



NIS2-RICHTLINIE

WAS UNTERNEHMEN WISSEN MÜSSEN

AGENDA

Was ist das?

Anforderungen und Maßnahmen

Wer prüft das Ganze?

Unser Support

Fazit

WAS IST DIE NIS2-RICHTLINIE UND WEN BETRIFFT SIE?

Die NIS2-Richtlinie gilt für viele Branchen, die für die europäische Wirtschaft und Gesellschaft von entscheidender Bedeutung sind. Dazu gehören nicht nur Energie, Wasserwirtschaft und Gesundheitswesen, sondern auch neu hinzugekommene Sektoren wie digitale Infrastruktur, öffentliche Verwaltung und Zulieferer von kritischen Dienstleistungen.

- ✓ Betroffene Einheiten: Unternehmen werden in „kritische“ und „wichtige“ Einheiten eingeteilt. Kritische Einheiten unterliegen strengeren Anforderungen.
- ✓ KMU-Ausnahme: Kleine und mittlere Unternehmen (KMU) sind von NIS2 ausgenommen, sofern sie keine kritischen Dienstleistungen erbringen.

WICHTIGE ANFORDERUNGEN UND MAßNAHMEN ZUR EINHALTUNG

Risikomanagement und Schutzmaßnahmen

- ✓ Risikobewertung: Unternehmen müssen ihre Cybersicherheitsrisiken bewerten und entsprechende Maßnahmen implementieren.
- ✓ Technische Maßnahmen: Firewalls, Netzwerksegmentierung und regelmäßige Software-Updates zur Sicherstellung der Sicherheit.
- ✓ Organisatorische Maßnahmen: Erstellung und Schulung von Krisenteams, Sicherheitsrichtlinien und Zugriffskontrollen.

Meldepflichten bei Sicherheitsvorfällen

- ✓ 24-Stunden-Erstmeldung: Unternehmen müssen Sicherheitsvorfälle innerhalb von 24 Stunden nach deren Erkennung melden.
- ✓ Detaillierte Meldung: Innerhalb von 72 Stunden nach der Erstmeldung ist eine umfassende Analyse des Vorfalls erforderlich.
- ✓ Zusätzliche Meldungen: Bei bedeutenden Vorfällen sind zusätzliche Meldungen an Behörden und Kunden notwendig.



WICHTIGE ANFORDERUNGEN UND MAßNAHMEN ZUR EINHALTUNG

Sicherheit der Lieferkette

- ✓ Absicherung der Lieferkette: Auch externe Dienstleister und Zulieferer müssen über Cybersicherheitsmaßnahmen verfügen.
- ✓ Service Level Agreements (SLAs): Unternehmen sollten klare Sicherheitsanforderungen und Meldepflichten in Verträge mit Drittanbietern aufnehmen.

Dokumentation und Nachweisführung

- ✓ Nachweispflicht: Unternehmen müssen dokumentieren, wie sie die NIS2-Richtlinie einhalten, einschließlich ihrer Risikomanagement- und Cybersicherheitsmaßnahmen.
- ✓ Regelmäßige Audits: Organisationen müssen regelmäßige Audits durchführen, um die Wirksamkeit ihrer Maßnahmen zu überprüfen.



WICHTIGE ANFORDERUNGEN UND MAßNAHMEN ZUR EINHALTUNG

Schulung und Sensibilisierung der Mitarbeiter

- ✓ Cybersicherheitsschulungen: Alle Mitarbeiter müssen regelmäßig geschult werden, um das Bewusstsein für Cybersicherheitsrisiken zu erhöhen.
- ✓ Awareness-Programme: Unternehmen sollten Programme zur Sensibilisierung der Mitarbeiter für Cyberbedrohungen etablieren.

WER PRÜFT DIE EINHALTUNG DER NIS2- RICHTLINIE?

Die Einhaltung der NIS2-Richtlinie wird durch nationale Behörden in jedem EU-Mitgliedstaat geprüft. Dazu gehören:

- ✓ Nationale Cybersicherheitsbehörden: Verantwortlich für die Überprüfung der Maßnahmen und Dokumentationen der Unternehmen.
- ✓ Zusammenarbeit auf EU-Ebene: Die EU-Agentur für Cybersicherheit (ENISA) unterstützt bei der Umsetzung und Koordination zwischen den Mitgliedstaaten.
- ✓ Audits und Kontrollen: Unternehmen müssen regelmäßig Audits und Sicherheitsprüfungen durchführen und die Ergebnisse dokumentieren. Bei Nicht-Einhaltung können empfindliche Bußgelder verhängt werden.



WIE ICH ALS BERATER SIE OPTIMAL UNTERSTÜTZEN KANN

Als Berater helfe ich Ihnen, alle Anforderungen der NIS2-Richtlinie systematisch umzusetzen und Ihre Cybersicherheitsstrategien zu optimieren. Hier sind die Schritte, mit denen ich Sie unterstützen kann:

- ✓ Risikobewertung und GAP-Analyse
- ✓ Erstellung eines maßgeschneiderten Umsetzungsplans
- ✓ Unterstützung bei der Dokumentation und Nachweise
- ✓ Schulung und Sensibilisierung der Mitarbeiter
- ✓ Kontinuierliche Verbesserung und Anpassung

FAZIT

Die NIS2-Richtlinie fordert von Unternehmen eine umfassende Cybersicherheitsstrategie und die Etablierung solider Schutzmaßnahmen. Durch eine systematische Planung und Umsetzung lassen sich die Anforderungen erfüllen und die Sicherheit der Unternehmensinfrastruktur gewährleisten. Als Berater begleite ich Sie durch den gesamten Umsetzungsprozess und unterstütze Sie dabei, die Anforderungen der NIS2-Richtlinie effektiv und effizient zu erfüllen.



KONTAKTIEREN SIE UNS FÜR WEITERE
INFORMATIONEN ODER UM EINE MAßGESCHNEIDERTE
BERATUNG ZU ERHALTEN. GEMEINSAM SICHERN WIR
IHR UNTERNEHMEN VOR DEN HERAUSFORDERUNGEN
DER MODERNEN CYBERSICHERHEITSLANDSCHAFT.

Daniel Aßmann

Datenschutz & QM

Haldenwangfeld 1 - 87677 Stöttwang

Büro: 08345-1896727

www.assmann-daniel.de