MEDIALINE

IT Security

NIS 2 - The new cybersecurity directive

Effective cybersecurity - responsibility for management and companies

The EU's NIS 2 Directive places new requirements on cybersecurity in companies. This data-sheet highlights the most important changes, obligations and risks and provides solutions to ensure compliance.

Critical sectors and risks affected

The directive applies to organizations in sectors classified as either high criticality (essential entities) or other critical sectors (important entities):

Sectors of High Criticality (Essential Entities):

- Energy (electricity, district heating and cooling, oil, gas, hydrogen)
- Transport (air, rail, water, road)
- Banking
- Financial Market Infrastructures
- Health (including manufacture of pharma-ceutical products, vaccines)
- Drinking Water
- Waste Water
- Digital Infrastructure (internet exchange points, DNS service providers, TLD name registries, cloud computing providers, data centers, content delivery networks, trust service providers, public electronic communication services)
- ICT Service Management (managed service pro-viders, managed security service providers)
- Public Administration
- Space

Other Critical Sectors (Important Entities):

- Postal and Courier Services
- Waste Management
- Chemicals
- Food Production
- Manufacturing (medical devices, computers, elec-tronics, machinery, motor vehicles, trailers)
- Digital Providers (online marketplaces, search en-gines, social networking platforms)
- Research Organizations

The effects of NIS 2

- **Extended management responsibility**
  Executives are responsible for developing, implementing and monitoring safety strategies. Non-compliance can result in personal liability (only applies to managing directors, not team or department heads).
- **Increased accountability**
  Companies must regularly document their security measures and prove compliance to the authorities.

⚠ Associated risks

- Greater vulnerability to cyber attacks
- Increase in reporting obligations for security incidents
- Damage to reputation and brand in the event of security breaches

Core obligations under NIS 2

Incident reports

- Obligation to report security incidents within 24 hours.
- Detailed follow-up reports are required within 72 hours.

Implementation of safety standards

- Introduction of technical and organisational measures for risk analysis and mitigation.
- Regular safety checks and audits.

Consequences of non-compliance

Sanctions:

- Fines up to **€10 million** or **2%** of annual global turnover for **essential entities**
- Fines up to **€7 million** or **1.4%** of annual global turnover for **important entities**

Reputational risks:
Loss of trust among customers and partners.

Operational effects:
Downtime due to inadequate IT security.

Our solution for your compliance

We support you in implementing the NIS 2 requirements:

Analyse your status quo:
Identification of weak points and risks.

Development of security concepts:
Customised strategies for compliance with the directive.

Training courses and workshops:
Sensitisation of management and employees.

Implementation and monitoring:
Introduction of robust IT security measures and continuous monitoring.

Act now!

Protect your company proactively to avoid sanctions and minimize risks.
Contact us for more information at **sales@medialine.com**