General Report

TREND MICRO

Best Practice Guide for Implementing NIS2

Prof. Dennis-Kenji Kipker

November 2023

Best Practice Guide for Implementing NIS2

01

What is NIS2 and why is NIS2 important for your business?

1. What is NIS2 and why is NIS2 important for your business?

NIS2 is the "Directive on measures for a high common level of cybersecurity across the Union" and is an **EU-wide cybersecurity legislation** designed to improve and unify the overall level of European cybersecurity. In terms of content, NIS2 (Directive 2022/2555) is based on the European NIS-1 Directive from 2016, which was primarily concerned with the IT security regulation of "critical infrastructures" and digital services. Since then, not only has the cyber threat situation worsened significantly, but the networking and use of cloud technology has also increased significantly. NIS2, which will replace NIS1, addresses this situation which has changed significantly, as well as the need for improved Union-wide cooperation on cybersecurity matters. Besides adapting the legally required cybersecurity measures, NIS2 also considerably expands the **target audience of the new European legal act**. Companies and institutions in the sectors listed below are generally affected:

Energy	**Transportation**	**Banking**
Financial market infrastructures	**Healthcare**	**Drinking water**
Sewage	**Digital infrastructure**	**Management of ICT services (business to business)**
Public administration	**Aerospace**	**Postal and courier services**
Waste management	**Production, manufacturing and trading in chemical substances**	**Production, processing and distribution of food**
Manufacturing/ Production of goods	**Digital service providers**	**Research**

As NIS2, just like the previous regulation, is an **EU directive**, it must first be implemented into national law to be effective for companies. A tight schedule applies in this respect, as NIS2 stipulates that it must be implemented into the law of the EU member states by October 17, 2024. NIS1 will then be repealed with effect from October 18, 2024. Therefore, **mid-October 2024 is the cut-off date** for the new EU cybersecurity requirements. With regard to the cybersecurity compliance of companies, it should be noted that NIS2 **is not the only European legal act** that deals with the topic. Cybersecurity can have many facets and application scenarios. Although NIS2 broadly covers many companies from a wide range of sectors, there are also **sector-specific legal acts**. Particularly worth mentioning in the financial sector is the "Digital Operational Resilience Act" **(Regulation 2022/2554, DORA)**, which contains sector-specific requirements for cyber protection. For the numerous companies that process personal data, the requirements for **data security from the GDPR** must be observed, as NIS2 essentially addresses the maintenance of the functionality of a company, that uses networked information technology processes. Looking ahead, another European legal act should be mentioned at this point. The draft of a **"Cyber Resilience Act" (CRA)** presented by the EU Commission in September 2022, is expected to impose further requirements on the cybersecurity of products with digital elements in the coming years. Overall, NIS2 represents only one – albeit important – component of the new European cybersecurity compliance architecture.

Practical tip: How NIS2 differs from other legal acts

Although NIS2 represents a core regulation of European cybersecurity compliance, it must always be checked whether sector-specific legal acts may take precedence. At the beginning of the respective regulations, important information is included in the scope of application detailing which legal regulation applies to which entity. In particular, the distinction between NIS2 and CRA in terms of content is clear: The NIS2 directive applies to companies, whereas the CRA regulation applies to products.

02

What specific requirements does NIS2 specify to improve cybersecurity in practice?

2. What specific requirements does NIS2 specify to improve cybersecurity in practice?

Article 14 of NIS1 defines the requirements for the security of network and information systems. It stipulates that operators of essential services must take appropriate and proportionate technical and organizational measures to "manage the risks to the security of the network and information systems they use for their activities". In addition, the directive specifies that these measures must ensure a level of security that is appropriate to the existing risk, taking into account the state of the art. According to NIS1, the impacts of security incidents that affect the provision of services must be prevented or the impacts should be minimized to maintain the availability of services.

Since **NIS2 is based on the content of NIS1**, the new European cybersecurity requirements are also centered around a risk-based approach, which can now be found in Article 21 and also incorporate various specific details and extensions. The affected institutions must take appropriate and proportionate **technical, operational and organizational measures** to reduce the risks to the security of the IT systems used for operation or service provision and to prevent or minimize the impact of security incidents on service recipients or other services. NIS2 refers not only to the **"state of the art"**, but also to the relevant European and international standards.

Practical tip: To Determining the "state of the art"

The much-cited "state of the art" is a general legal clause that requires interpretation and, by definition, falls within the triad of terms between "generally recognized rules of technology" and "state of the art in science and technology". The determination of the specific state of the art required to meet a legal requirement cannot therefore be determined abstractly or generally, but rather depends, for example, on the specific risk exposure of a company. In recent years, however, various guidelines have been published with tools for determining the current state of the art in cybersecurity, which can in principle also be used for NIS2.

