Teleport

Achieving NIS2 Directive Compliance Requirements with Teleport

Contents

Understanding the NIS2 Directive 3

Who Must Comply with NIS2? 3

Key Cybersecurity Measures Under NIS2 4

Non-Compliance Consequences: Significant Financial and Operational Risks 5

NIS2 Compliance is an Opportunity, Not Just an Obligation 6

Looking Ahead: The Future of Cybersecurity in the EU 6

How Teleport Can Help with NIS2 Requirements 7

Eliminating Credentials and Standing Privileges 7

Monitoring and Responding to Weak Access Patterns. 8

Managing Policy and Incident Intervention 8

Modernizing Privileged Access: Boosting Productivity Alongside Security. 9

Seamless Integration with NIS2's Reporting and Monitoring Requirements 9

Conclusion 10

The EU's revised Network and Information Security (NIS2) Directive has expanded its scope to bolster cybersecurity measures across essential services and critical entities throughout the EU.

While this framework sets the stage for a new era of resilience, it also brings new complexities organizations must navigate in order to earn and maintain compliance.

Understanding the NIS2 Directive

The NIS2 Directive is a groundbreaking regulation designed to bolster the cybersecurity posture of essential and important entities across the EU. By expanding upon its predecessor, NIS1, the directive introduces more comprehensive requirements and extends its reach to cover a broader range of organizations. Whether your firm is a part of the energy, healthcare, finance, or digital infrastructure sectors, if you're operating in the EU and meet certain criteria, NIS2 likely impacts your organization.

NIS2 mandates that covered entities adopt a risk-based approach to cybersecurity with a focus on preventing, mitigating, and reporting security incidents. This shift ensures that organizations are not only prepared to handle the inevitable cybersecurity threats but are also able to minimize the impact of breaches and recover swiftly. Member States have until October 17, 2024 to transpose the NIS2 Directive into national law, which means that covered organizations will be legally obligated to comply in early Q4 2024.

Who Must Comply with NIS2?

The directive applies to organizations with more than 250 employees, annual turnover (revenue) exceeding €50 million, or balance sheets over €43 million. Smaller, but still significant entities with more than 50 employees and a turnover or balance sheet above €10 million are also included. If your organization fits these criteria and operates in a sector deemed essential to societal functions or the economy, you are required to adhere to the stringent cybersecurity and reporting measures set forth by NIS2.

Essential Entities Covered

- Banking
- Digital Infrastructure
- Drinking Water
- Energy
- Financial Infrastructure
- Healthcare
- ICT Service Management (MSPs/MSSPs)
- Public Administration
- Space
- Transport

Important Entities Covered

- Chemicals (Distribution, Manufacture, Production)
- Digital Service Providers
- Food (Distribution, Manufacture, Production)
- Manufacturing
- Research
- Postal and Courier Services
- Waste Management

Key Cybersecurity Measures Under NIS2

Organizations within the scope of NIS2 must implement robust security measures across their network and information systems. These measures aren't just regulatory checkboxes; they represent industry best practices that can significantly enhance your organization's cybersecurity defenses.

Critical NIS2 measures include:

- **Comprehensive Risk Analysis and Security Policies:** Develop and maintain policies that provide a thorough analysis of risks and ensure your information systems are secure.
- **Incident Handling Procedures:** Ensure rapid detection, response, and mitigation of cybersecurity incidents to minimize disruption and damage.
- **Business Continuity and Crisis Management:** Implement backup management, disaster recovery strategies, and crisis response procedures to ensure operations can continue during and after an attack.
- **Supply Chain Security:** Strengthen security relationships with suppliers and service providers to mitigate risks from third parties.
- **Secure System Development and Vulnerability Management:** Ensure that all systems are securely developed, maintained, and that vulnerabilities are handled and disclosed appropriately.
- **Cyber Hygiene and Employee Training:** Establish basic cyber hygiene practices and ensure that staff are trained to recognize and respond to potential threats.
- **Use of Cryptography and Encryption:** Where appropriate, deploy cryptographic measures to protect sensitive data and communications.
- **Access Control and Asset Management:** Implement strict policies for human resources security, access control, and asset management to protect critical infrastructure.
- **Multi-Factor Authentication and Secure Communications:** Adopt multi-factor authentication (MFA) or continuous authentication solutions to protect access, as well as secure communication systems for emergencies.

These measures ensure organizations subject to NIS2 not only meet regulatory requirements, but are positioned to build stronger and more resilient cybersecurity postures that protect critical data and operations.

