Network and Information Security (NIS2)

What the new EU directive means for corporate cybersecurity

Introduction

The NIS2 (Network and Information Security) Directive is a directive to improve the collective cybersecurity level of all EU Member States. It came into force in January 2023 and obliges all relevant organisations and companies to comply with the new requirements by 18 October 2024.

The NIS2 Directive replaces the 2016 NIS Directive, which was the first EU-wide cybersecurity directive. It strengthens security requirements, addresses supply chain security, harmonises reporting requirements and introduces stricter oversight measures and tougher enforcement requirements, including harmonised sanctions across the EU.

NIS2 involves more industrial sectors

NIS2 also expands the scope of application and now requires more entities and sectors to act. These include providers of essential and important services, digital service providers, public administrations, manufacturers of consumer IoT devices and cybersecurity service providers.

Companies required to comply with the NIS2 requirements:

Sectors of High Criticality	
Energy	Electricity, oil, gas, hydrogen, heating, and cooling
Transport	Road, rail, air, and water
Banking	Banks, stock markets, financial institutions
Healthcare	Hospitals, labs, research centers, pharmacies, and medical devices
Water	Wastewater and drinking water
Digital infrastructure	Telco, Data centers, cloud computing, DNS providers, etc.
ICT services	Managed services and managed security services
Public administration	Central and regional goverment entities
Space	Operators of ground infrastructure

Other Critical Sectors	
Post and couriers	Mail and package shipping
Waste management	Waste collection, processing, and recycling
Chemicals	Production and distribution of chemicals
Food	Production, processing, and distribution of foods
Manufacturing	Manufacturers of medical devices, machinery, vehicles, and electric/electronic devices
Digital services	Search engines, online marketplaces, and social networks
Research	Research organisations

Source: Official website of the European Union, https://eur-lex.europa.eu/eli/dir/2022/2555/oj

NIS2 and the new requirements for cybersecurity

As mandated by NIS2, affected companies must comply with several new obligations:

- Risk Management

  Organisations need monitoring measures to minimise cyber risks. These include incident reporting and management, supply chain resilience, enhanced network security, access control, and encryption.

- Management Responsibility

  Management must monitor and approve cybersecurity measures and train the workforce to deal with cyber risks. Violations will result in fines for management, including liability and possible temporary disqualification from management duties.

- Reporting Requirements

  Critical entities must have procedures in place to quickly report security incidents that could significantly impact their operations. NIS2 sets specific reporting deadlines: an initial report must be submitted within 24 hours, followed by a full report within 72 hours. Finally, a report containing a detailed description of the incident must be submitted within one month of the initial notification of the incident.

- Business Continuity
  Organisations must be positioned to ensure business continuity in the event of major cyber incidents. In addition, clear procedures must be defined for system recovery, emergency procedures, and the establishment of a crisis response team.

The most important elements of the NIS2 Directive and their meaning

The NIS2 Directive is intended to help raise the level of cybersecurity in Europe in the long term and create a single market for cybersecurity. It also aims to increase the confidence of citizens and businesses in digital services and increase resilience to cyber threats.

Incident reporting and management in NIS2 is of immense importance because it should significantly improve the security and reliability of the network and information systems in the European Union.

Incident reporting allows competent authorities to assess risks, take appropriate countermeasures, and minimise the impact on users and public order.

Incident management enables providers of essential and digital services to protect, monitor, and continuously improve their systems to reduce or even prevent future incidents.

Supply chain resilience is essential for the security and reliability of critical infrastructure in the EU.

The Directive requires operators of critical services to take appropriate technical and organisational measures to reduce the risks of cyber-attacks on their software supply chain and increase the resilience of their systems.

A disrupted or compromised supply chain can lead to serious consequences for public safety, public health, the economy, and the environment.

It is therefore important that operators of essential and critical services ensure the resilience of their supply chain by verifying the origin, integrity and trustworthiness of their suppliers, including security requirements in their contracts, and conducting regular audits.

