SANS

ICS SECURITY

The differences between the original EU NIS *(Network and Information Systems)* Directive and the updated NIS2 Directive.

The NIS Directive, adopted in 2016, was the first EU-wide legislation on cybersecurity. Its main goal was to establish a common level of security for network and information systems across the European Union. The NIS2 Directive is an updated and more comprehensive version of the NIS Directive, aiming to address the shortcomings of the original legislation and to adapt to the evolving digital landscape.

Key differences between the NIS Directive and NIS2 Directive include:

1. ***SCOPE:*** The NIS2 Directive expands the scope of the original NIS Directive, covering a broader range of entities. It now includes more sectors and organizations, such as medium-sized companies, public entities, and digital service providers that were not covered under the original directive.
2. ***ESSENTIAL AND IMPORTANT ENTITIES:*** The NIS2 Directive introduces a distinction between Essential Entities (previously Operators of Essential Services in NIS) and Important Entities. Essential Entities are subject to stricter requirements, while Important Entities have more flexible obligations.
3. **HARMONIZED SECURITY REQUIREMENTS:** The NIS2 Directive provides more harmonized and specific security requirements across the EU member states, aiming to create a more consistent approach to cybersecurity. It establishes minimum cybersecurity baseline measures that entities must follow and report on.
4. ***INCIDENT REPORTING:*** The NIS2 Directive introduces stricter and clearer rules for incident reporting. It sets out explicit timeframes for reporting incidents (within 24 hours of detection) and the need for entities to provide follow-up reports. It also expands the scope of incidents that must be reported.
5. ***SUPERVISION AND ENFORCEMENT:*** The NIS2 Directive enhances the role of national competent authorities and Computer Security Incident Response Teams (CSIRTs) in supervising and enforcing the rules. It introduces the possibility of cross-border collaboration and joint investigations for incidents affecting multiple member states.
6. ***PENALTIES:*** The NIS2 Directive introduces more stringent penalties for non-compliance, including fines that can be as high as 10 million euros or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. ***SUPPLY CHAIN SECURITY:*** The NIS2 Directive emphasizes the importance of securing the supply chain and requires Essential and Important Entities to assess the cybersecurity risks associated with their suppliers and service providers.

These are some of the main differences between the original NIS Directive and the updated NIS2 Directive. The NIS2 Directive aims to enhance the overall cybersecurity posture of the European Union by addressing the shortcomings of the original legislation and adapting to the evolving digital landscape.

NIS DIRECTIVE VS NIS2 DIRECTIVE

01 SCOPE

- **NIS Directive:** Limited to essential services and digital service providers
- **NIS2 Directive:** Expanded to include more sectors, medium-sized companies, and public entities

02 ENTITY CLASSIFICATION

- **NIS Directive:** Operators of Essential Services
- **NIS2 Directive:** Essential Entities *(stricter requirements)* and Important Entities *(more flexible obligations)*

03 SECURITY REQUIREMENTS

- **NIS Directive:** General cybersecurity measures
- **NIS2 Directive:** Harmonized, specific requirements, and minimum cybersecurity baselines

04 INCIDENT REPORTING

- **NIS Directive:** General reporting rules
- **NIS2 Directive:** Stricter rules, 24-hour reporting, follow-up reports, and expanded scope of incidents

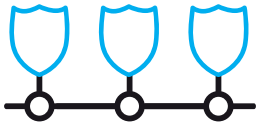
05 SUPERVISION & ENFORCEMENT

- **NIS Directive:** National competent authorities and CSIRTs
- **NIS2 Directive:** Enhanced roles, cross-border collaboration, and joint investigations

06 PENALTIES

- **NIS Directive:** Variable penalties
- **NIS2 Directive:** Fines up to 10 million euros or 2% of global annual turnover *(whichever is higher)*

07 SUPPLY CHAIN SECURITY



- **NIS Directive:** Not emphasized
- **NIS2 Directive:** Focus on assessing and securing supply chain risks

Would you like to discover how SANS can help you prepare for these developments or how we can help you train your team(s) and become compliant with this new directive?

Find out more on sans.org/ics

SANS | GIAC CERTIFICATIONS