cloudm

Ensuring compliance with NIS2

A comprehensive guide to data backup and security for IT professionals

cloudm.io

Contents

Introduction

The Network and Information Systems (NIS) Directive is a crucial part of the European Union's approach to enhancing cybersecurity across its member states. It aims to harmonize cybersecurity regulations across the EU, reducing fragmentation and ensuring a consistent level of security across member states.

The original directive, adopted in 2016, laid the groundwork for improving the overall security level of network and information systems within the EU. However, a rapidly evolving cyber threat landscape in which criminals leverage emerging technologies to carry out increasingly sophisticated attacks required a more comprehensive and robust framework, leading to the introduction of the NIS2 Directive.

In this guide, we explain the background, timeline and remit of NIS2. We summarize its key requirements and explore what organizations should do to ensure compliance.

In 2023, the global cost of cybercrime was estimated to be

$8.5 trillion.

[source: Statista]

What is the state of cybersecurity in the EU?

The cybersecurity threat landscape in the EU is dynamic and increasingly complex, encompassing a wide range of threats: from cybercrime to state-sponsored cyberattacks, and affecting individuals, businesses, and governments alike.

Cybercrime

Ransomware attacks remain one of the most significant threats, with criminals targeting businesses, critical infrastructure, and public institutions. Victims of ransomware attacks face dire consequences such as financial losses, operational disruptions, and reputational damage.

Phishing and social engineering are used to deceive individuals into revealing sensitive information or installing malware. Increasingly sophisticated, both individuals and organizations can be targets, with spear-phishing attacks often directed at high-value targets within organizations.

Financial fraud is also evolving, with cybercriminals exploiting vulnerabilities in online banking systems to steal money or credentials and leveraging cryptocurrencies for new forms of fraud such as Ponzi schemes and fake investment opportunities.

State-sponsored attacks

Espionage: government agencies, defense contractors, and critical infrastructure are primary targets for state-sponsored espionage. Threat actors use sophisticated malware and prolonged campaigns to gather intelligence to further their political or economic agenda.

Disinformation campaigns leverage social media to spread false information rapidly and widely. The motivation behind them is to influence public opinion, disrupt elections, and undermine trust in institutions.

According to the World Economic Forum's (WEF) 2023 Global Risks Report, cybersecurity is in the current and future top 10 risks globally, and the cost of cybercrime is projected to hit **US$10.5 trillion** annually by 2025.

Critical infrastructure

Industrial Control Systems (ICS) in sectors such as energy, water, transportation and manufacturing are increasingly targeted due to their critical nature. As the infrastructure often suffers from outdated security measures, attacks can lead to significant disruptions, physical damage, and safety risks.

Healthcare institutions are frequent targets due to the critical nature of their services and often inadequate cybersecurity defenses. Data breaches are particularly common as sensitive patient information is highly valuable on the black market.

Emerging technologies

The proliferation of Internet of Things (IoT) devices which often lack robust security measures offers criminals more opportunities to attack: devices can be hijacked for botnet attacks, espionage, or to cause physical damage.

The accelerated adoption of cloud services has introduced new security challenges, including misconfigurations and vulnerabilities in cloud infrastructure. Cloud-based data storage and processing can be argets for large-scale data breaches.

