensweise wichtig. Consultants bauen mit den Unternehmen ein effektives Patch- und Update-Management auf und führen die notwendigen Dokumentationsprozesse ein. Außerdem unterstützen sie bei der Entwicklung von Richtlinien und Prozessen, um sicherzustellen, dass Updates zeitnah und unter Berücksichtigung von potenziellen Auswirkungen implementiert werden.

## Kryptographie

Das Unternehmen leitet geeignete Schritte ein, um die Vertraulichkeit der Netzwerkkommunikation und des Datenzugriffs zu gewährleisten. Hierfür müssen Strategien und Prozesse für den Einsatz von Kryptographie entwickelt und, wo immer notwendig, Verschlüsselungsverfahren eingesetzt werden.

### Wie kann Endian hier helfen?

Über ein Virtual Private Network (VPN) wird die Kommunikation auf den Netzwerken verschlüsselt. Dank der Verwendung moderner kryptographischer Algorithmen ist der Datenaustausch jederzeit abgesichert.



### Wie können Consultants hier helfen?

Bei der Entwicklung von kryptografischen Strategien und Richtlinien für die individuellen Anforderungen eines Unternehmens können Consultants einen wertvollen Beitrag leisten. Um im Rahmen einer generellen Sicherheitsstrategie ein hohes Sicherheitsniveau zu erreichen, können sie helfen, kryptografische Verfahren in Geschäftsprozesse und IT-Systeme zu integrieren.

## Zugriffskontrolle

Das Unternehmen definiert Rechte und Rollen für den Zugriff auf seine Infrastruktur.

### Wie kann Endian hier helfen?

Das Management-Tool Endian Switchboard bietet ein sehr granulares Rollen- und Berechtigungsmanagement für den Zugriff auf verteilte Ressourcen gemäß der Zero Trust Policy. Gleichzeitig ist es möglich, Rechte und Berechtigungen in Echtzeit zu ändern.

### Wie können Consultants hier helfen?

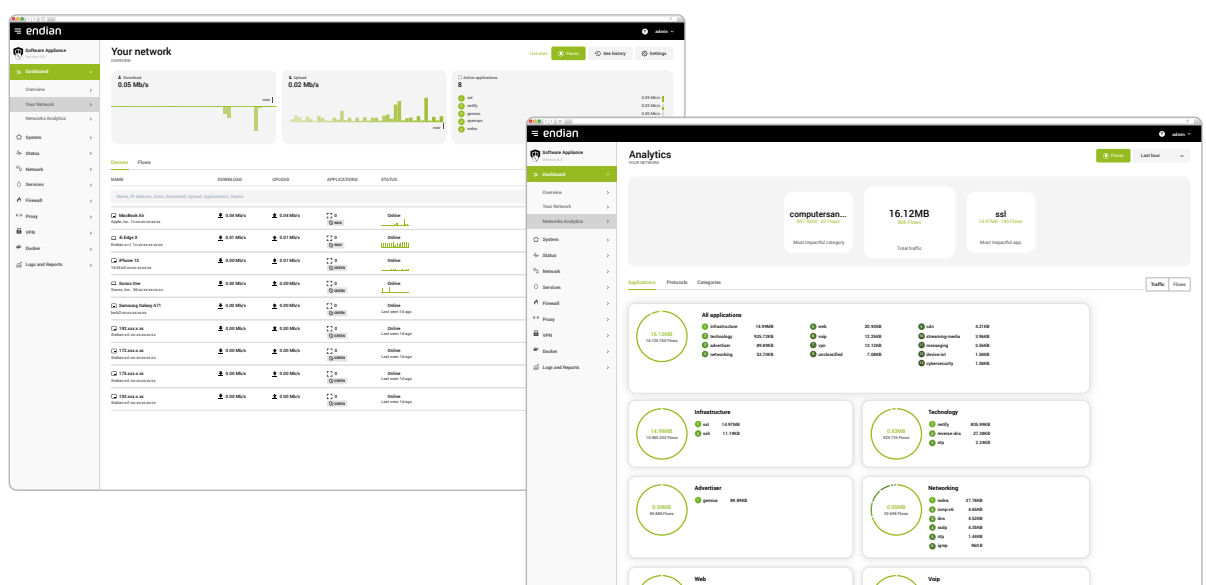
Für eine optimale Zugriffsverwaltung in einem Unternehmen müssen Berechtigungsstrategien und Richtlinien gestaltet werden. Consultants unterstützen bei der Definition klarer Rollen und Verantwortlichkeiten, der Implementierung von Freigabeprozessen sowie der regelmäßigen Überprüfung und Aktualisierung von Berechtigungen.

## Asset-Verwaltung

Das Unternehmen bestimmt und versteht die Anforderungen zur Sicherstellung wesentlicher Dienste in Netzwerken und Informationssystemen.

### Wie kann Endian hier helfen?

Die Endian Lösung Network Awareness bietet einen kompletten Überblick über die IT- und OT-Netzwerke. Es zeigt die Assets innerhalb der Netzwerke sowie ihre Verbindung untereinander und bildet damit die Basis für die Netzwerksegmentierung.



## Authentifizierung

Das Unternehmen ergreift geeignete Maßnahmen, um Benutzer auf seiner eigenen Infrastruktur auf sichere Weise zu authentifizieren.

### Wie kann Endian hier helfen?

Endian bietet Multi-Faktor-Authentifizierung für verschiedene Dienste und unterstützt externe Dienste, wie Microsoft Active Directory (AD) und Windows New Technology Lan Manager (NTLM). Microsoft-Nutzer können sich damit einfach auf den Endian-Systemen authentifizieren.

## Kommunikation im Notfall:

Das Unternehmen definiert eine Kommunikationsstrategie für den Notfall.

### Wie kann Endian hier helfen?

Tritt ein Notfall ein, ist schnelles Handeln entscheidend. Endian bietet ein Alarmierungssystem, das automatisch eine Benachrichtigung per Mail oder SMS versendet, sobald ein Ereignis eintritt, beispielsweise eine Cyberattacke oder ein anderer kritischer Vorfall. Damit lassen sich schnell Gegenmaßnahmen treffen und der Vorfall abmildern.

### Wie können Consultants hier helfen?

Ein Notfallplan definiert klare Verantwortlichkeiten, Eskalationswege und Kommunikationsprotokolle für den Ernstfall. Consultants unterstützen bei der Implementierung eines Notfallplans von der Identifizierung der relevanten Ansprechpartner und Entscheidungsträger bis hin zur passenden Kommunikationsstrategie.

## Umsetzung von NIS-2 Richtlinien – jetzt handeln

Alle EU-Staaten müssen die NIS2-Richtlinie bis Oktober 2024 in nationales Recht umwandeln.

Wer nun neu unter die Richtlinie fällt, sollte schnell handeln. Denn Beratung, die Auswahl passender Technologien und deren Implementierung brauchen Zeit.

**Gerne beraten und unterstützt Endian Sie bei der Umsetzung der NIS2 Richtlinie – nehmen Sie dazu gerne Kontakt mit uns auf.**

