asvin

NIS 2 IN A NUTSHELL

A brief Q & A overview of the EU NIS2 the European Framework for Cyber Security at Critical Infrastructure Operators.

Swipe

asvin.io

asvin

What's the EU NIS 2?

NIS 2 is an EU directive that improves cybersecurity by establishing minimum security requirements for digital service providers and critical infrastructure operators and by creating a network for information exchange.

Its goal is to define cybersecurity in a single European framework and increase resilience in affected enterprises.

asvin.io

asvin

Who is responsible for NIS 2 in the company?

NIS 2 requires company management to ensure compliance through establishing policies and procedures, allocating resources, and regularly reviewing measures. Non-compliance can result in significant consequences.

asvin.io

asvin

What are the deadlines for the NIS 2 regulation?

The Directive was published on December 27, 2022, so it will officially go into effect on January 16, 2023. EUMember states have 21 months from that date to transpose the directive into national law.
At asvin we assume that the implementation in a company, depending on the size and current state of cyber security takes up to 18 months. Therefore, we recommend to start with the implementation in the next 3 months via appropriate partners.

asvin.io

To whom does the NIS 2 regulation apply?

NIS 2 applies to companies with at least 50 employees and over 10 million euros in revenue. The companies are defined in 16 sectors, instead of 8 so far. These sectors are divided into „SECTORS OF HIGH CRITICALITY“ and „OTHER CRITICAL SECTORS“, with stricter checks and closer attention paid to the former. A list of all sectors and their entities can be found on the next 2 slides

asvin

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity*
1. Energy	(a) Electricity	Electricity undertakings which carry out the function of supply | Distribution system operators Transmission system operators | Producers | Nominated electricity market operators Market participants providing aggregation, demand response or energy storage services Operators of a recharging point (that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider)
	(b) District heating and cooling	Operators of district heating or district cooling
	(c) Oil	Operators of oil transmission pipelines | Operators of oil production, refining and treatment facilities, storage and transmission | Central stockholding entities
	(d) Gas	Supply undertakings | Distribution system operators | Transmission system operators Storage system operators | LNG system operators | Natural gas undertakings Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	Air carriers | Airport managing bodies | airport Traffic management control operators providing air traffic control (ATC) Entities operating ancillary installations contained within airports|
	(b) Rail	Infrastructure managers | Railway undertakings, including operators of service facilities
	(c) Water	Inland, sea and coastal passenger and freight water transport companies Managing bodies of ports | entities operating works and equipment contained within ports Operators of vessel traffic services (VTS)
	(d) Road	Road authorities responsible for traffic management control Operators of Intelligent Transport Systems
3. Banking		Credit institutions | Operators of trading venue
4. Financial market infrastructures		Operators of trading venues | Central counterparties (CCPs)
5. Health		Healthcare providers | EU reference laboratories | Entities carrying out research and development activities of medicinal products | Entities manufacturing basic pharmaceutical products and pharmaceutical preparations | Entities manufacturing medical devices considered to be critical during a public health emergency
6. Drinking water		Suppliers and distributors of water intended for human consumption
7. Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water
8. Digital infrastructure		Internet Exchange Point providers | TLD name registries | Cloud computing service providers Data centre service providers | Content delivery network providers | Trust service providers | Providers of public electronic communications networks | Providers of publicly available electronic communications services | DNS service providers, excluding operators of root name servers
9.ICT service management (b2b)		Managed service providers | Managed security service providers
10. Public administration		Public administration entities of central governments | Public administration entities at regional level
11. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

asvin.io

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity*
1. Postal and courier services		Postal service
2. Waste management		Undertakings carrying out waste management
3. Manufacture, production and distribution of chemicals	,	Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures
4. Production, processing and distribution of food		Food businesses which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices Entities manufacturing in vitro diagnostic medical devices
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	
	(e) Manufacture of motor vehicles, trailers and semi-trailers	
	(f) Manufacture of other transport equipment	
6. Digital providers		Providers of online marketplaces
		Providers of online search engines
		Providers of social networking services platforms
7. Research		Research organisations

*Note: This is only an shortened compilation of the types of entity.
For a complete list of entities defined by the EU and their exceptions, please use the official document of the European Parliament at EUR-Lex.

asvin

What are the to dos for companies in relation to NIS 2?

• Secure the Supply Chain

- Focus on securing and documenting the software supply chain
- Assess and consider the cybersecurity practices of suppliers and service providers, including their secure development processes
- Ensure overall quality and resilience of products and services through risk management measures

• Cybersecurity is the Responsibility of Corporate Management

- Implement risk assessment and management measures
- Be accountable for compliance and review

• Stricter Reporting Requirements for Security Incidents

- Report not only actual incidents, but also potential incidents
- If an essential or important facility becomes aware of a significant security incident, they must send an early warning within 24 hours

• Obligation to Notify ENISA

- Operators and manufacturers of essential or important services must submit notifications to ENISA

• Promote Cyber Hygiene and Employee Sensitization

- Adopt a range of basic cyber hygiene practices, such as zero trust principles, software updates, device configuration, network segmentation, identity and access management, or user awareness
- Organize training for employees and raise awareness of cyber threats, phishing, and social engineering techniques

Note: This is only an shortened compilation based on the DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022. It does not claim to be complete, nor does it constitute legally binding advice.
For a complete Information, please use the official document of the European Parliament at EUR-Lex.

asvin.io

asvin

ARE YOU STRUGGLING CRACKING THE HARDEST CYBERSECURITY NUTS??

Let‘s talk about it! Just write to us and let‘s see how we can help.

Don‘t forget, you can easily save and share the info PDF with your colleagues and network. Don‘t miss out on this valuable resource.
Take action now and let‘s work together to strengthen our cybersecurity defenses.

And don‘t forget to share your thoughts and questions about the upcoming NIS 2 regulation in the comments.

asvin.io