cpl.thalesgroup.com

THALES
Building a future we can all trust

New Network and Information Security Directive NIS2

Help your organisation to comply with the European Union's NIS2 directive with Thales

NIS2: Tightens the Gaps in the Network and Information Security (NIS) directive

In 2016, the European Commission proposed the EU Network and Information Security (NIS) directive. The NIS directive was the first piece of EU-wide cybersecurity legislation. The goal was to enhance cybersecurity across the European Union. The NIS directive was adopted in 2016 and subsequently, since it was an EU directive, every EU member state had to adopt a national legislation, which followed or transposed the directive. However while contributing to improving cybersecurity, the 2016 NIS directive relied heavily on the discretion of individual member states, and lacked the accountability required.

On May 13th 2022, in order to respond to the growing threats posed by increasing digitalisation and the surge in cyber-attacks, the European Commission announced plans to replace the NIS Directive in order to strengthen security requirements and cyber resilience, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the European Union. The expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Before becoming effective in June 2024, the agreement has to be approved by the European Parliament and the Council.

With NIS2, the European Commission aims to strengthen the following:

Scale

- First, it significantly expands the scope of application, which is of major importance. Growing interconnectedness, rapid digitisation and ubiquitous connectivity mean more enterprises are becoming systemically important to defend from cyber risk. Redefining the original scope to now be more clear in covering "essential services" – including, transport, banking and public administration, and entities operating in these services such as food production, postal services and waste management – means cyber resilience measures will need to be taken at a much larger scale across the continent.

Governance

- Enhancing security governance and making senior managers in a business accountable for cyber resilience is also a major step. Accountability drives behavior and outlining that senior management needs to know security standards and oversee processes aligned to risk management practices, and sufficient to manage that risk, will drive change from top to bottom in an organisation. Cybersecurity has to be a board-level and senior management issue and not delegated to technical teams. Accountability will empower chief information security officers (CISOs), though it also comes with expectations that they can communicate effectively with senior management and be technical and business leaders.

Fines and sanctions

- Governance is especially important when combined with increased fines and broadening of sanctions. NIS2 mandates a more comprehensive set of powers to be conferred on competent authorities. They will be able to penalize at least equal to a fixed amount or 2% of worldwide turnover for essential entities. This is a significant incentive for businesses to make sure they are meeting their obligations. These new potential penalties will be a major lever for resilience in the EU and beyond.

Incident response obligations

- Finally, gaps have been closed and revisions made on incident response obligations. For example, what constitutes a "significant impact" on an entity has been clarified. It will no longer be a defined metric (number of impacted users) but rather whether there was disruption to critical services, or financial or material loss. Also, notifications have been reduced from 72 to 24 hours, and reporting will be to users of services and potentially the public. Taken together, these revisions to reporting obligations will incentivise greater responsibility to be cyber resilient and provide greater transparency to all parties affected by a potential breach. Disclosure drives responsibility. As outlined in NIS2, governance at this level can be a good thing for business and the economy. While many will look at these increasing responsibilities as a potential cost to business, building a more resilient digital ecosystem is a strategic necessity.

NIS2 Technical and Organisational Measures Focus Area Case Study

The NIS2 proposal includes a list of key elements that all companies must address or implement as part of the measures they take.

In particular, Article 18 - Cybersecurity risk management measures, calls for "entities shall take appropriate and proportionate technical and organisational measures" [Article 18(1)]. And adds that the "measures shall include at least the following":

- "supply chain security including (...) providers of data storage and processing services or managed security services" [Article 18(2d)] and
- "the use of cryptography and encryption" [Article 18(2g)]

What does that mean?

NIS2 holds organisations directly responsible. When outsourcing their Information Communications Technology (ICT) activities, for instance to process and store data in the cloud, organisations must apply additional "technical and organisational measures" to be able to indeed take their share of responsibility and thus compensate the loss of control (outsourcing).

Why Cryptography and Encryption?