NIS2 Reporting Process: Proactive Incident Management

One of the standout features of the NIS2 Directive is its focus on timely and transparent incident reporting. Unlike its predecessor, NIS2 creates a clear and rigorous reporting process to ensure that significant cybersecurity incidents are reported swiftly to the relevant authorities. This allows for rapid containment, mitigates potential damage, and provides authorities with the information they need to assess cross-border impacts.

- **Early Warning:** Organizations must notify the relevant Computer Security Incident Response Team (CSIRT) or other competent authorities within 24 hours of becoming aware of a significant incident.
- **Initial Report:** Within 72 hours, an initial report must be submitted, detailing the severity, impact, and Indicators of Compromise (IOCs) of the incident.
- **Final Report:** A comprehensive final report must follow within one month, outlining the root causes, mitigation measures, and cross-border impacts of the incident.

These tight timelines not only push organizations to enhance their cybersecurity capabilities but also ensure a coordinated, EU-wide effort to prevent and mitigate cyber threats.

Non-Compliance Consequences: Significant Financial and Operational Risks

Failure to comply with NIS2 can have far-reaching consequences. Beyond the risk of increased vulnerabilities and cybersecurity breaches, non-compliant organizations face severe financial penalties. Essential entities can be fined up to €10 million or 2 percent of global annual turnover, while important entities risk fines of up to €7 million or 1.4 percent of turnover.

These costs go beyond fines — reputational damage, potential management suspensions, and increased scrutiny from regulatory audits all loom large for organizations should they fall short of these requirements.

With the directive's enhanced supervisory powers, regulators will have greater capacity to audit and enforce these penalties, ensuring that cybersecurity is taken seriously at all levels of the organization.

NIS2 Compliance is an Opportunity, Not Just an Obligation

Far from being a bureaucratic burden, NIS2 compliance offers a unique opportunity for organizations to modernize and strengthen their security posture. By adhering to these comprehensive requirements, companies can:

1. **Build resilience** against increasingly sophisticated cyber threats
2. **Foster trust with customers and partners** by demonstrating a proactive approach to security
3. **Improve operations** through harmonized risk management and reporting processes
4. **Gain a competitive edge** within markets where cybersecurity maturity is valued as a differentiator

Looking Ahead: The Future of Cybersecurity in the EU

As the cyber threat landscape evolves, so too must the defenses and resilience strategies of Europe's essential industries. NIS2 is not just a regulatory framework, it's a cornerstone for the EU's commitment to build a secure and resilient digital ecosystem. For organizations that embrace these requirements and prioritize cybersecurity, NIS2 offers the blueprint to navigate the future with confidence.

How Teleport Can Help with NIS2 Requirements

Key areas of the NIS2 Directive focus on secure access controls, robust incident response, risk management, and auditing capabilities. Teleport's comprehensive suite of secure infrastructure access solutions — including Teleport Access, Teleport Identity, and Teleport Policy — align directly with these mandates, helping organizations meet compliance while simultaneously improving operational efficiency and productivity.

Eliminating Credentials and Standing Privileges

The NIS2 Directive emphasizes the need for secure access control mechanisms to protect network and information systems, with a particular attention on minimizing unauthorized access. Teleport eliminates the need for credentials and standing privileges, reducing the risk of compromised credentials — a leading cause of data breaches.

By leveraging cryptographic-based, ephemeral credentials, Teleport eliminates static passwords, SSH keys, and long-lived tokens, which are often the target of cyberattacks.

- **Meet NIS2 Access Control Requirements:** The directive mandates strong access control, and by eliminating standing credentials, Teleport enforces the principle of least privilege. This ensures that users only have access to the systems they need when they need it, and no persistent access can be exploited by attackers. This also promotes a Zero Trust Architecture (ZTA) that specifies that no endpoint or user should be trusted until verified.
- **Secure Remote Access:** Teleport enables secure, remote access to applications and workloads from anywhere in the world, which is crucial for organizations with distributed teams or those that rely on external partners. This aligns with NIS2's focus on securing supply chain relationships and remote services.
- **Cryptographic Identity Security:** Teleport leverages short-lived cryptographic identities to assign access to users, machines, and workloads, eliminating the need for credentials or secrets by requiring authentication. This aligns with NIS2's requirements on the utilization of cryptographic security measures and continuous authentication to protect access.

Monitoring and Responding to Weak Access Patterns

Effective identity management is critical to the NIS2 Directive's requirements for secure access to sensitive systems. Teleport provides robust monitoring and real-time response capabilities to ensure the integrity of user access.