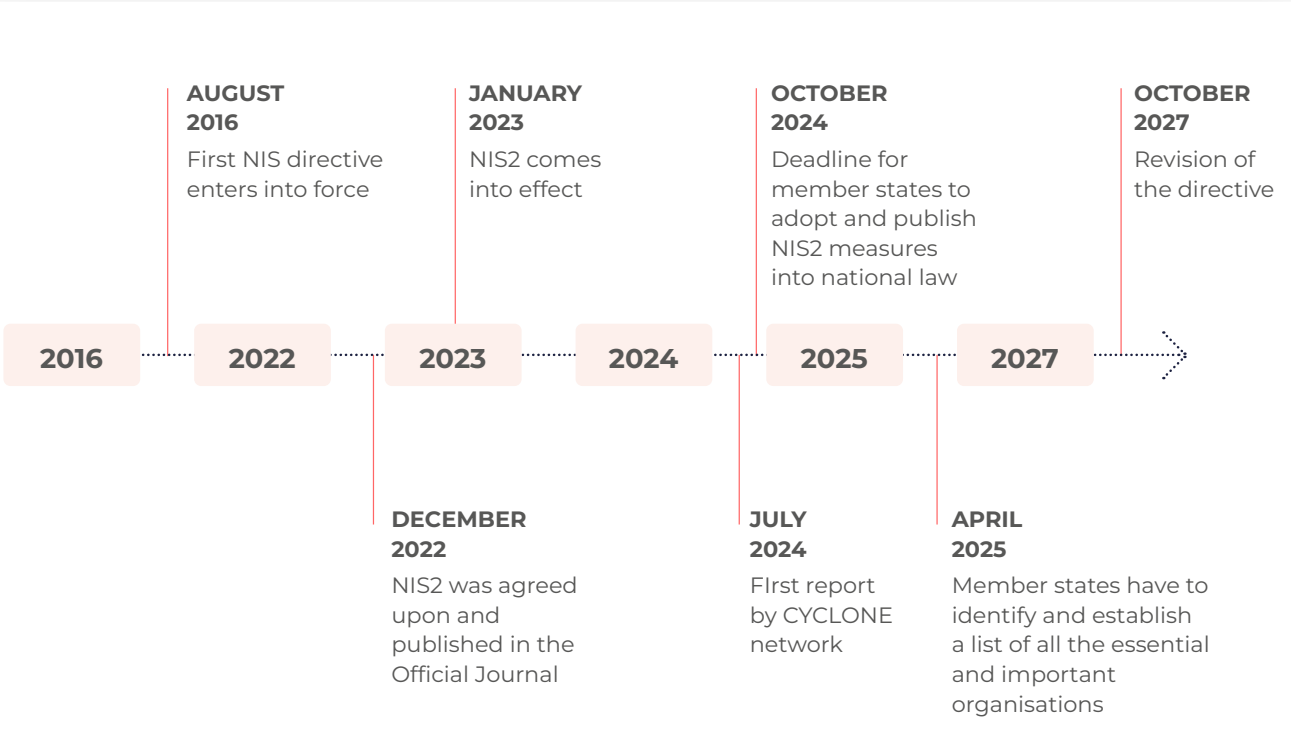
Supply chain attacks

Third-party vulnerabilities pose a major threat to organizations. High-profile incidents like the SolarWinds attack have highlighted the potential for widespread disruption via supply chain compromises.

What is NIS2 and when does it come into force?

NIS2 is a significant enhancement of the original 2016 directive. It aims to address the growing rate of digitization, the evolving cybersecurity landscape and the increasing threats to network and information systems. NIS2 broadens the scope, strengthens security requirements, and enhances cooperation among EU member states.

Published in December 2022, EU member states must adopt and publish the measures necessary to comply with the NIS2 directive by 17 October 2024 and apply those measures from 18 October 2024.



Who has to comply with NIS2?

NIS2 is not limited to EU-based organizations:

The directive applies to any organization that is considered essential or important (see below for details) AND provides services or undertakes activities within the EU.

NIS2 categorizes organizations into two main groups: essential and important entities.

Both groups have specific size thresholds, although an entity may still be considered "essential" or "important" even if it does not meet the size criteria. This can be the case if it is the sole provider of a critical service for societal or economic activity in a member state. Both essential and important entities must comply with NIS2, but the level of oversight and specific requirements may vary based on their categorization.

Essential entities:	Important entities:
Size threshold: varies by sector, but generally 250 employees, annual turnover of €50 million or balance sheet of €43 million	**Size threshold:** varies by sector, but generally 50 employees, annual turnover of €10 million or balance sheet of €10 million
Examples of essential entities Energy Banking Financial market infrastructures The health sector Digital infrastructure Information and communication service providers Providers of managed services and managed security	**Examples of important entities** Postal and courier services Waste management Manufacturing Providers of certain digital services (online marketplaces, search engines and social networking services) Research

What are the key requirements of NIS2?

NIS2 expands its scope to include more sectors than the original directive, covering critical areas like banking, healthcare, energy, transport, digital infrastructure, and public administration. It applies to medium and large organizations within these sectors and includes digital service providers such as cloud computing services, online marketplaces, and search engines.

NIS2 requires organizations to comply with stringent security requirements to manage risk and enhance security.

Organizations must implement stringent security measures, including risk management, incident handling, business continuity, monitoring, auditing, and testing. They are required to establish and update cybersecurity policies and ensure supply chain security by assessing and managing risks from third-party dependencies.

NIS2 defines how organizations have to notify authorities following incidents and what security mechanisms must be in place.

NIS2 mandates that organizations notify authorities of significant incidents promptly, detailing the nature, impact, and mitigation measures. An early warning system is established for timely information sharing and coordinated responses among member states.

Organizations must develop and maintain business continuity and disaster recovery plans, ensuring resilience and quick restoration of services after disruptions. They must also establish clear accountability for cybersecurity with designated roles and responsibilities, and regularly report on cybersecurity measures, incidents, and risk assessments.

EU member states will appoint national authorities responsible for the implementation and auditing of NIS2, with supranational networks coordinating between member states.

Each member state must designate national cybersecurity authorities to oversee NIS2 implementation, audit organizations, and impose sanctions for non-compliance. Member states must also impose effective penalties for non-compliance, including fines and corrective measures.

