SOPHOS

The NIS 2 Directive

Requirements – Effects – Key data

This whitepaper was written in cooperation with attorney Dr. David Bomhard of Noerr Partnerschaftsgesellschaft mbB.

In response to the increased threat of cyberattacks and the associated need to increase defenses (including technical defenses) against such incidents, the Council of the European Union and the European Parliament adopted the Network and Information Security Directive 2.0 (Directive (EU) 2022/2555, "NIS 2 Directive") in December 2022. This Directive provides for revised and broader IT security requirements in all EU member states. One of the most important purposes of this IT security legislation in the EU is to contribute "to the effective functioning of its economy and society" (see Recital 1 of the NIS 2 Directive).

This whitepaper is to provide you with information about the new and broadened requirements that the NIS 2 Directive places on companies doing business in the European market, and how Sophos solutions can help you comply with these new requirements.

A Sophos Whitepaper, May 2023

A. Background and significant content of the NIS 2 Directive

I. Roadmap: from NIS 1 to NIS 2

The first Network and Information Security Directive (Directive (EU) 2016/1148, "NIS 1 Directive"), adopted in 2016, brought the first cyber security standardization efforts at the EU level into the legal systems of EU member states.

In December 2022, the Council and the European Parliament adopted the NIS 2 Directive, which revised and broadened cybersecurity requirements throughout the EU. Since the NIS 2 Directive is also a directive and not a regulation, it is not directly applicable in the member states, but first requires transformation into national law. National legislators are therefore required to amend their national IT security laws by the deadline set by European legislators, October 17, 2024.

Even if national legislators meet this deadline ahead of schedule, companies are not required to comply with the new provisions until October 18, 2024. Nevertheless, companies are strongly advised to examine the new requirements of the NIS 2 Directive and their possible impact as soon as possible.

> **Example:**
>
> *Because the NIS 2 Directive's scope of application is broader than that of the first directive and the national laws implementing it, some companies (or authorities) that were previously not subject to IT security law could now be subject to the NIS 2 Directive. It is imperative that such company or authority examine potential implementation measures and the effects they may have on business processes and administrative procedures as soon as possible.*

II. Cybersecurity as a management task

With the NIS 2 Directive, European legislators have made it clear that they view ensuring cybersecurity and preventing IT security incidents as the responsibility of the top management of every company. Pursuant to Article 20(1) of the NIS 2 Directive, the "management bodies" must monitor compliance with risk management measures (outlined under IV. below) and – even more importantly – can be held (personally) liable for violations in this area.

> **Example:**
>
> *The management of an automotive group is advised not to simply delegate all implementation of cybersecurity measures, but rather to take initiative to closely supervise and monitor compliance with the legal requirements, as the members of the management team themselves can ultimately be held liable for violations of these requirements at their entity.*

According to Article 32(6) of the NIS 2 Directive, these consequences can also be felt by public administration entities, without prejudice to any national provisions on the liability of public servants or other public officials. In this respect, it remains to be seen how the member states will implement and structure the management liability in detail.

III. Broadened scope of the NIS 2 Directive

1. More regulated sectors

The NIS 2 Directive significantly broadens the previous scope and now covers 18 sectors, both public and private.

> **Example:**
>
> *The NIS 2 Directive broadens the sectors covered to include, for example, aerospace and critical public administration services.*

As a European directive, the applicability of the NIS 2 Directive requires a certain connection to the EU. Therefore, the Directive applies to entities that provide their services or do business in the European Union. A company that merely acts as a supplier to a European company but does not itself provide services in the EU or do business in the EU is at most indirectly affected by the NIS 2 Directive via specific risk management measures (see IV.2. below).

The following 18 sectors are covered by the NIS 2 Directive:

SECTORS OF HIGH CRITICALITY (ANNEX I OF THE NIS 2 DIRECTIVE):	OTHER CRITICAL SECTORS (ANNEX II OF THE NIS 2 DIRECTIVE):
Energy	Postal and courier services
Transport	Waste management
Banking	Manufacture, production and distribution of chemicals
Financial market infrastructures	Production, processing and distribution of food
Health	Manufacturing
Drinking water	Digital providers
Waste water	Research
Digital infrastructure	
ICT service management (B2B)	
Public administration	
Space	

Due to the broader scope, it is no longer up to the member states to determine which sectors should be subject to cybersecurity regulation.