03

Cost-benefit analysis in cybersecurity

3. Cost-benefit analysis in cybersecurity

The costs arising from the implementation measures in relation to the risks or the benefits achieved by a measure must also be included in the risk assessment as an **adequacy criterion**, as the European legislator is also aware that despite all the efforts made in this respect, **it is impossible to achieve 100% cybersecurity**. In addition, as part of the cybersecurity measures regulated by NIS2, **security incident reporting** must be taken into account, which is already specified by NIS1, but was further optimized by NIS2 based on the experience of previous years. The reporting system in particular requires that affected companies not only act in a reactionary manner to cybersecurity incidents, but also take measures in the spirit of a preventive management system, which can also include documentation and proof of the measures taken.

Practical tip: The "adequacy" of cybersecurity measures to be taken under NIS2

Cybersecurity measures must be proportionate and economical - NIS2 also does not require "cybersecurity at any price" and therefore does not impose a disproportionate financial and administrative burden on affected institutions. In general, however, a level of cybersecurity must be achieved that is appropriate to the existing risk. When assessing this proportionality, due consideration must be given to the following characteristics:

- Level of an entity's risk exposure
- Size of the entity
- Probability of security incidents occurring
- Severity of security incidents, including their social and economic impact (for example, also with regard to the security of supply)
- Technical standard and implementation costs

The adequacy assessment therefore requires a careful analysis of components, systems and processes as well as the associated risks. Appropriate mitigation measures can then be derived from the analysis carried out. However, based on these risk analysis criteria, it is also clear that there is no uniform standard for weighing risks. Rather, the risks can also depend to a large extent on the sectors and industries in which an entity or company operates or whether it provides services that are critical for society. It is also clear that the impacts of cybersecurity incidents, particularly in supply-related sectors, can extend far beyond the entity affected by NIS2. The following questions can therefore be helpful in determining the level of cybersecurity:

- What is an entity's criticality level?
- To what extent does an entity depend on networked IT systems in order to function?
- Does the functioning of the entity depend on the functioning of digital supply chains?
- Have there already been incidents in the past or is it likely that attacks will increase in the future?
- Is an entity particularly exposed in the public eye?
- What could potential attackers gain as a result of successfully compromising the system?

Overall, the result of a risk analysis naturally means that the measures derived from it must be suitable to actually reduce cybersecurity threats, and not just to reduce or prevent the economic consequences of a successful cyberattack. Therefore, for example, taking out a cyber policy alone may not be sufficient to meet the requirements.

In specifying concrete requirements for technical, operational and organizational measures, **NIS2 goes beyond the regulatory content of NIS1**. In particular, the **concept of a "all-hazards approach"** is pursued, which aims to protect not only the network and information systems themselves, but also the physical environment of these systems. This also clearly highlights the connection to the increasingly prevalent **hybrid threat situation**.

Practical tip: The hybrid threat situation and its influence on cybersecurity

With NIS2, the "all-hazards approach" comes into focus in addition to classic cybersecurity measures. This aims to protect networked IT systems and their physical environment from events such as

- Theft,
- Fire,
- Floods,
- Telecommunications or power outages,
- unauthorized physical access to information and data processing equipment, damage to this information and equipment, and any related unauthorized actions.

Countermeasures in this area can include access control, protection against system errors, human errors, malicious acts and natural phenomena.

The expanded regulatory content of NIS2 is also reflected in the corresponding national proposals for the implementing laws, in that it is no longer just a matter of avoiding disruptions in the IT systems and processes that are crucial for the functioning of the operated infrastructure, but rather to avoid any disruptions in the IT systems and processes that the entities use to provide their services. This is likely to result in adjustments to the risk management approach of those companies that are already affected by NIS1, for example.

04

Guidelines for effective risk assessment and the implementation of measures

4. Guidelines for effective risk assessment and the implementation of measures

For entities affected by NIS2, cybersecurity risk management measures should take into account the level of entity's dependence on network and information systems, as well as measures to identify any risks of a security incident, and to prevent, detect, respond to, recover from and mitigate security incidents and their consequences. The security of network and information systems should also extend to stored, transmitted and processed data. Cybersecurity risk management measures should provide for a systemic analysis that takes into account the human factor in order to obtain a complete picture of the security of the network and information system. The measures apply regardless of whether IT systems are maintained internally or their maintenance is outsourced. According to the NIS2 proposal, it will also be possible in the future to carry out risk assessments of critical supply chains coordinated by industry in order to identify the critical ICT services, systems or products as well as relevant threats and vulnerabilities for each sector.