- **Weak Access Pattern Monitoring:** Teleport continuously monitors access patterns, identifying anomalies or signs of potential compromise, such as unusual login locations or excessive access requests. This proactive approach helps organizations adhere to NIS2's requirement for continuous monitoring and incident detection.
- **Compromised User Lockouts:** When compromised users or malicious activity is detected, Teleport can automatically lock these accounts, limiting the risk of a broader security breach. This capability aligns with NIS2's requirement for rapid incident response and containment.
- **Access Requests and Reviews:** Teleport enables just-in-time access requests, where users must request specific access that is time-limited and subject to approval. This minimizes the risk of unauthorized access and satisfies NIS2's mandate for controlled and auditable access to critical systems. Regular access reviews ensure that privileges are kept up to date and unnecessary permissions are revoked.

Managing Policy and Incident Intervention

The NIS2 Directive requires organizations to implement comprehensive cybersecurity policies and have the ability to intervene swiftly during cybersecurity incidents. Teleport helps organizations develop, monitor, and enforce policies across their entire infrastructure, ensuring compliance and rapid response to emerging threats.

- **Analyzing Access Relationships:** Teleport provides visibility into the web of access relationships across an organization, helping administrators understand who has access to what, and identifying potential risks or unauthorized access points. This level of transparency is crucial for meeting NIS2's requirements for access review and risk analysis.
- **Incident Intervention:** In the event of a security threat, Teleport allows administrators to intervene in real time by modifying or revoking access, implementing additional security measures, or isolating compromised systems. This ensures compliance with NIS2's emphasis on rapid response to cyber incidents.
- **Unified Policy Management:** Teleport enables the creation and application of security policies across all systems and infrastructure, from cloud environments to on-premises data centers. This unification simplifies the enforcement of consistent security standards, as required by NIS2, while reducing the complexity often associated with managing disparate environments.

Modernizing Privileged Access: Boosting Productivity Alongside Security

One of the unique challenges many organizations face is achieving the ideal balance between securing privileged access and maintaining engineering productivity. Teleport's approach to modernizing privileged access not only enhances security, but also increases the productivity of engineers and developers who need timely access to infrastructure in order to complete their work.

- **Identity-Centric Infrastructure Access:** Unlike traditional systems that rely on static credentials and manual processes, Teleport is built on a foundation of identity security. Engineers and developers can access infrastructure easily through their authenticated identity, eliminating the risks posed by credential management or constant manual oversight. This streamlined approach supports NIS2's mandates for automation and reduced human error, which are key components in mitigating security risks.
- **Time-to-Market and Security Alignment:** By simplifying access management, Teleport reduces the operational burden on engineers and developers, allowing them to focus on innovation and core business objectives. This increase in efficiency supports not only compliance, but also key organizational goals — accelerating time-to-market objectives while ensuring security and compliance do not generate friction for critical business operations.

Seamless Integration with NIS2's Reporting and Monitoring Requirements

The NIS2 Directive places heavy emphasis on incident reporting and maintaining comprehensive logs of access and system changes. Teleport's platform automatically logs every access request, session, and action, providing an auditable trail that meets the reporting requirements under NIS2.

- **Incident Reporting:** Should a cybersecurity incident occur, Teleport's detailed logs can quickly provide the necessary information to report the incident to national Computer Security Incident Response Teams (CSIRTs) within the 24-hour timeframe specified in NIS2 requirements.
- **Compliance Audits:** Teleport's automated, centralized logging system makes audit preparation simple, allowing organizations to demonstrate their compliance with NIS2's requirement for documented access controls, security measures, and incident responses.
- **Integrations with SIEM Tools:** Teleport integrates reporting with popular SIEM tools like Datadog and Splunk.

Conclusion

Teleport's integrated solutions for access control, identity management, and policy enforcement also provide a seamless path to NIS2 compliance. By eliminating standing credentials, enabling secure remote access, continuously monitoring user activity, and managing security policies across all infrastructure, Teleport addresses key requirements of the NIS2 Directive — all the enhancing engineering and development productivity.

For organizations looking to meet these evolving cybersecurity standards, Teleport offers a unified, scalable, and efficient solution that not only ensures compliance but also strengthens the overall cybersecurity resilience of your organization.

About Teleport

Teleport modernizes infrastructure access, improving efficiency of engineering teams, fortifying infrastructure against bad actors or error, and simplifying compliance and audit reporting. The Teleport Access Platform delivers on-demand, least privileged access to infrastructure on a foundation of cryptographic identity and zero trust, with built-in identity security and policy governance.