Implementing cryptography and encryption is a way for organisations to enforce technical and organisational measures: encrypted data can no longer be accessed without additional information (a cryptographic key) and thus give organisations controls over their cloud-based assets.

Encryption and Key Management Systems (KMS) are "technical measures" and are managed by organisations, not the cloud provider, hence defined as "organizational measures".

NIS 2 Article 18

1. Member States shall ensure that essential and important entities shall take the appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems which those entities use in the provision of their services....
2. The measures referred to in paragraph 1 shall include at least the following:
   (a) risk analysis and information system security policies;
   (b) incident handling (prevention, detection, and response to incidents);
   (c) business continuity and crisis management;
   (d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as the providers of data storage and processing services or managed security services;
   (e) security in network and information security systems acquisition, development and maintenance, including vulnerability handling and disclosure;
   (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
   (g) the use of cryptography and encryption.

Affected Sectors

The main sectors affected by NIS2 include:

- Providers of public electronic communications networks or services
- Digital services such as social networking services platforms and data centre services
- Wastewater and waste management
- Space
- Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)
- Postal and courier services
- FMCG
- Public administration

Failure to comply with NIS2 can have the following ramifications for organizations:

- Fines up to 10 million EUR or 2% of the total global annual turnover
- Management liability
- Temporary bans against managers
- Designation of a monitoring officer

How Thales can help

Thales offers comprehensive data security solutions that help organisations to act in accordance with and be accountable towards the NIS2 directive

- **Protect transaction and personal data at rest:** Thales CipherTrust Manager, Luna Hardware Security Modules (HSMs) and the Data Protection on Demand (DPoD) marketplace, enable organisations to centrally manage encryption keys and deliver a variety of encryption, tokenisation and data masking solutions to protect transaction and personal data in files, folders, applications, and databases on premises, in the cloud, and across hybrid environments.
- **Encrypt financial and personal data in motion:** Thales High Speed Encryptors (HSE) provide your organization with a single platform to encrypt data in transit everywhere— from network traffic between data centres and the headquarters to backup and disaster recovery sites, whether on-premises or in the cloud.
- **Develop and maintain secure systems and applications:** Thales Luna HSMs, available on-premises and in the cloud as Luna Cloud HSM on DPoD, enable organisations to securely store signing material in a trusted hardware device, thus ensuring the authenticity and integrity of any application code files.
- **Implement strong access control measures:** Thales CipherTrust products can be setup for unique, multifactor administrative access to enterprise systems on-premises and in the cloud. In addition, SafeNet Trusted Access enables you to centrally manage unique user identities, risk-based authentication policies, and add/revoke access to systems across hybrid IT.
- **Track and monitor all access to sensitive data:** Designed to help ensure compliance, the suite of Thales data security solutions provide your organisation with the tools to help track and monitor access to data, and offer audit logs to verify such. For example the Thales CipherTrust data protection portfolio produce audit records that log any encryption key lifecycle operations (creation/deletion/rotation/revocation) and other administrative functions that can be used to reconstruct events.

Conclusion

The NIS2 directive aims to establish the minimum standards for cyber risk management and reporting obligations through a broader application than the present NIS Directive by including additional industries and both medium and large organisations. With more security measures required to be implemented to strengthen cybersecurity for key information and communication technologies, the affected organisations will also have the obligation to submit an initial notification within 24 hours to the relevant competent authority in case of any significant cyber threat. Failure to comply may result in EU member states conducting coordinated risk assessments of essential supply chains in collaboration with the Commission and the European Union Agency for Cybersecurity and resulting fines and sanctions.

Drawing on decades of experience helping corporate entities and public enterprises adhere to compliance mandates, Thales offers aforementioned products and services that enable organizations to strengthen their cybersecurity capabilities and cyber resilience, address the security of supply chains, streamline reporting obligations and comply with more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the European Union. In addition, Thales works closely with partners to offer comprehensive solutions that can reduce the scope of your compliance burden.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us