AUVESY-MDT

NIS2-Richtlinie:
Ein Überblick zu den EU-Vorgaben in Cybersicherheit.

Was Unternehmen wissen müssen und wie octoplant unterstützt.

Die verbindliche EU-Richtlinie zur Cybersicherheit (NIS2) tritt dieses Jahr am 17. Oktober in Kraft und betrifft eine Vielzahl von Branchen. Unternehmen müssen geeignete Cybersicherheitsmaßnahmen ergreifen und schwerwiegende Vorfälle melden.

NIS2: Die Zukunft der Cybersicherheit in der EU

Die Richtlinie zur Netz- und Informationssicherheit (NIS2) revolutioniert die Sicherheitslandschaft. Hier sind ihre Schlüsselmerkmale:

1. **Verschärfte Sicherheitsanforderungen:** Die Sicherheit der Lieferketten wird verbessert, die Meldepflichten werden gestrafft, und es werden strengere Aufsichtsmaßnahmen eingeführt.
2. **Harmonisierte Sanktionen:** Strengere Durchsetzungsvorschriften, EU-weit harmonisierte Sanktionen bisher nicht beziffert.
3. **Risikobewertungen und Multifaktor-Authentifizierung:** Die Richtlinie umfasst Risikobewertungen, Multifaktor-Authentifizierung und Sicherheitsverfahren für Mitarbeiter mit Zugang zu sensiblen Daten.
4. **Sicherheit der Lieferkette und Meldung von Zwischenfällen:** NIS2 legt Anforderungen für Lieferketten-Sicherheit, Business Continuity-Pläne, Incident Reporting und Management-Haftung bei Nichteinhaltung der Cybersicherheitsanforderungen fest.

Von NIS2 betroffene Einrichtungen und Unternehmen:

Diese Einrichtungen müssen die Sicherheits- und Meldeanforderungen der Richtlinie erfüllen:

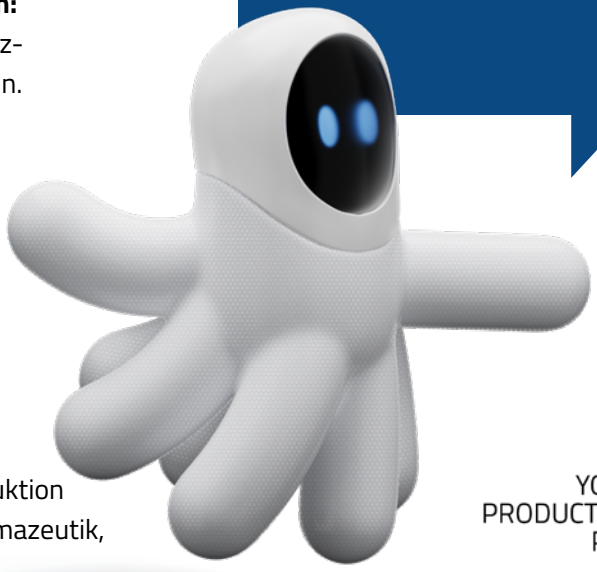
- **Anbieter wesentlicher Dienstleistungen:** Energie, Verkehr, Wasser, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen.
- **Wichtige Dienstleistungsanbieter:** Öffentliche Verwaltung, Raumfahrt, Forschung, Postdienste, Abfallwirtschaft, Maschinenbau.
- **Wichtige Anbieter digitaler Dienste:** Suchmaschinen, Cloud-Computing-Dienste, Online-Marktplätze.
- **Verarbeitendes Gewerbe / Herstellung von Waren:** Automobil / Zulieferer, Produktion & Verarbeitung von Lebensmitteln, Pharmazeutik, medizinische Geräte.

Gilt NIS2 für Ihre Organisation?

Machen Sie die Betroffenheitsanalyse:

Qualtrics Survey

https://survey.pwc.com/jfe/form/SV_b7wc0Tg7IxcaqBo



YOUR PRODUCTION PRO

octoplant powered by AUVESY-MDT

Maßnahmen, die gemäß den NIS2-Vorschriften zu ergreifen sind:

Im Folgenden werfen wir einen genaueren Blick auf die Maßnahmen, die gemäß den NIS2-Vorschriften zu ergreifen sind:

1. **Risikomanagement:** Management von Zwischenfällen, mehr Sicherheit in der Lieferkette, verbesserte Netzsicherheit, bessere Zugangskontrolle, Verschlüsselung von Daten.
2. **Verantwortlichkeit der Geschäftsführung:** Die Firmenführung ist für die Überwachung und Teilnahme an Schulungen zur Cybersicherheit verantwortlich. Bei Verstößen drohen Sanktionen und vorübergehender Ausschluss aus Führungsaufgaben.
3. **Meldeverpflichtungen:** Wesentliche und wichtige Einrichtungen müssen Verfahren zur unverzüglichen Meldung von Sicherheitsvorfällen verfügen, die erhebliche Auswirkungen auf ihre Dienstleistungen oder auf die Empfänger haben.
4. **Geschäftskontinuitätsplan:** Unternehmen benötigen Pläne für größere Cybervorfälle, die Systemwiederherstellung, Notfallverfahren und die Einrichtung eines Krisenreaktionsteams umfassen.

octoplant sorgt für mehr Cybersicherheit:

Die neue EU-Richtlinie zielt auf eine höhere Widerstandsfähigkeit der IT- und OT-Systeme zum Schutz vor Cyberangriffen ab. octoplant kann helfen, die Anforderungen und Standards zu erfüllen.

Incident Management mit octoplant:

Asset Management:

In komplexen Produktionsumgebungen ist die Versionierung vieler Projekte und Änderungen eine mühsame, aber kritische Aufgabe. octoplant bietet **Versionsmanagement** und automatische Backups, damit immer die richtige Version läuft. Das spart Zeit, reduziert Fehler und macht die Programmierung und Gerätekonfiguration zuverlässiger.

Business Continuity:

Im Ernstfall ermöglicht **Instant Recovery (Backup Management)** die schnelle Wiederherstellung aller notwendigen Projekt- und Programmierstände. Mit octoplant können einzelne Geräte oder die gesamte Produktionsanlage jederzeit wieder in einen gültigen Zustand versetzt werden. So werden Ausfälle minimiert, und Fehler oder Manipulationen rückgängig gemacht.

Vulnerability Management:

Als Teil der **Cybersecurity-Strategie** überwacht octoplant Anlagen und informiert automatisch über Schwachstellen und Risiken. **Änderungs- und Schwachstellenerkennung** mit einem separaten **Risiko-Score** für jedes Asset helfen, ungeplanten Ausfällen vorzubeugen.

Business Continuity Management
BCM umfasst Maßnahmen zur Vorbeugung, Erkennung und Bewältigung von Cyber-Vorfällen, einschließlich Backup-Management, Disaster Recovery und Krisenmanagement. Es umfasst auch die Entwicklung eines Sicherheitskonzepts, einschließlich der Definition des Informationsnetzes und der erforderlichen Komponenten für Geschäftsprozesse.

ÜBER 3.000 UNTERNEHMEN WELTWEIT VERTRAUEN AUF OCTOPLANT!

Jetzt Cybersicherheit verbessern und Risiken minimieren:

Hier klicken: octoplant Jetzt testen

https://auvesy-mdt.com/de/jetzt-testen

Wir freuen uns auf Ihren Kontakt!

+49 6341 6810-300
info@auvesy-mdt.com
www.auvesy-mdt.com

AUVESY-MDT