ITcares

NIS2 Richtlinie sicher und effizient umsetzen

Für viele Firmen in Deutschland und Europa wird die Zeit knapp: Laut der europäischen Cybersicherheitsverordnung NIS2 (Network and Information Security) müssen sich Unternehmen, die Teil internationaler Lieferketten sind, bis 17. Oktober 2024 verpflichtend und nachweisbar effektiver gegen IT-Angriffe absichern.

Bei Nichterfüllung oder unzureichender Umsetzung der geforderten, umfassenden Maßnahmen drohen hohe Strafen und Sanktionen.

Geforderte Cybersicherheits-Maßnahmen

- Policies / Richtlinien
- Incident Management
- Business Continuity
- Supply Chain Security
- Training
- Asset Management
- Reportingpflicht

Um zu überprüfen, ob ein Unternehmen unter die NIS-2-Richtlinie fällt gibt es konkrete Handlungsempfehlungen und Checklisten.

Hier eine Zusammenfassung der wichtigsten Schritte

Überprüfung der Betroffenheit

Unternehmen sollten zunächst überprüfen, ob sie in den Anwendungsbereich von NIS2 fallen. Die NIS2-Richtlinie betrifft Unternehmen, die Dienstleistungen in der EU erbringen, mehr als 50 Personen beschäftigen oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Millionen Euro haben und einem der kritischen Sektoren angehören.

Angemessene Sicherheitsmaßnahmen

Es ist wichtig, dass Unternehmen ihre vorhandenen Sicherheitsmaßnahmen und Prozesse überprüfen und sicherstellen, dass ihre Netzwerk- und Informationssysteme ausreichend vor Cyberbedrohungen geschützt sind.

Identifikation und Schutz kritischer Infrastrukturen

Unternehmen sollten ihre kritischen Geschäftsprozesse und sensiblen Daten identifizieren und deren Sicherheitsniveau bewerten, einschließlich der Entwicklung von Wiederherstellungsplänen nach Angriffen.

Einrichtung von Mechanismen zur Erkennung von Cybervorfällen

Unternehmen sollten Vorkehrungen treffen, um Cyberbedrohungen schnell zu erkennen. Dies gilt für alle Systeme.

Risikomanagement und Verfahren für den Umgang mit Sicherheitsvorfällen

Unternehmen sind verpflichtet, Risikomanagement zu betreiben und Prozesse für den Umgang mit Sicherheitsvorfällen zu implementieren.

Monitoring und Reporting

Unternehmen müssen sowohl die Rechtslage als auch ihre internen Prozesse kontinuierlich überwachen und auf Änderungen reagieren.

Gap-Analyse: Um individuell erforderliche Maßnahmen zu ermitteln, sollten Unternehmen eine Gap-Analyse durchführen.

Mit unseren Managed Services setzen Sie die NIS2-Richtlinien sicher um:

- Managed Server
- Managed Firewall / Managed Cloud Firewall
- Managed Endpoint Detection & Response
- Managed Backup & Disaster Recovery
- Managed E-Mail Security
- Managed E-Mail Archiv
- Security Awareness Trainings für Ihre Mitarbeiter
- SOC Security Operations Center

Im Rahmen unserer Managed Services überwachen und managen wir proaktiv Ihre IT-Infrastruktur und führen notwendige Updates sicher und automatisiert durch. Dies führt zu einer deutlich verbesserten Sicherheit und Verfügbarkeit Ihrer Systeme und Anwendungen, zu planbaren Kosten und einer deutlichen Entlastung Ihrer eigenen IT.

Die Vorteile unserer Managed Services

- Ein Ansprechpartner für alle Themen
- Zugriff auf qualifiziertes Personal - 7x24
- Aktuelles Expertenwissen zu jeder Zeit
- Minimierung von Ausfallzeiten
- IT-Kosten zum monatlichen Festpreis
- Fokus auf Ihr Business
- Mehr Wachstum & gesteigerte Wirtschaftlichkeit

Mit dem NIS2 Quick-Check unterstützen wir Unternehmen dabei, die Betroffenheit zu prüfen und die notwendigen Schritte einzuleiten.

Buchen Sie jetzt Ihr Beratungsgespräch und lassen Sie uns über die Sicherheit Ihrer IT sprechen.

SIE MÖCHTEN MEHR ÜBER UNSERE MANAGED SERVICES ERFAHREN?

Rufen Sie uns unter +49 711 414141-42 an, oder schicken Sie eine E-Mail an mail@ITcares.de

Wir informieren Sie gerne persönlich über alle Einsatzmöglichkeiten und Vorteile.

ITcares GmbH
Industriestraße 4
D-70565 Stuttgart

+49 711 414141-0
mail@ITcares.de
ITcares.de

ITcares