The following table illustrates the increase in sectors covered by the NIS 2 Directive as compared to the first NIS directive:

NIS 1 DIRECTIVE	NIS 2 DIRECTIVE
Energy	Energy
Drinking water supply and distribution	Drinking water, Wastewater
Digital infrastructure	Digital infrastructure
Health sector	Health
Banking, Financial market infrastructures	Banking, Financial market infrastructures
Transport	Transport, Space (partial), Postal and courier services
	Production, processing and distribution of food
	Waste management
	ICT service management (B2B)
	Public administration
	Manufacture, production and distribution of chemicals
	Manufacturing
	Digital providers
	Research

The NIS 2 Directive is generally applicable to any entity in the sectors listed in its Annexes I and II that, according to the terminology of European law, reaches the thresholds for medium-sized enterprises. This is generally the case if the entity has at least 50 employees or achieves an annual turnover or an annual balance sheet total of more than EUR 10 million.

Article 2(2)-(5) of the NIS 2 Directive explicitly adds certain entities to its scope regardless of their size. These include providers of public electronic communications networks or publicly available electronic communications services, as well as certain public administration bodies. For such entities, the number of employees as well as the annual turnover and the annual balance sheet total are not decisive factors

> **Example:**
>
> *In the health sector, the NIS 2 Directive will place many more entities under the regulatory scope of EU cybersecurity law. In contrast to the previous directive and its national implementing laws, all manufacturers of medical devices within the meaning of the European Medical Devices Regulation (EU) 2017/745 will be covered by the requirements of the NIS 2 Directive as opposed to only manufacturers of medicinal products that exceed certain thresholds which are further shaped by the member states.*
>
> *As a result, manufacturers of wearables such as fitness trackers, for example, will be required to comply with EU cybersecurity law.*

2. Essential and important entities

In principle, the scope of application of the NIS 2 Directive only extends to companies that have at least 50 employees or achieve an annual turnover or an annual balance sheet total of over EUR 10 million. In certain cases (e.g., providers of publicly available electronic communications services), the NIS 2 Directive also applies regardless of the entity's size.

The NIS 2 Directive links most of its requirements to the classification of an operator as an "essential" or "important" entity.

"Essential entities" are:

- Entities in the sectors listed in Annex I that exceed the thresholds of at least 250 employees or an annual turnover of over EUR 50 million and an annual balance sheet total of over EUR 43 million;
- Qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- Providers of public electronic communication networks or publicly available electronic communications services that exceed the thresholds of at least 50 employees or an annual turnover or an annual balance sheet total of over EUR 10 million;
- Public administration entities of the central government of a member state (as defined by that member state);
- Entities explicitly classified by a member state as "essential entities";
- Entities identified as critical entities under the CER Directive (EU) 2022/2557;
- If the member state so provides, entities which that member state identified as operators of essential services under the NIS 1 Directive or national law.

"Important entities" are:

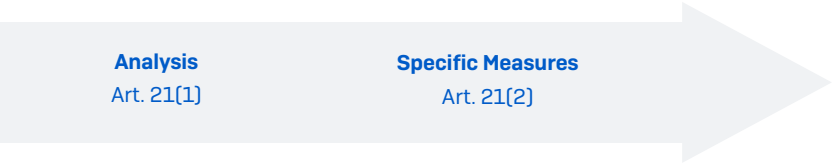
- Entities in the sectors listed in Annex I or II that do not qualify as essential entities;
- Entities explicitly identified by member states as "important entities".

ESSENTIAL ENTITY	IMPORTANT ENTITY
Sector listed in Annex I + at least 250 employees or annual turnover of over EUR 50M and annual balance sheet total of over EUR 43M	**Sectors listed in Annexes I & II +** at least 50 employees or annual turnover or annual balance sheet total of over EUR 10M (if not already qualifying as essential)
Exceptional cases, e.g. central government, DNS service providers or classification as essential by member state	Exceptional cases irrespective of size, e.g. through classification as important by member state

IV. Central obligation: risk management action

The NIS 2 Directive requires essential and important entities to take appropriate and proportionate technical, operational and organizational action to manage the risks posed to the security of the network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on the recipients of their services and on other services (Article 21(1) NIS 2 Directive).

