tenable®

Embarking on the NIS2 Compliance Journey

Embarking on the NIS2 Compliance Journey

Operators of essential services in the European Union (EU) must comply with the NIS2 Directive, with this directive affecting at least 500% more organizations than its predecessor.

Learn the key reasons to prepare for NIS2 and gain insights into achieving compliance.

Strengthening EU Cyber Capabilities

In an effort to elevate the cybersecurity resilience of EU member states, NIS2 fosters cross-border collaboration to enhance information flow on incidents, threats, and vulnerabilities. This initiative complements existing EU regulations, such as GDPR, the Cybersecurity Act, DORA, and the Cyber Resilience Act.

Evolution from NIS to NIS2

The NIS Directive aimed to bolster the EU's resilience to cyber threats. However, recognizing challenges, the EU introduced the NIS2 Directive in December 2022, addressing previous issues and fortifying cybersecurity. NIS2 broadens the scope, introduces more robust incident reporting, introduces potential sanctions, mandates training and emphasizes use of encryption.

Key Dates

The NIS2 Directive (Directive 2022/2555) became effective on January 16, 2023. EU member states must transpose NIS2 Directive rules into their national laws by October 17, 2024. This means integrating the directive's regulations and requirements into national legislation. Member states must identify and register essential and important entities falling within the NIS2 Directive's scope by April 17, 2025. This involves identifying organizations covered by the directive and registering them accordingly.

Scope Expansion in NIS2

While sectors covered by the original NIS Directive remain, NIS2 adds eight new sectors. A new size-cap rule simplifies identification as a critical service, encompassing Essential and Important Entities.

ESSENTIAL ENTITIES	IMPORTANT ENTITIES
Energy	Postal and Courier Services
Transport	Waste Management
Banking	Chemicals (Manufacture, Production and Distribution)
Financial Market Infrastructures	Food (Production, Processing and Distribution)
Health	Manufacturing
Drinking Water	Digital Service Providers
Waste Water	Research
Digital Infrastructure	
ICT Service Management (MSPs and MSSPs)	
Public Administration	
Space	

Your organization falls within its scope if it belongs to Essential Entities with over 250 employees and an annual turnover above 50 million EUR, or a balance sheet over 43 million. Alternatively, Important Entities with over 50 employees and an annual turnover or balance sheet above 10 million EUR are included. The European Commission expects a 500% increase in organizations within the NIS2 scope, indicating a higher likelihood of impact compared to the first NIS Directive.

NIS2 Directive Security Measures

Organizations within scope must adhere to Chapter IV, Article 21 of the NIS2 Directive for cybersecurity risk management and reporting obligations. It underscores a systematic, risk-based approach to minimize cyber incidents and outlines essential security measures all organizations must implement to safeguard their network and information systems.

NIS2 Directive security measures which all affected organizations should adopt are below:

A. policies on risk analysis and information system security;
B. incident handling;
C. business continuity, such as backup management and disaster recovery, and crisis management;
D. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
E. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
F. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
G. basic cyber hygiene practices and cybersecurity training;
H. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
I. human resources security, access control policies and asset management;
J. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Reporting Obligations

In addition to security measures, organizations within NIS2 scope must adopt a risk-based approach and comply with reporting obligations. These obligations aim to enhance cyber capabilities across EU member states through cross-border collaboration, ensuring swift information dissemination on incidents, threats, and vulnerabilities.

Reporting Process

- Early Warning: Organizations encountering significant incidents must promptly alert the nation's CSIRT or the relevant competent authority.
- Timely Submission: Warnings should be issued within 24 hours of incident awareness.
- Initial Report: Within 72 hours, submit a report detailing the incident's initial assessment, including impact, severity, and indicators of compromise.
- Final Report: Within one month, create a comprehensive report covering cross-border impact, ongoing mitigation measures, and the incident's root cause.

Consequences of Non-Compliance

Supervisory capabilities increase in NIS2, making audits more likely. Non-compliance may result in administrative fines, temporary management suspension, and reputational damage.

