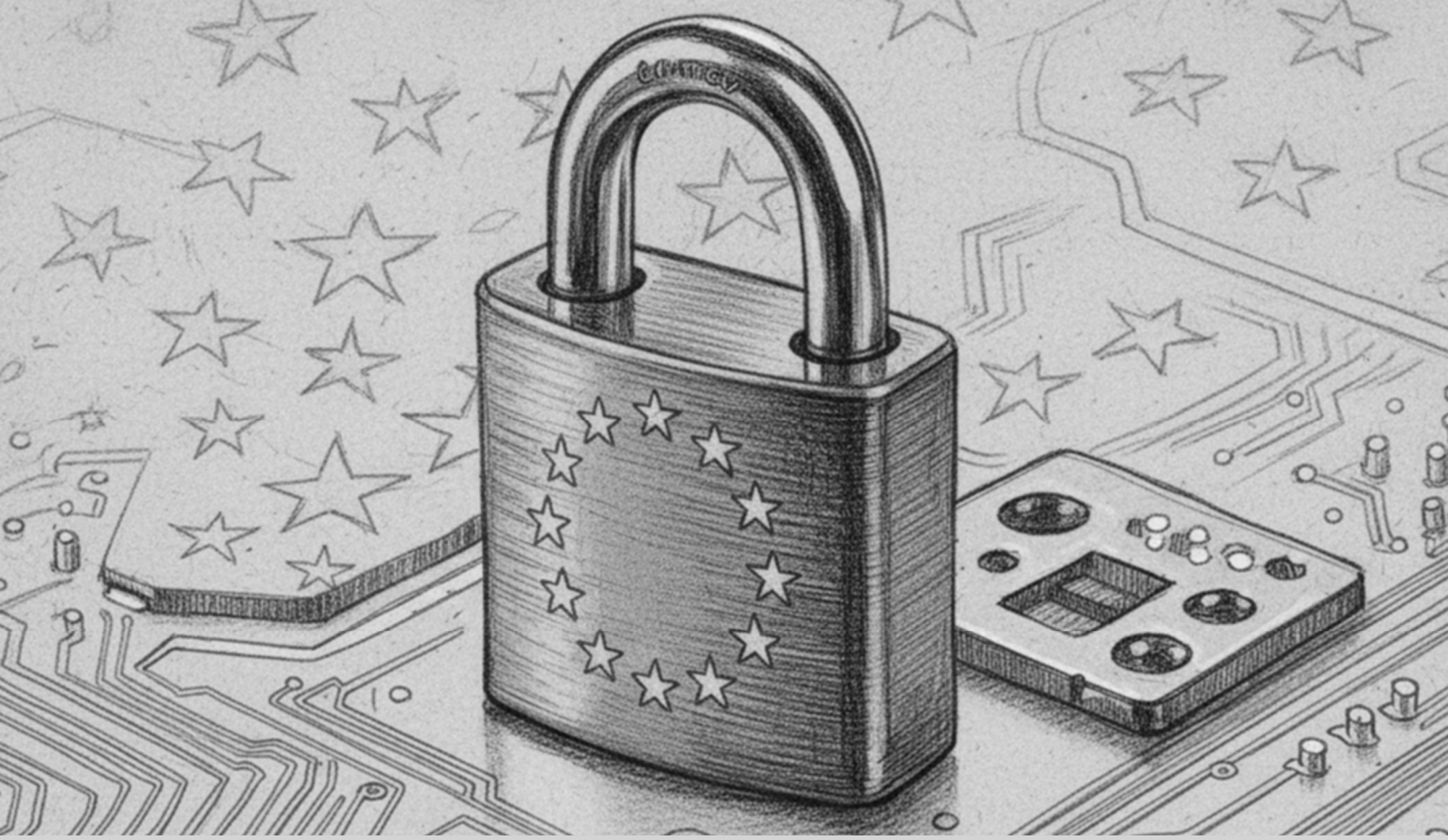

Sind Sie NIS-2-ready?

5 Schritte zur NIS-2-Compliance

SECURAM
consulting

SECURAM Consulting GmbH • Neue ABC-Straße 8 • 20354 Hamburg

Unsere 5 Schritte zur NIS-2-Compliance

Schritt 1: GAP-Analyse

Mit der SECURAM-GAP-Analyse helfen wir Ihnen, Abweichungen zwischen Ist- und Soll-Zustand zu identifizieren. Dadurch leiten wir mit Ihnen gezielt NIS-2-Umsetzungsmaßnahmen ab.

