octoplant

A Comprehensive Guide to EU Cybersecurity Requirements

The binding EU cybersecurity directive, NIS-2, takes effect on October 17, impacting numerous industries. Companies must now implement robust cybersecurity measures and report critical incidents. The NIS-2 Directive requires EU Member States to transpose it into national laws for enforcement.

While the directive sets a baseline for cybersecurity, Germany may adopt higher standards ("minimum harmonization"). The NIS2 UmsuCG (The NIS2 Implementation Law) is expected to take effect in March 2025, at which point affected organizations must comply immediately, with no transition period. Learn if your company is affected and discover how octoplant can provide the support you need.

The NIS-2 directive is transforming the cybersecurity landscape. Here's a breakdown of its key characteristics:

Expanded Scope of Cybersecurity Regulation

The scope of cybersecurity regulations has expanded beyond operators of critical infrastructures (Kritis) in sectors like energy, IT, healthcare, and finance. With the introduction of the NIS-2 Directive and NIS2UmsuCG, new industries such as chemical production, food distribution, and various manufacturing sectors now fall under these regulations. This includes subsectors like the production of data processing equipment, electrical devices, and motor vehicles. Additionally, small and medium-sized enterprises (SMEs) with over 50 employees or a turnover exceeding €10 million may now be impacted. As a result, an estimated 25,000 companies will be newly subject to cybersecurity requirements.

All-hazards Risk Management

A comprehensive all-hazards risk management approach is essential for addressing various threats, as required by Article 21 (NIS-2 Directive) and Section 30 (BSIG-E). This includes implementing policies for risk analysis, information system security, incident handling, business continuity (such as backup management and disaster recovery), and ensuring supply chain security through contractual agreements, incident handling, and patch management.

Supply Chain Impact

Suppliers and service providers, even those not directly covered by NIS-2, must adhere to NIS-2-compliant cybersecurity standards through contractual obligations. This ensures that the entire supply chain aligns with cybersecurity goals, promoting principles like security by design and security by default.

Stricter Standards for Operators of Critical Facilities

These entities must adhere to higher standards, including the use of attack detection systems though octoplant itself is not an attack detection system, it enhances the ability to detect and track attack patterns through software version analysis).

Additional Required Measures

- Network and information system security during acquisition, development, and maintenance
- Vulnerability handling and disclosure
- Cyber hygiene practices and regular cybersecurity training
- Use of cryptography and encryption policies where appropriate
- Human resources security, access control, and asset management policies
- Use of multi-factor authentication, secured communications, and emergency communication systems

Management Accountability

Cybersecurity is now a key responsibility of senior management. Management bodies are required to implement and oversee risk management measures actively, participate in regular training, and maintain sufficient knowledge to identify and assess risks in information security. Passive roles are no longer acceptable—cybersecurity must be actively managed at the highest levels.

Large companies or institutions violating cybersecurity obligations face fines up to €10 million or 2% of global annual turnover. If important entities with cybersecurity deficits don't comply with BSI orders by the deadline, their operating license may be partially or fully suspended, and unreliable management may be temporarily barred. Management bodies violating cybersecurity obligations are liable for any damages caused.

Stricter Reporting Requirements for Cyber Incidents under NIS-2

In the event of a significant security incident, entities must follow a strict reporting process to the Federal Office for Information Security (BSI), which includes:

- Early Warning: Submitted within 24 hours of identifying the incident.
- Detailed Incident Report: Provided within 72 hours of discovery.
- Intermediate Report: May be requested during the investigation.
- Final Report: Submitted within one month, detailing the threat, root cause, and corrective measures taken or planned.

The NIS-2 directive enhances protection for IT and OT systems against cyberattacks by boosting system resilience. Octoplant helps ensure your IT and OT infrastructure meets the necessary compliance standards.

Enhanced Security Profile

Octoplant enables manufacturers to proactively manage vulnerabilities, mitigating risks associated with production downtime, data breaches, and unauthorized access.

Business Continuity

With octoplant, individual devices or the entire production facility can be quickly returned to a valid state, minimizing downtime, reducing disruptions, and allowing for error or manipulation reversal.

CVE Mapping and Assessment

With access to criticality scores and detailed asset information, customers can prioritize and address high-risk vulnerabilities, ensuring a targeted and effective cybersecurity strategy.

Compliance Management

Octoplant ensures NIS-2 compliance by enhancing production transparency with configuration and asset management, enabling quick recovery, and reducing downtime.

EFA Automazione, parte del gruppo Relatech, opera da 30 anni in ambito di automazione industriale con prodotti, soluzioni e know how dedicati al mondo della connettività per l'integrazione di sistemi.
La sinergia con Relatech rende EFA un polo dotato di competenze, tecnologie e assets a 360 gradi in ambito di convergenza IT/OT, attraverso il quale le aziende possono accedere alle tecnologie digitali più avanzate.

OCTOPLANT PREFERRED PARTNER

efa.it