Fines vary based on organizational categorization—essential or important entity. The maximum is €10,000,000 or 2% of total annual turnover for essential entities and €7,000,000 or 1.4% of total annual turnover for important entities. Non-compliance may also result in the temporary suspension of top management.

Why Start Now

EU member states must implement the NIS2 Directive by October 17, 2024. Organizations within the scope must comply by October 18, 2024. Early preparation is essential to meet obligations promptly.

Getting Started

First of all, make a thorough analysis of whether or not your organization is within the scope of the NIS2 Directive. After this is done, you should follow the national discussion regarding the NIS2 Directive to get a better picture of how it will be implemented into your national law.

If you have identified that your organization is within the scope of the NIS2 Directive you should review and audit your vulnerability management program. Risk-based vulnerability management is a proactive approach to cybersecurity that considers the likelihood of a vulnerability being exploited and the potential impact of events when deciding which vulnerabilities to remediate.

Risk-based vulnerability management also includes detailed documentation and reporting of identified vulnerabilities, their associated risks, and the steps taken to address them. This information is critical for the incident reporting requirements of NIS2.

How Tenable Helps

Inventorying the complete attack surface and then removing vulnerabilities and misconfigurations is fundamental to any program to manage the risk posed to the security of network and information systems. An effective exposure management program helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to support optimal business performance. Tenable delivers the capabilities described below to help entities manage risk across their complete attack surface.

Tenable offers a range of cybersecurity products designed to help you establish compliance with the NIS2 Directive. With its comprehensive suite of products, Tenable covers many aspects required by NIS2. User-friendly interfaces and intuitive tools simplify the process, addressing compliance measures with ease. Tenable provides expert support and guidance to assist tailoring solutions to the needs of the customer.

1. **Vulnerability Management**: Tenable's solutions help organizations identify and address vulnerabilities in their network and information systems. This is crucial for complying with NIS2, which requires organizations to implement measures to manage and mitigate cyber risks.
2. **Risk Assessment**: Tenable's tools assist organizations in conducting risk assessments and evaluating the effectiveness of their cybersecurity risk management measures.
3. **Continuous Monitoring**: Tenable's solutions offer continuous monitoring capabilities, allowing organizations to keep a constant watch on their network and information systems. This is important for detecting and responding to incidents as required by NIS2.
4. **Incident Detection and Response**: Tenable's tools help aid in the detection of cybersecurity incidents, helping organizations meet NIS2's incident reporting requirements. Quick incident detection and response are essential for compliance.
5. **Compliance and Reporting**: Tenable solutions include reporting features that help organizations demonstrate compliance with various cybersecurity regulations. This can be valuable for NIS2 compliance, as organizations are required to report incidents and maintain proper documentation.
6. **Security Hygiene Practices**: Tenable solutions may support organizations in implementing basic cyber hygiene practices and cybersecurity training, which are required by NIS2.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at tenable.com.

With Tenable's exposure management solutions, you can translate technical asset, vulnerability and threat data into clear business insights and actionable intelligence for compliance initiatives or security executives. Combine broad exposure coverage spanning IT assets, cloud resources, containers, web apps and identity platforms, with threat intelligence and data science. This allows you to focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

Final Thoughts

While the above steps can help you begin to navigate the complexities that this new directive brings, there are other considerations that organizations must consider while preparing and implementing policies aligned with NIS2. The NIS2 compliance journey requires effort and it is essential not only for legal adherence, but also for strengthening your organization's cybersecurity posture.

Tenable offers a feature-rich toolset to enhance cyber resilience and addresses many NIS2 requirements effectively, providing solutions for organizations navigating the complexities of compliance. Tenable can help your organization with compliance readiness across vulnerability management, identity security, cloud security, and more.

For more information on how Tenable can help your organization, check out our Tenable Products and NIS2 Directive solutions pages. Are you not sure where to start, or need assistance in your security journey? Feel free to reach out. Contact us at sales@tenable.com or visit tenable.com/contact

Copyright

tenable®