Schritt 2: Verantwortlichkeiten klären

Ihre Geschäftsführung steht im Fokus und muss sicherstellen, dass Risiken minimiert und Lücken geschlossen werden. Sie muss Ressourcen bereitstellen und Maßnahmen überwachen sowie regelmäßige Reportings etablieren.

Schritt 3: ISMS als Fundament

ISO/IEC 27001 ist das Fundament für Ihre erfolgreiche NIS-2-Compliance. Richtlinienwerk, Risikomanagement, Maßnahmenkataloge und Nachweisführung dienen als guter Ausgangspunkt und sollten um NIS-2-spezifische Anforderungen ergänzt werden. Aus den Vorgaben werden konkrete Maßnahmen in der Operationalisierung dargestellt und messbar gemacht.

Schritt 4: Incident Response und Meldewesen

Vorfall erkennen, melden, dokumentieren, Gegenmaßnahmen einleiten. Sie müssen Sicherheitsvorfälle innerhalb von 24 Stunden an das BSI melden. Ein gelebter Meldeprozess ist essenziell für Ihre NIS-2-Compliance.

Schritt 5: Lieferkette und Entwicklungsprozesse

Lieferkette und Entwicklungsprozesse absichern. Vereinbaren Sie Sicherheitsklauseln, Nachweise und Audit-Rechte. Bewerten Sie Dritte risikobasiert und binden Sie sie in Melde- und Notfallprozesse ein. Für die Eigenentwicklung von Software müssen Sie sichere Entwicklungs- und Wartungsprozesse etablieren.

Was ist NIS-2?

Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments vom 14. Dezember 2022 verpflichtet Mitgliedsstaaten in der EU zu einer schärferen Cyber-Security-Strategie anhand nationaler Umsetzungsgesetze. Dabei werden Strafen bei Verstößen harmonisiert.

Stand in Deutschland

Am 13.11.2025 hat der Deutsche Bundestag den Gesetzesentwurf zur Umsetzung der NIS-2-Richtlinie verabschiedet. Die ca. 30.000 betroffenen Einrichtungen müssen prüfen, welche Maßnahmen kurzfristig ergriffen werden müssen, um kostspielige Sanktionen zu vermeiden.

Wichtige Maßnahmen (Auswahl)

- Einführung eines Meldeprozesses bei Vorfällen
- Kontinuierliches Risikomanagement
- Regelmäßige Schulung der Geschäftsführung

Seit 2012 vertrauen Unternehmen SECURAM Consulting

Seit unserer Gründung beraten wir Unternehmen mit Leidenschaft, Verantwortung und Agilität. Wir schaffen Sicherheit und Resilienz durch umfassende Analysen, maßgeschneiderte Maßnahmen und die Umsetzung aktueller regulatorischer Anforderungen wie z.B. NIS-2, TISAX®, sowie DORA.

Unsere Experten entwickeln Notfall- und Krisenmanagement, bauen Informationssicherheitsmanagement- und Risikosysteme auf, führen interne Audits durch und begleiten Zertifizierungen. Darüber hinaus weisen wir den Weg zur sinnvollen und rechtlich korrekten Implementierung und Verwendung von Künstlicher Intelligenz.

Auf Wunsch stellen wir externe Business Continuity Manager oder Informationssicherheitsbeauftragte (ISB/CISO) bereit.

Unser Produktportfolio umfasst technische Lösungen zur automatisierten Stärkung der IT-Security unserer Kunden wie z.B. SIEM und SOC, und zur Schulung der Awareness der Mitarbeiter.

Ihr persönlicher Ansprechpartner

Informationssicherheit basiert auf Vertrauen. Daher ist uns die Nähe zu unseren Kunden wichtig. Neben den projektbezogenen Ansprechpartnern aus unserem Consulting steht Ihnen daher ein persönlicher Ansprechpartner zur Verfügung, der für Sie themenübergreifend erreichbar ist.

Nadine Eibel
Geschäftsführerin

+49 40 298 4553 – 0
sales@securam-consulting.com