NIS 2
KRITIS

mcs
Ihre IT Zukunft

NIS2-RICHTLINIE
UNTERNEHMER IN DER PFLICHT

Mit der NIS2-Richtlinie der Europäischen Union werden Unternehmen zu umfangreichen Risikomanagementmaßnahmen verpflichtet, auch innerhalb der eigenen Lieferkette. Die Hauptziele der Regelungen sind, die kritischen Einrichtungen der EU-Mitgliedsstaaten vor Cyberangriffen zu schützen und ein europaweit verbessertes Schutzniveau zu schaffen.

Den Unternehmen wird dabei von behördlicher Seite keine Betroffenheit mitgeteilt. Es liegt in der Verantwortung der Unternehmensleitung, die notwendige NIS2-Umsetzung festzustellen, zu melden und die Anforderungen Regulatorik konform und wirksam umzusetzen.

Wichtig:
Die Meldepflicht für Ihr Unternehmen obliegt Ihnen.
Machen Sie hier eine Betroffenheitsanalyse.

Wesentliche Einrichtungen	Wichtige Einrichtungen
Große Organisationen in Sektoren mit hoher Kritikalität sowie Sonderfälle	**Große Organisationen sonstiger kritischer Sektoren und mittlere Unternehmen**
▪ > 250 Mitarbeiter ▪ > 50 Millionen € Umsatz ▪ > 43 Millionen € Bilanzsumme	▪ 50 - 250 Mitarbeiter ▪ 10 - 50 Millionen € Umsatz ▪ < 43 Millionen € Bilanzsumme
u. a. Bankwesen, Gesundheitswesen, Energie, Trinkwasser, Abwasser, Verkehr, Digitale Infrastruktur, Weltraum, Finanzmarktstruktur	u. a. Abfallbewirtschaftung, Forschung, Post- und Kurierdienste, Verarbeitendes Gewerbe, Lebensmittelproduktion -verarbeitung &-Handel

Die NIS2-Richtlinie definiert EU-weite Mindeststandards für Netzwerk- und Informationssicherheit. Die Umsetzung in nationales Recht definiert die Anforderungen je EU-Land. Für Deutschland ist die gesetzliche Umsetzung von EU NIS2 zur Stärkung der Cybersicherheit (NIS2UmsuCG) zum **18. Oktober 2024** geplant.

STARKER PARTNER FÜR STARKE LÖSUNGEN

Management System ISO/IEC 27001:2013
TÜVRheinland ZERTIFIZIERT
www.tuv.com ID 9108652210

In Unternehmen, die sich bisher wenig mit dem Thema Cybersicherheit beschäftigt haben, besteht somit dringender Handlungsbedarf. Neben den formalen und prozessualen Anforderungen, wie strukturelles Risiko- und Krisenmanagement, Wiederherstellungsstrategien sowie die Einhaltung von Meldepflichten ist die Absicherung der operativen Betriebssicherheit von entscheidender Bedeutung.

Security Operations Center (SOC)
Überwachung, Analyse, Alarmierung

Hierzu gehören z.B.

- Schwachstellen-Management der Netzwerkinfrastruktur
- Anomalie-Erkennung und Alarmierungsmechanismen
- Backup und Wiederherstellungskonzepte
- Rechte- und Rollenverteilung
- Multifaktor-Authentifizierung

Unabhängig von der Erfüllung der NIS2-Anforderungen ist angesichts der rasant wachsenden Gefahr durch Cyberbedrohungen die Implementierung von IT-Sicherheitsmaßnahmen geboten. Insbesondere Schadprogramme, die mit dem Ziel entwickelt wurden, Daten auszuspähen und durch unbefugten Zugriff auf IT-Systeme den Geschäftsbetrieb lahmzulegen und Geld zu erpressen, sind eine sehr reale Bedrohung, insbesondere auch für mittelständische Unternehmen.

Gemeinsam mit unserem Partner Cosanta schützen wir Ihr Geschäft und Ihre Kunden vor Cyberbedrohungen!

Mit lizenzbasierten Services aus dem deutschsprachigen Security Operations Center (SOC) verteidigen wir Ihre IT-Infrastruktur und Ihr digitales Business vor externen Angriffen – wir helfen, Ihre Wettbewerbsfähigkeit zu sichern!

Neben einer effektiven Gefahrenabwehr im Betrieb, stellen wir eine auditierbare Compliance mit der gültigen Regulatorik sicher.

Services im Überblick:

- ✓ IT-Consulting
- ✓ Sicherheitskonzepte & -strategien
- ✓ Managed Security Services
- ✓ BSI-konform gemäß KRITIS-Regulierung
- ✓ Schwachstellenmanagement
- ✓ Security Information & Event Management (SIEM)
- ✓ Network Intrusion Detection (NIDS)
- ✓ IT Security Validation / Pentests
- ✓ Data Center Security
- ✓ Cloud Security
- ✓ Recovery

Für mehr Informationen - Hier scannen

+49 (0)40 53773-0

info@mcs.de