Companies or authorities subject to the NIS 2 Directive should first determine the measures necessary for them and, in a second step, implement them.



Step 1: Analysis of required measures

The starting point for assessing which measures to take in a particular case is a systemic analysis of the circumstances of the individual case, taking into account the human factor and the degree of dependence on network and information systems. The proportionality of the measures to be taken is determined by the potential social and economic impact of any cyber incident. The more serious the effects could be, the greater the efforts the entity needs to make when implementing risk management measures. In the light of this, failing to take certain risk management measures for cost reasons would require considerable justification – particularly in the case of essential entities.

All in all, the requirements for risk management are based on an "all-hazards approach": not only "digital" but also physical hazards are to be included in the analysis.

> **Example:**
>
> *When analyzing necessary risk management measures, a tech company should not only include the risk of phishing or hacking scenarios, but also consider negative incidents such as theft, fire (e.g., in the data center) or power outages.*

Step 2: Specific risk management measures

Specifically, the NIS 2 Directive's requirements include the following measures as part of active risk management:

- **Policies:** policies on risk analysis and information systems security
- **Business continuity:** for example, backup management and disaster recovery and crisis management
- **Incident handling:** handling security incidents
- **Purchasing:** security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- **Training:** basic cyber hygiene practices and cybersecurity training
- **Encryption:** policies and procedures regarding the use of cryptography and, where appropriate, encryption
- **Supply chain:** supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- **Effectiveness:** policies and procedures to assess the effectiveness of cybersecurity risk management measures
- **Other organizational measures:** human resources security, access control policies and asset management
- **Other technical measures:** multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

As a result of the obligation to also ensure security in the supply chain, even companies that are not themselves subject to the scope of the NIS 2 Directive may be indirectly affected by it. Even non-European companies can be affected by the cybersecurity action requirements that are passed along throughout the supply chain by a directly obligated entity.

> **Example**:
>
> *According to Article 21(2) NIS 2 Directive, a car manufacturer is also obligated to ensure cybersecurity in its supply chain. Thus, to fulfill its own obligation to take risk management measures under the NIS 2 Directive, it may approach its suppliers and – for example contractually – require certain cybersecurity measures on the part of the suppliers.*

V. Standardization and certification

The NIS 2 Directive allows member states to require essential and important entities to use EU cybersecurity certifications and/or certified products. For this reason, certified technical solutions will be worth considering for operators to demonstrate compliance with the NIS 2 Directive requirements in a time- and cost-efficient manner. The certification of such products is based on European schemes for cybersecurity certification under the EU Cybersecurity Act (Regulation (EU) 2019/881).

The NIS 2 Directive also gives the European Commission the power to implement delegated acts to require certain categories of essential and important entities to use certain certified technical solutions or to obtain a corresponding certificate. However, such delegated acts can only be adopted if the Commission has previously identified insufficient levels of cybersecurity and has set a deadline for implementation.

It can be assumed that in the future, at least the member states will establish corresponding obligations. Companies should therefore closely follow the transformation of this authorization into national law so that they can procure the required certifications or certified products in good time.

The member states are also required by the NIS 2 Directive to promote the use of European and international standards and technical specifications for the security of network and information systems (e.g., ISO/IEC 27001). Such standards will therefore become even more important under the NIS 2 Directive.

VI. Sanctions for violations

The NIS 2 Directive places the EU member states under an obligation to create provisions regarding fines for violations of Article 21 (risk management measures, see above) and Article 23 (reporting obligations for significant security incidents) of the NIS 2 Directive. The NIS 2 Directive also sets minimum values for the upper limit of the range of fines:

ESSENTIAL ENTITIES	IMPORTANT ENTITIES
Administrative fines of up to **EUR 10 million** or **2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.**	Administrative fines of up to **EUR 7 million** or **1.4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.**

Any fine comes in addition to other supervisory and enforcement measures that a competent authority may impose in the event of a (potential) violation.

