Neue NIS2 –Richtlinie*

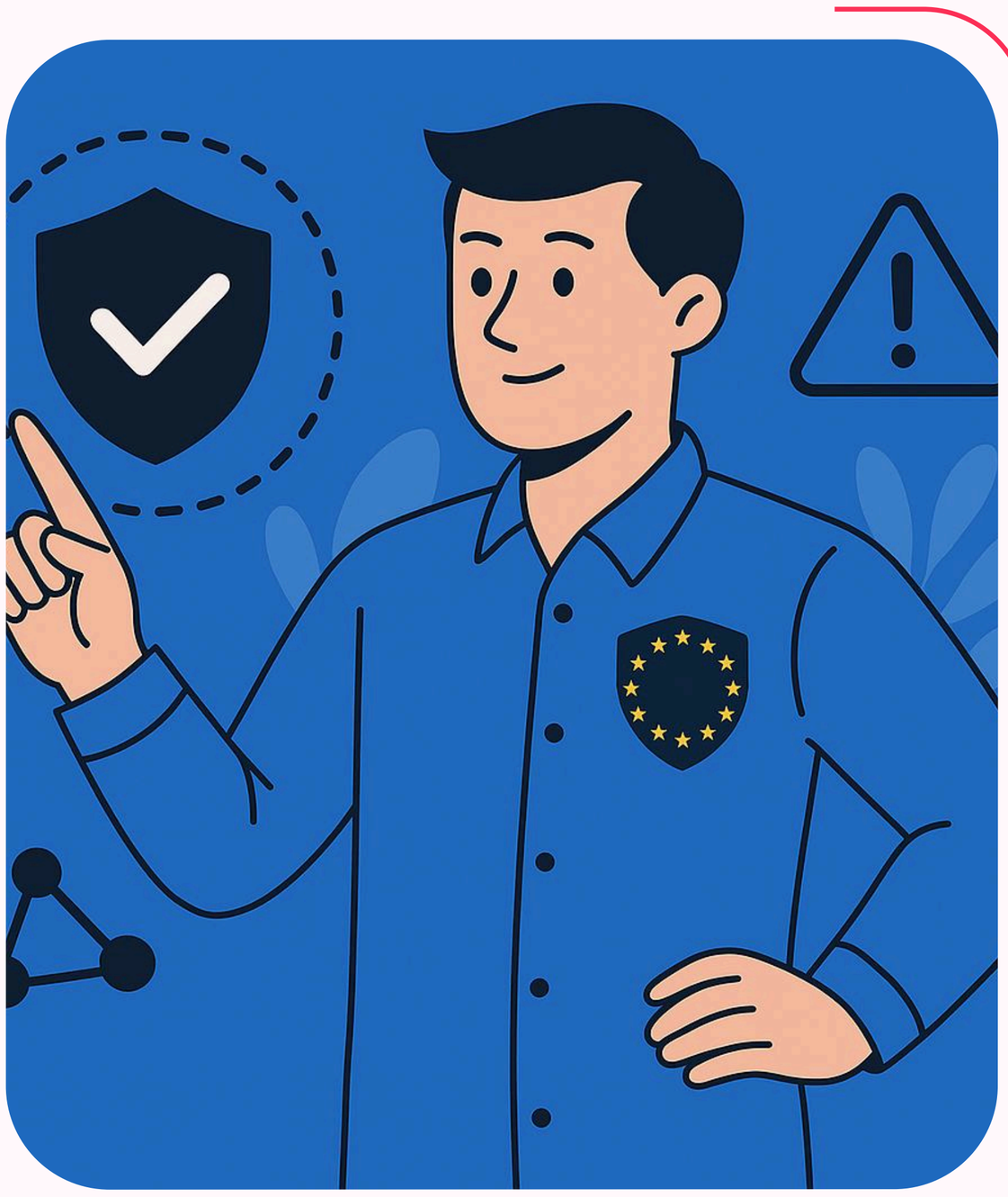
* Fakten und Anwendung

Da die Cyber-Bedrohungen zunehmen und die Angreifer immer fortschrittlicher werden, schaffen Regierungen und globale Organisationen neue Vorschriften, um die Cybersicherheit zu verbessern. Doch wenn eine neue Verordnung herauskommt, kann es schwierig sein, sie zu verstehen und anzuwenden, bevor sie in Kraft tritt.