Access control is an essential part of the NIS2 Directive. This is intended to significantly improve the security of network and information systems in the EU.

It means that only authorised persons or devices can access the data or resources they need, and that unauthorised access is prevented or detected. This protects the confidentiality, integrity, and availability of systems and the information they contain.

Access control is therefore essential to reduce the risk of cyber-attacks and data loss or theft, and to increase the trust of users.

The Directive aims to increase resilience and trust in the digital infrastructure within the EU by imposing requirements on providers of essential and important services, as well as on digital service providers. Data encryption is one of the measures that needs to be taken to protect systems from cyber-attacks and to maintain the confidentiality of customer data.

NIS2 use cases

- Threat Intelligence and Incident Response
  The implementation of a real-time threat intelligence platform that continuously monitors potential threats and anomalies helps organisations to quickly detect and respond to incidents. In this context, clearly defined response plans and tools are required to effectively mitigate the impact of cyber attacks.
- Data Security Anywhere

  With the use of hybrid infrastructures, i.e. on-premises combined with cloud solutions, data security is becoming increasingly important. Recommended measures include implementing a highly-automated data governance solution as well as end-to-end encryption of sensitive data to prevent data loss and avoid potentially high fines.
- Supply Chain Cyber Resilience

  Companies are required to ensure adequate cyber resilience within their entire software supply chain. This means that they must also assess the cyber risks of the individual software components within the supply chain and take appropriate measures.
- IoT & Operational Technology (OT) Security

  In the context of IoT and OT devices, cyber resilience involves securing access to devices, networks, and data to prevent unauthorised access.

  Implementing strong authentication mechanisms and monitoring unusual device behaviour should be part of a resilience strategy to comply with the NIS2 Directive.

Our approach

- Threat Intelligence and Incident Response

  AI-driven behavioural analysis (no training required), real-time intelligent correlation, security monitoring, threat detection and incident response, and out-of-the-box detections: All these features help you comply with NIS2 policies through continuous monitoring of critical services and intelligent and rapid response to potential threats.

  Find out more:

  https://www.microfocus.com/en-us/cyberres/secops

  https://cloudsecurity.cyberres.com/threat-intelligence/
- Data Security Anywhere

  OpenText's enterprise security solutions provide a unique data governance platform helping organisations to discover, visualise, classify, and protect sensitive data. Unique and customisable workflow automation is standard and also available for hybrid environments.

  Companies subject to NIS2 compliance are thus in control of their data at all times and can avoid non-compliance and the risk of huge fines.

  Find out more:

  https://www.microfocus.com/en-us/cyberres/data-privacy-protection
- Supply Chain Cyber Resilience

  With centralised identity & access management, governance and advanced access rights management, and intelligent monitoring capabilities, we help organisations grant the right permissions to the right stakeholders for the right assets, reducing the risks of compromising critical infrastructure and data.

  Internally-developed applications can be tested for security vulnerabilities by offering static, dynamic and mobile application security testing besides verifying trivial open-source components. This helps ensuring reliable end-to-end supply chain code resilience.

  Find out more:

  https://www.microfocus.com/en-us/cyberres/identity-access-management

  https://www.microfocus.com/en-us/cyberres/use-cases/securing-the-software-supply-chain
- IoT & Operational Technology (OT) Security

  NetIQ Advanced Authentication supports a variety of strong authentication methods, such as multi-factor authentication (MFA) and biometric authentication. These robust authentication mechanisms provide an additional layer of security and protect sensitive infrastructure from unauthorised access and identity theft.

  Find out more:

  https://www.microfocus.com/en-us/cyberres/identity-access-management/advanced-authentication

  Of course, we also offer support for many other NIS2 use cases relevant to your organisation or industry. You can learn more here about our cyber security portfolio or contact our specialists for more detailed information.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. WP_092523