

März 2024

Whitepaper zu NIS2 von Lexxton AG

Um was geht es?

Die NIS2-Richtlinie ist ein wichtiges Regelwerk, das die EU zur Verbesserung der Cybersicherheit und zum Schutz kritischer Infrastrukturen erlassen hat. Sie zielt darauf ab, kritische Sektoren durch die Einführung höherer Cybersicherheitsstandards zu sichern, aber sie befasst sich auch mit einer schnellen Meldung von Vorfällen und einer besseren Koordination der EU-Länder im Bereich der Cybersicherheit.

Was sind die Ziele der NIS2-Richtlinie?

Betreiber in der EU müssen mindestens folgende Cyber Security Massnahmen umsetzen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen:

- **Policies:** Richtlinien für Risiken und Informationssicherheit
- **Incident Management:** Prävention, Detektion und Bewältigung von Cyber Incidents
- **Business Continuity:** BCM mit Backup Management, DR, Krisenmanagement
- **Supply Chain:** Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern
- **Einkauf:** Sicherheit in der Beschaffung von IT- und Netzwerk-Systemen
- **Effektivität:** Vorgaben zur Messung von Cyber und Risiko Massnahmen
- **Training:** „Cyber Security Hygiene“
- **Kryptographie:** Vorgaben für Kryptographie und wo möglich Einsatz von Verschlüsselungssystemen
- **Personal:** Human Resources Security
- **Zugangskontrollen:** Regelung der Zugangskontrollen zu den sensitiven Zonen
- **Asset Management:** Sicherstellung des Gesamtüberblicks über die gesamte Netzwerkinfrastruktur
- **Authentication:** Einsatz von Multi Factor Authentisierung und SSO
- **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- **Notfall-Kommunikation:** Einsatz gesicherter Notfall-Kommunikations-Systeme

Welche Organisationen sind von NIS2 betroffen?

Wesentliche Sektoren		Wichtige Sektoren	
Grenzwert > 250 Mitarbeitende > 43 Mio. € Bilanz		Grenzwert 50 – 249 Mitarbeitende 10 – 43 Mio. € Bilanz	
> 50 Mio. € Umsatz		10 – 50 Mio. € Umsatz	
Energie	Verkehr	Post- und Kurierdienste	Abfallentsorgung
Banking	Finanzmärkte	Chemie	Lebensmittel
Gesundheit	Trinkwasser	Produktion	Digitale Dienste
Abwasser	Digitale Infrastruktur	Forschungseinrichtungen	
IKT-Service-Management	Öffentliche Verwaltung		
Weltraum			

Wichtiger Hinweis: Organisationen, die die genannten Schwellenwerte für wichtige Sektoren überschreiten, aber trotzdem nicht unter die wesentlichen Einrichtungen fallen, müssen die Richtlinie gemäss den Vorgaben für wichtige Einrichtung erfüllen.

Zeitplan zur Erfüllung der NIS2-Anforderungen?

NIS2 trat offiziell am 16. Januar 2023 in Kraft. Die Mitgliedstaaten müssen die NIS2-Richtlinie **bis zum 17. Oktober 2024** in nationales Recht umsetzen, um die Compliance sicherzustellen. **Wenn die Anforderungen der NIS2-Richtlinie nicht innerhalb dieser Frist umgesetzt werden, können Bussgelder sowohl für Einzelpersonen als auch für Organisationen erhoben werden.**

Wie kann Lexxton Sie auf dem Weg zur NIS2-Compliance unterstützen?

Unser Cyber Resilience Assessment gibt Ihnen einen klaren und detaillierten Überblick über Ihre Cyber Maturität. Als Ergebnis nach dem Assessment resultiert ein Katalog mit konkreten Massnahmen, welche umzusetzen sind, damit sie NIS2-compliant werden.

Ihre Ansprechpartner:



Felix Burri
CDO, Cyber Resilience Lead
felix.burri@lexxton.com
+41 79 908 04 04



Urban Lederer
CEO
urban.lederer@lexxton.com
+41 79 766 11 55