Die Richtlinie zur Netz- und Informationssicherheit 2 (NIS2) schreibt vor, dass Organisationen in der Europäischen Union die Einhaltung der Vorschriften gewährleisten müssen. Die Verantwortung für die Cybersicherheit liegt nun bei der Unternehmensleitung, die für alle durch Sicherheitsverletzungen verursachten Schäden haftet. Um Unternehmen den Einstieg zu erleichtern, haben wir dieses Whitepaper über NIS2 zusammengestellt, damit Sie mit der Umsetzung beginnen können.

Was ist NIS2?

NIS2 ist die aktuellste Version der EU-Netzwerk- und Informationssicherheitsrichtlinie und zielt darauf ab, die Cybersicherheit in den Mitgliedstaaten zu stärken. NIS2 legt Anforderungen an Risikomanagement, Vorfallmeldung und Lieferkettensicherheit fest. Sie führt außerdem strengere Aufsichts- und Durchsetzungsmaßnahmen ein, darunter höhere Bußgelder bei Nichteinhaltung. Die Richtlinie soll die Zusammenarbeit und den Informationsaustausch zwischen den EU-Ländern verbessern. Insgesamt zielt NIS2 darauf ab, Europa widerstandsfähiger gegen wachsende Cyberbedrohungen zu machen.



Wie wirkt sich NIS2 auf ein Unternehmen aus?

Fällt eine Organisation unter NIS2, muss sie gemäß Artikel 21 der NIS2-Richtlinie geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen zur Bewältigung von Cybersicherheitsrisiken ergreifen.

Die Richtlinie beschreibt zehn zentrale Maßnahmen für das Risikomanagement im Bereich Cybersicherheit:

1. Risikoanalyse und Richtlinien zur Informationssystemsicherheit.

Entwicklung und Pflege von Richtlinien auf Grundlage von Risikobewertungen zum Schutz von Systemen und Daten.

2. Umgang mit Sicherheitsvorfällen.

Implementierung von Prozessen zur Erkennung, Bewältigung und Reaktion auf Cybersicherheitsvorfälle.

3. Geschäftskontinuität, Backup und Krisenmanagement.

Sicherstellung der Betriebskontinuität durch Backups, Wiederherstellungspläne und Krisenreaktion.

4. Sicherheit der Lieferkette.

Bewältigung von Risiken im Zusammenhang mit Lieferanten und Drittanbietern.

5. Sicherheit bei Beschaffung, Entwicklung und Wartung von Netzwerken und Informationssystemen.

Anwendung sicherer Verfahren bei Systemdesign, -entwicklung und -aktualisierungen.

6. Umgang mit und Offenlegung von Schwachstellen.

Effektives Management von Schwachstellen, einschließlich eines Prozesses zur koordinierten Offenlegung.

7. Schulungen und Sensibilisierung für Cybersicherheit.

Schulen Sie Ihre Mitarbeiter regelmäßig, um den menschlichen Aspekt der Cybersicherheit zu stärken.

8. Zugriffskontrolle und Asset-Management.

Beschränken Sie den Zugriff auf Systeme und Daten basierend auf Rollen und Verantwortlichkeiten.

9. Verschlüsselung und Datenschutz.

Nutzen Sie Verschlüsselung und andere Sicherheitsmaßnahmen zum Schutz von Daten, insbesondere sensibler oder personenbezogener Daten.

10. Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierungslösungen.

Verstärken Sie die Authentifizierung, um das Risiko eines unbefugten Zugriffs zu reduzieren.

Wie können wir Ihnen helfen?

Wir unterstützen Sie dabei, die NIS2-Ziele effizient zu erreichen, indem wir:

01 **Sie bei der Implementierung von Maßnahmen zum Cybersicherheits-Risikomanagement unterstützen** (Incident Response, Geschäftskontinuität, Zugriffskontrollen).

02 **Sie bei der Einführung von Sicherheitsüberwachungs-, Erkennungs- und Reaktionssystemen** (SIEM, Firewalls, Antivirus) beraten.