Overall, it is the duty of European Member States to ensure that entities affected by NIS2 immediately take all necessary, appropriate and proportionate cybersecurity measures. In implementing the measures, the management bodies in particular are obliged by NIS2 to approve measures and monitor their implementation.

Practical tip: "Minimum catalog" for cybersecurity measures according to NIS2

In terms of a minimum catalog, NIS2 stipulates the following cybersecurity provisions:

- Concepts related to risk analysis and security for information systems
- Managing security incidents
- Maintenance of operations, such as backup management, disaster recovery and crisis management
- Supply chain security, including security-related aspects of the relationships between individual entities and their immediate vendors or service providers
- Security measures in the acquisition, development and maintenance of network and information systems, including management and disclosure of vulnerabilities
- Concepts and procedures for assessing the effectiveness of risk management measures in the area of cybersecurity
- Basic procedures in the area of cyber hygiene and training in the area of cybersecurity
- Concepts and procedures for the use of cryptography and, if necessary, encryption
- Personnel security, concepts for access control and management of systems
- Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and, where appropriate, secured emergency communications systems within the facility

By October 17, 2024, the European Commission shall adopt implementing acts defining the technical and methodological requirements for risk management measures in the area of cybersecurity for DNS service providers, TLD name registries, cloud computing service providers, data center service providers, operators of content delivery networks, managed service providers, managed security services providers, online marketplace providers, online search engines, social networking service platforms and trust service providers. NIS2 also contains the possibility for the adoption of further implementing acts to specify the measures for the essential and important facilities. However, the specific implementing acts do not emerge in a vacuum. Rather, they are based as closely as possible on European and international standards and relevant technical specifications for cybersecurity. Otherwise, NIS2 also refers to European and international norms and standards in information security for implementation, for example explicitly to the ISO/IEC 27000 series.

05

Decrypting the cybersecurity management requirements in NIS2

5. Decrypting the cybersecurity management requirements in NIS2

Legal requirements that are to be applied to cybersecurity management and this **additional helpful information** can be found not only in the specific catalog of measures in Article 21 of NIS2, but also in various other places in the EU legal act. Some of these references are not always immediately clear from the wording of the regulations, which makes it more complicated to implement the requirements in practice. These concern, among others, the following questions and requirements:

- **Coherence between physical security and cybersecurity** and, in particular, (official) coordination on cybersecurity issues and non-cyber-related risks.
- **Use of artificial intelligence** to detect and prevent cyberattacks, because AI is seen by the EU as an innovative technology that can help use existing resources more effectively to defend against cyberattacks and increase capacities,
- **Also taking into account data protection requirements** when implementing cybersecurity, because in order to implement NIS2 it may also be necessary to process personal data, whereby the data protection principles according to the GDPR, data protection through technology design and data protection-friendly default settings apply,
- **Not only can the use of open-source cybersecurity tools and applications** contribute to a higher level of openness, it can also have a positive impact on the efficiency of industrial innovation; open standards can also facilitate the interoperability of cybersecurity tools.
- **Focusing on SME-centric cybersecurity measures** makes it easier, especially for companies with limited economic and human resources, to improve cybersecurity, for example through increased cybersecurity awareness, as incidents in this area can also have an impact on the (digital) supply chain.
- **Active cyber protection measures** address the issue of which requirements are suitable for actively contributing to the prevention, detection, monitoring, analysis and mitigation of security breaches in a network. These can include, in particular, measures such as encryption, network mapping and segmentation, identification and access management.
- **Vulnerability detection** is a key aspect of cybersecurity because the exploitation of vulnerabilities can result in significant disruption and damage, which is why appropriate procedures should be determined to deal with discovered vulnerabilities and procedures should be put in place to receive vulnerability information, for example from third parties.
- **Defense against industrial espionage and protection of trade secrets** means that companies must especially address the risks arising from their interactions and relationships with external parties in a broader ecosystem that can extend beyond purely technical cybersecurity.
- **Cyber hygiene** includes fundamental practices such as zero trust principles, software updates, device configuration, network segmentation, identity and access management, user awareness and training, raising awareness of phishing and social engineering, for example,
- **enhanced cybersecurity governance at company management level** means that in the future the management bodies will also be more closely involved in NIS2 implementation and it will no longer be possible to freely delegate IT security measures, as their own expertise and management practices must be established,

- **Documentation requirements** serve to demonstrate cybersecurity to supervisory authorities and business partners, but can also be relevant in the course of improving your own cybersecurity process management,

- **Supply chain security** concerns relationships with suppliers, such as providers of data storage and processing services, providers of managed security services or software manufacturers. Therefore, it is important to assess and consider the overall quality and resilience of external products and services as part of risk management. This can also be done through contractual agreements.