Enhanced cooperation and coordination are promoted through the European Cyber Crises Liaison Organization Network (EU-CyCLONe) and the Computer Security Incident Response Teams (CSIRTs) network.

How does NIS2 seek to strengthen business continuity?

NIS2 requires organizations to comply with stringent security requirements to manage risk and enhance security.

Organizations must implement stringent security measures, including risk management, incident handling, business continuity, monitoring, auditing, and testing. They are required to establish and update cybersecurity policies and ensure supply chain security by assessing and managing risks from third-party dependencies.

According to IBM's 2023 Cost of a Data Breach Report, the average cost of a cyber-breach is **US$4.45 million.**

Backup requirements under NIS2

NIS2 defines how organizations have to notify authorities following incidents and what security mechanisms must be in place.

NIS2 mandates that organizations notify authorities of significant incidents promptly, detailing the nature, impact, and mitigation measures. An early warning system is established for timely information sharing and coordinated responses among member states.

Organizations must develop and maintain business continuity and disaster recovery plans, ensuring resilience and quick restoration of services after disruptions. They must also establish clear accountability for cybersecurity with designated roles and responsibilities, and regularly report on cybersecurity measures, incidents, and risk assessments.

EU member states will appoint national authorities responsible for the implementation and auditing of NIS2, with supranational networks coordinating between member states.

Each member state must designate national cybersecurity authorities to oversee NIS2 implementation, audit organizations, and impose sanctions for non-compliance. Member states must also impose effective penalties for non-compliance, including fines and corrective measures.

Enhanced cooperation and coordination are promoted through the European Cyber Crises Liaison Organization Network (EU-CyCLONe) and the Computer Security Incident Response Teams (CSIRTs) network.

What are the consequences of non-compliance?

Non-compliance with NIS2 can lead to severe consequences, including substantial monetary fines based on the organization's turnover:

Essential entities may see penalties of up to €10 million or 2% of the global yearly revenue, whichever is the greater amount

For important entities, the fine can be up to €7 million or 1.4% of the annual global revenue, whichever the greater amount

One of the critical aspects of NIS2 is its focus on ensuring business continuity and effective incident response through stringent backup and recovery requirements. These requirements are designed to mitigate the impact of cyber incidents and enhance the resilience of critical infrastructure and essential services.

Backups are a fundamental component of any cybersecurity strategy, providing a safeguard against data loss due to cyber incidents, hardware failures, or human error. NIS2 emphasizes the importance of robust backup procedures to ensure the availability and integrity of data.

To comply with NIS2, organizations must implement the following:

Regular backups: NIS2 mandates regular backups of critical data to ensure that up-to-date copies are available and can be restored in the event of an incident. The frequency of backups should be determined based on the criticality of the data and the organization's risk assessment. Backup procedures should be tested regularly to ensure their effectiveness.

Offsite storage: to protect against physical disasters such as fires or floods and to ensure that backup data remains accessible even if the primary site isn't, NIS2 requires that backup data be stored offsite. This could involve cloud-based solutions or physically remote data centers.

According to a Verizon survey, 69% of consumers surveyed would avoid a company that had suffered a data breach, and

29% would never visit that business again

Data integrity and encryption: ensuring the integrity and confidentiality of backup data is paramount. NIS2 specifies that backups must be protected using encryption to prevent unauthorized access. Additionally, integrity checks should be implemented to ensure that the backup data has not been tampered with or corrupted.

Access controls: strict access controls should be in place to limit who can access backup data. This includes implementing multi-factor authentication (MFA) and ensuring that only authorized personnel can restore data from backups.

CloudM Backup enables organizations to comply with the requirements of the NIS2 directive and keep their vital business data safe.

With CloudM Backup, organizations are able to:

- **Ensure smooth disaster recovery and crisis management** by quickly restoring their Google Workspace data following a data loss event. CloudM Backup offers granular item and folder restoration as well as mass restoration of entire users or drives, enabling businesses to prioritize business critical data when it matters.
- Ascertain that their backup policies and processes are in line with internal guidelines and external regulatory requirements using **CloudM Backup's extensive logs, reporting dashboards and notifications.**
- **Remain in full control of their own data** by backing up to a GCP or AWS storage location of their choice.
- **Automate** many time-consuming, manual workflows while also reducing the risk for human error.
- **Know that their data is safe:** we use encryption standard AES-256 to secure your data in transit and at rest and are ISO 27001 certified. Our cloud storage complies with the strictest security standards and of course we follow secure coding practices, use code analysis tools and carry out 3rd party penetration tests.

Find out more

Official sources:

NIS2 Directive (Directive (EU) 2022/2555)
High level summary of NIS2 with associated links published by the European Commission
NIS2 FAQs published by the European Commission

cloudm

cloudm.io