03 **Regelmäßige Schulungen für Mitarbeiter zur Cybersicherheit organisieren.**

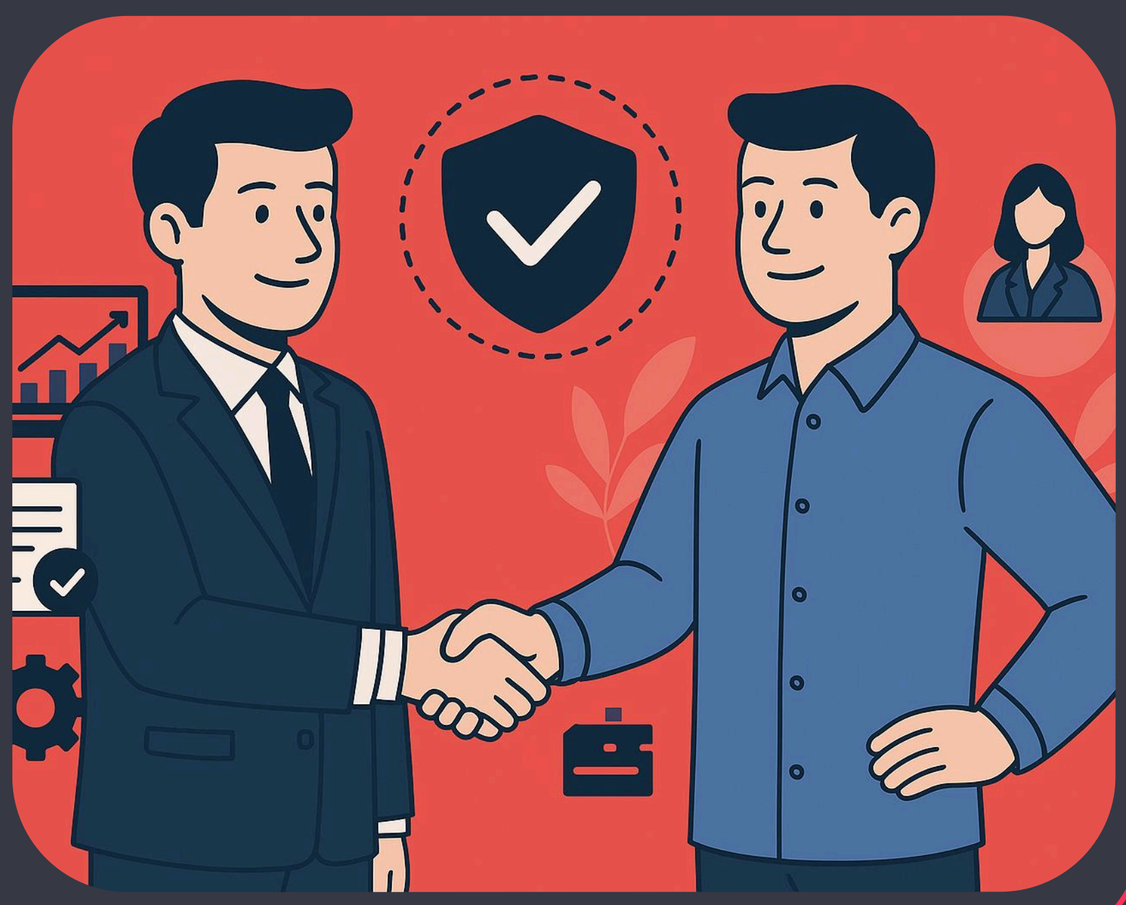
04 **Rahmenbedingungen schaffen, um Lieferanten und Drittanbietern bei der Einhaltung der NIS2-Sicherheitsstandards zu unterstützen.**

05 **Unterstützung beim Aufbau eines Meldesystems für schwerwiegende Cybersicherheitsvorfälle innerhalb von 24 Stunden** (und eines vollständigen Berichts innerhalb von 72 Stunden).

Warum es wichtig ist?

Die Einhaltung der NIS2-Richtlinie ist verpflichtend – auch für Unternehmen in Deutschland. Verstöße können zu erheblichen Bußgeldern, Reputationsschäden und einem Vertrauensverlust bei Partnern führen. Weitere Informationen erhalten Sie beim Bundesamt für Sicherheit in der Informationstechnik (BSI):

Sicherheit in der Informationstechnik (BSI)



Fazit

Die NIS2 wurde von der Europäischen Union eingeführt, was bedeutet, dass alle Mitgliedstaaten sie in ihre eigenen Gesetze einbinden müssen. Dies wird in den einzelnen Ländern zu unterschiedlichen Zeiten geschehen. Warten Sie nicht, bis sie in Kraft tritt, sondern beginnen Sie jetzt mit den Vorbereitungen!

Die Einhaltung der Vorschriften wird ohnehin obligatorisch sein. Deshalb sollten Sie sich einen Vorsprung verschaffen, indem Sie sich an die Net Group wenden, die Ihnen mit maßgeschneiderten Cybersicherheitslösungen, Risikobewertungen und Anleitungen zur Einhaltung der Vorschriften bei der reibungslosen Anpassung an die NIS2-Anforderungen helfen kann.