AUVESY-MDT

The NIS2 Directive:
An Overview of EU Cyber-security Requirements.

What Companies Need to Know and How octoplant Can Assist.

The binding EU directive on cybersecurity (NIS2) will come into effect this year on October 17 and applies to a wide range of industries. Companies must take appropriate cybersecurity measures and report serious incidents. Find out if your company is affected and how octoplant can support you!

NIS2: The Future of Cybersecurity in the EU

The Network and Information Security (NIS2) directive is revolutionizing the security landscape. Here are its key features:

1. **Tightened Security Requirements:** Supply chain security is enhanced, reporting obligations are streamlined, and stricter supervisory measures are introduced.
2. **Harmonized Sanctions:** Stricter enforcement rules, EU-wide harmonised sanctions not yet quantified.
3. **Risk Assessments and Multifactor Authentication:** The directive covers risk assessments, multifactor authentication, and security procedures for employees with access to sensitive data.
4. **Supply Chain Security and Incident Reporting:** NIS2 establishes requirements for supply chain security, business continuity plans, incident reporting, and management liability in case of non-compliance with cybersecurity requirements.

Entities and Companies Affected by NIS2:

These entities must comply with the security and reporting requirements of the directive:

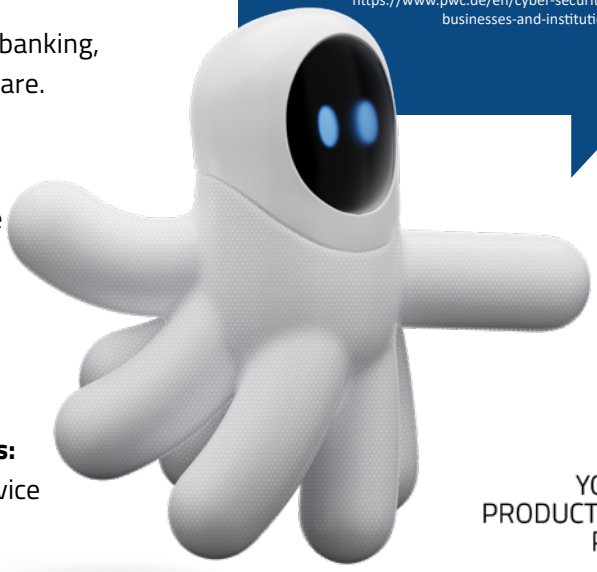
- **Providers of Essential Services:** Including energy, transportation, water, banking, financial market infrastructures, healthcare.
- **Significant Digital Service Providers:** Encompassing public administration, aerospace, research, postal services, waste management, mechanical engineering.
- **Key Providers of Digital Services:** Such as search engines, cloud computing services, online marketplaces.
- **Manufacturing and Production of Goods:** Including the automotive and medical device sectors production & processing of food, Pharmaceuticals.

Does NIS2 apply to your organization?

Conduct the impact analysis:

Qualtrics Survey

https://www.pwc.de/en/cyber-security/european-nis2-directive-implications-for-businesses-and-institutions.html#nis-2



YOUR PRODUCTION PRO

octoplant powered by AUVESY-MDT

Measures to Be Taken According to NIS2 Regulations:

Let's take a closer look at the measures to be taken in accordance with NIS2 regulations:

1. **Risk Management:** Incident management, enhanced supply chain security, improved network security, better access control, and data encryption.
2. **Management Accountability:** Company leadership is responsible for monitoring and participating in cybersecurity training. Violations may result in sanctions and temporary exclusion from leadership roles.
3. **Reporting Obligations:** Essential and significant entities must have procedures for promptly reporting security incidents that have significant impacts on their service provision or recipients.
4. **Business Continuity Plan:** Companies need plans for handling major cyber incidents, including system recovery, emergency procedures, and the establishment of a crisis response team.

How octoplant Enhances Cybersecurity:

The new EU directive aims to protect IT and OT systems from cyberattacks by increasing the resilience of these systems. octoplant can assist you in meeting the requirements and ensuring that your IT and OT infrastructure complies with the required standards.

Incident Management with octoplant:

Asset Management:

In complex production environments, managing multiple projects and their changes can be cumbersome yet critical. octoplant offers **version control** and automatic backups for all versions and modifications, ensuring that the correct version is always running. Automated backups save time, reduce errors, and enhance the reliability of device programming and configuration.

Business Continuity:

In case of emergencies, **Instant Recovery (Backup Management)** enables rapid restoration of essential programs and data. With octoplant, individual devices or the entire production facility can be brought back to a valid state at any time. This minimizes downtime, disruptions, and allows for the reversal of errors and manipulations.

Business Continuity Management
BCM encompasses measures for prevention, detection, and handling of cyber incidents, including backup management, disaster recovery, and crisis management. It also involves developing a security concept, including defining the information network and necessary components for business processes.

Vulnerability Management:

As part of your **cybersecurity strategy**, octoplant monitors assets and automatically notifies companies of **vulnerabilities and risks**. A separate **risk score** for each asset highlights potential threats. Additional preventive features, such as change and vulnerability detection, actively help prevent outages.

OVER 3,000 COMPANIES WORLDWIDE TRUST OCTOPLANT!

Improve cybersecurity and minimize risks:

Click here: Test octoplant now

https://auvesy-mdt.com/en/test-now

We are looking forward to your contact!

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

AUVESY-MDT