- **Taking into account and avoiding "non-technical risk factors"** such as undue influence of a third country on suppliers and service providers (resulting in hidden vulnerabilities or backdoors and potential systemic supply disruptions, including with regard to dependence on certain technologies).

Practical tip: There is no "one-size-fits all" solution for the legally compliant implementation of NIS2

When looking at risk management measures in cybersecurity, it quickly becomes clear that the NIS2 Directive primarily contains process-related content, but very few concrete technology-related elements. This "ambiguity" may present companies with a certain degree of legal uncertainty with regard to implementation, but it is fully intended by the legislator. Furthermore, a similar approach can also be found in various other areas of EU technology regulation, such as the EU GDPR.

There are two main reasons for this: On the one hand, in reality the "state of the art" and thus the measures to be taken can change more quickly than can be reflected in law by the legislator. On the other hand, NIS2 not only covers a large number of different sectors and industries in its scope of application, but also company sizes, so that not all cases can be conclusively legally represented in the sense of a casuistry. Therefore, there are basically several and different ways to meet the requirements of NIS2 using cybersecurity measures, as every information security management must always be tailored to individual operational needs.

06

NIS2 implementation: A holistic approach to legal, technical and organizational requirements

6. NIS2 implementation: A holistic approach to legal, technical and organizational requirements

The variety of the above-mentioned implementation requirements for NIS2 makes it clear that for the effective and practice-oriented implementation of the new legal requirements, more than ever and even beyond NIS-1, a **holistic approach** is required, for which in the context of concrete application scenarios, the use of various tools is required and, in addition to the purely technical implementation, the **operational and organizational components** will need to be considered to a greater extent than before.

Practical tip: Why the implementation of NIS2 is important for the companies affected

NIS2 clearly establishes that the responsibility for ensuring cybersecurity lies significantly with the affected entities. This requires that institutions promote and develop a risk management culture. This risk management culture includes, among other things, risk assessment and the application of the previously outlined risk management measures in the area of cybersecurity. But it's not just this intrinsic motivation that plays a role in the implementation of NIS2. Companies should always be aware that cybersecurity incidents can not only cause reputational damage and thus economic damage, but can also result in legal consequences that may result in negative economic effects. Likewise, a breach of cybersecurity can also be linked to a data breach.

Failure to comply with cybersecurity can, for example, result in contractual or tortious claims for damages if the risk management measures were not implemented correctly, inadequately or, in the worst case, not at all, thereby disregarding the "due diligence required in business".

In addition, NIS2 provides for comprehensive official control powers, sanctions and fines. According to European law, supervisory and enforcement measures should be "effective, proportionate and dissuasive". On the other hand, the affected institutions have obligations to cooperate, for example to grant access to data, data processing systems or to provide evidence of the implementation of cybersecurity concepts. Resulting regulatory actions may include, but are not limited to, the following:

- Violation warnings
- Mandatory instructions for rectifying a security incident
- Cyber threat notifications to service recipients
- Instructions for public notification of violations
- Compulsory fines
- Imposition of fines

When taking enforcement action under NIS2, various aspects are taken into account in the assessment:

- Severity of the violation
- Importance of the provisions that were violated
- Repetition of violations
- Failure to rectify defects according to binding instructions
- Providing false or grossly misleading information regarding cybersecurity risk management
- Duration of the violation
- Material or immaterial damages caused
- Intent/negligence
- Cooperation and damage reduction measures

Fines can be imposed in addition to the other official measures under NIS2 and are determined on a case-by-case basis. A distinction is made based on the severity of the violation and the entity affected within two limits for determining fines:

- Fines with a maximum amount of at least EUR 10,000,000 or a maximum amount of at least 2% of the company's total worldwide turnover in the previous financial year, whichever is higher
- Fines with a maximum amount of at least EUR 7,000,000 or a maximum amount of at least 1.4% of the company's total worldwide turnover in the previous financial year, whichever is higher

More information about NIS2

NIS2 comes with many questions: Who does NIS2 apply to? What are the requirements of NIS2? What exactly do customers need to do to achieve NIS2 compliance? Find answers to the most important questions on Trend Micro's dedicated NIS2 webpages.

More at **trendmicro.com**