> **Example:**
>
> *According to Article 32(5) NIS 2 Directive, when implementing the Directive, the member states are to endow the competent authorities with power that can be understood as a "last resort". In the event of non-compliance with supervisory measures, the authority responsible for enforcing the NIS 2 Directive may request other competent authorities or courts to temporarily prohibit the members of management from performing management tasks in the entity. In so doing, the European legislators are emphasizing the principle that cybersecurity is a "management task" (see above).*
>
> *The situation is similar in the public sector: although certain enforcement measures set forth by the NIS 2 Directive are explicitly not applicable to bodies of public administration (e.g., authorities), the member state's liability rules for public servants and public officials (public liability) apply.*

The management levels of significant and important entities are therefore well advised to carefully analyze at an early stage their obligation to take risk management action in order to avoid significant fines for violations.

It remains to be seen whether public administration bodies that are now covered by the NIS 2 Directive will also be subject to fines. According to Article 34(7) NIS 2 Directive, it is up to the member states individually to decide whether and to what extent administrative fines may be imposed on public administration entities.

B. Sophos products for operators of essential and important entities

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
Chapter IV, Article 20, Governance		
2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	**Sophos Training and Certifications**	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
Chapter IV, Article 21, Cybersecurity risk-management measures		
2. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems…based on a) policies on risk analysis and information system security;	**Sophos Intercept X** **Sophos Intercept X for Server**	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/ Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	24/7 threat detection and response identifies and neutralizes advanced cyber-attacks that technology alone cannot stop.
2. b) incident handling;	**Sophos Managed Detection and Response (MDR)**	Continuously monitors signals from across the security environment, including network, email, firewall, identity, endpoint, and cloud technologies, enabling us to quickly and accurately detect and respond to potential cybersecurity events. Full incident response service is included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting. Our average time to detect, investigate and respond is just 38 minutes.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	**Sophos Managed Detection and Response (MDR)**	Ensures the information security aspect of business continuity management with 24/7 detection of and response to security incidents across the IT environment, leveraging human expertise, AI, and advanced technologies.
	Sophos Intercept X **Sophos Intercept X for Server**	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	**Sophos Intercept X with XDR**	Provides comprehensive defense in depth against threats that get in via third-party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	**Sophos Managed Detection and Response (MDR)**	Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect personal data wherever it resides. Sophos NDR generates high-caliber actionable signals across the network infrastructure to optimize cyber defenses. Sophos MDR proactively responds to vulnerability disclosure by the client. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation.
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	**Sophos Managed Detection and Response (MDR)**	Investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk levels and prioritize response.
2. g) basic cyber hygiene practices and cybersecurity training;	**Sophos Training and Certifications**	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
2. h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	**Sophos Central Device Encryption**	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Email **Sophos Firewall**	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
	Sophos Mobile	Enforces device encryption and monitors compliance relative to encryption policy.

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	W IT HELPS
2. i) human resources security, access control policies and asset management;	**Sophos Managed Detection and Response (MDR)**	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities by regularly reviewing records of information system activity, such as audit logs, access logs, access reports, and security incident tracking reports.
	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources.
	Sophos Central	Keeps access lists and user privileges information up to date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos ZTNA	Enables better security and more agility in quickly changing environments by making it quick and easy to enroll or decommission users and devices. Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
2. 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	**Sophos Firewall**	Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
Chapter IV, Article 23, Reporting obligations		
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: ***(i) a detailed description of the incident, including its severity and impact;***	**Sophos Managed Detection and Response (MDR)**	On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation.
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: ***(ii) the type of threat or root cause that is likely to have triggered the incident;***	**Sophos Managed Detection and Response (MDR)**	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops. Full root cause analysis by Sophos MDR enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake, you can quickly answer business critical questions, correlate events from different data sources and take even more informed action. For eg., you can cross-reference against network information to get a broader view of an incident or what happened to devices that were knocked offline in an attack.

2023-05-23 EN-WP (NP)

SOPHOS