



NIS-2



NIS-2 Unterstützung

NIS-2 Grundlage für nachhaltige Cyber-Sicherheit

Digitale Geschäftsmodelle sind heute kritischer denn je und damit auch angreifbarer. Mit NIS-2 reagiert die EU auf genau diese Realität. Was mit NIS-1 nicht erreicht wurde, wird jetzt nachgeschärft: mehr Verantwortung auf Führungsebene, strengere Vorgaben, deutlich mehr betroffene Unternehmen.

BLUE Consult unterstützt Unternehmen NIS-2 strukturiert umzusetzen und ihre Cyber-Resilienz gezielt zu stärken. Dabei geht es nicht nur um Compliance, sondern um die wirksame Absicherung kritischer Geschäftsprozesse.

Durch die Verbindung von Governance, Risikomanagement sowie technischen und organisatorischen Maßnahmen entstehen belastbare, nachweisbare Sicherheitsstrukturen, als Schutz vor Cyberangriffen, Ausfällen und steigenden Anforderungen entlang der Lieferkette.

NIS-2 ist eine Chance: Richtig umgesetzt wird NIS-2 vom regulatorischen Aufwand zum strategischen Hebel für mehr Sicherheit, stabile Prozesse, echte Cyber-Resilienz und damit zum klaren Wettbewerbsvorteil.

Faktencheck:

- 80 % der Cyberangriffe richten sich gegen den Mittelstand
- 29.500 Unternehmen in Deutschland sind von NIS-2 betroffen
- Ca. 20.000 Unternehmen haben die Frist verpasst
- Nur ca. 39 % haben sich fristgerecht registriert
- 91 % der Unternehmen fühlen sich gut vorbereitet, erfüllen jedoch im Schnitt nur rund 56 % der gängigen Sicherheitsanforderungen und sind damit häufig noch nicht NIS-2-ready

Für wen ist das besonders relevant?

Besonders wichtig ist die NIS-2 Richtlinie für Unternehmen, die Teil kritischer oder digital vernetzter Wertschöpfungs- und Lieferketten sind, auch dann, wenn sie selbst nicht unmittelbar als regulierte Einrichtung eingestuft sind.

Denn durch Abhängigkeiten in IT-Systemen, Services und Partnerstrukturen entstehen indirekte Anforderungen, die klare Sicherheitsnachweise und belastbare Cyber-Sicherheitsstrukturen erforderlich machen.

Wie ist die Lage bei Ihnen?

- Wissen Sie, ob Ihr Unternehmen direkt oder indirekt von NIS-2 betroffen ist?
- Haben Sie eine klare Übersicht über Ihre aktuellen Cyber-Risiken?
- Sind Rollen, Verantwortlichkeiten und Prozesse im Ernstfall definiert?
- Können Sie Sicherheitsvorfälle fristgerecht melden und dokumentieren?
- Ist Ihre IT- und Sicherheitsstrategie auditierbar und nachweisbar?

Unsere Leistungen:

Wir kommen aus dem operativen IT-Betrieb und setzen Sicherheitsanforderungen seit Jahren technisch um, u. a. in den Bereichen Monitoring, Patch-Management, Backup, Identity & Access sowie Incident Handling. Statt isolierter Konzepte integrieren wir NIS-2 in Ihre vorhandene IT, damit Ihr Betrieb dauerhaft trag- und zukunftsfähig bleibt.

NIS-2-Umsetzung und nachhaltige Cyber-Resilienz

Wir begleiten Sie ganzheitlich bei der NIS-2-Umsetzung. Von der Betroffenheitsanalyse über die Bewertung und Priorisierung von Maßnahmen bis hin zur technischen Umsetzung und organisatorischen Verankerung.

Analyse & Betroffenheitsprüfung

Wir bestimmen Ihre NIS-2-Betroffenheit auf Basis von Sektor, Unternehmensgröße und KRITIS-Bezug und definieren den regulatorischen Scope (Organisation, Standorte, Systeme).

Readiness Assessment & GAP-Analyse

Wir bewerten Ihren Status quo entlang etablierter Frameworks (z. B. NIST CSF) und führen danach eine Reifegradanalyse mit priorisierter Handlungsempfehlung durch.

Governance & Organisation

Wir unterstützen beim Aufbau einer belastbaren Cyber-Security-Governance, definieren Rollen und etablieren Risk-Management- und Reporting-Strukturen.

Technische Sicherheitsmaßnahmen

Wir analysieren Ihre Security-Architektur und begleiten die Umsetzung zentraler Controls wie IAM, Monitoring, Backup-Strategien sowie Detection & Response.

Incident Response & Meldeprozesse

Wir etablieren strukturierte Incident-Response-Prozesse, inklusive Eskalationswegen und NIS-2-konformer Meldeverfahren sowie Krisenmanagement.

Validierung & Nachweisfähigkeit

Wir helfen den Status Ihrer Sicherheitsmaßnahmen transparent zu machen und alle relevanten Nachweise strukturiert bereitzustellen.

NIS-2 ist mehr als eine Pflicht:

Es ist die Chance, Sicherheitslücken zu schließen, Risiken zu minimieren und die Zukunftsfähigkeit Ihres Unternehmens nachhaltig zu stärken.

Ihr erster Schritt: NIS-2 Workshop

Ein strukturierter NIS-2 Workshop ist ein möglicher Einstieg, um Ihre Betroffenheit zu klären, den aktuellen Sicherheitsstatus zu bewerten und konkrete, priorisierte Maßnahmen abzuleiten, immer auf Basis Ihrer bestehenden IT und bereits vorhandenen Strukturen. Alternativ setzen wir auch gezielt an einzelnen Handlungsfeldern an und entwickeln diese Schritt für Schritt weiter.

Weitere Informationen, Blogbeiträge und Podcasts zum Thema, sowie aktuelle Termine zu Webinaren und Web-Schulungen finden Sie auf unserer Webseite unter:

blue-consult.de/nis2

Ihre Benefits

- **Strukturiertes Risikomanagement**
Klare Identifikation und Steuerung von Cyber-Risiken
- **Reduzierte Ausfall- und Schadensrisiken**
Frühzeitige Erkennung und schnelle Reaktion auf Vorfälle
- **Klare Governance-Strukturen**
Transparente Verantwortlichkeiten und Entscheidungswege
- **Audit- und Compliance-Sicherheit**
Nachweisbare Prozesse gegenüber Behörden und Partnern
- **Stärkung der Cyber-Resilienz**
Schutz Ihrer kritischen Geschäftsprozesse und Lieferketten

Christoph Winkelhage

Senior Management Consultant

✉ christoph.winkelhage@blue-consult.de

☎ +49 2151 6500 10

🌐 www.blue-consult.de

