CYBERARK®
The Identity Security Company

pwc

WHITEPAPER

Getting Ready for the NIS2 Directive

Why Identity Security is Key to Preparing for Compliance Updates

Table of Contents

Introduction

In January 2023, EU member states formally enacted a revision of the 2016 Network and Information Systems (NIS) Directive. Conceived in response to several widely publicised and damaging cyberattacks, the NIS2 Directive strengthens security requirements, streamlines reporting obligations and introduces more stringent supervisory measures and stricter enforcement requirements. The revised directive is intended to better defend critical entities against supply chain vulnerabilities, ransomware attacks and other cyber threats. **All 27 EU member states must incorporate the NIS2 Directive into their national laws by October 2024.**

This paper provides a brief introduction to NIS2 and explains how it might affect your business and how you can prepare.

How Will NIS2 Impact Your Organisation?

NIS2 significantly expands the breadth and depth of the original NIS Directive. It covers a wider range of industry sectors, introduces more comprehensive security controls, imposes more rigorous incident reporting requirements and increases enforcement measures and sanctions.

- **Previously exempt organisations** may be required to introduce new cybersecurity systems and practices to comply with NIS2.
- **Organisations bound by the original directive** may be required to revamp their security systems and practices to comply with NIS2.

What's New In NIS2?

NIS2 covers more industry sectors

Communications service providers, digital providers, food producers and distributors, manufacturers of certain critical products and other businesses deemed fundamental to society are now considered critical entities (see Table 1). Any entity that falls into a designated sector must comply with the revised directive.

NIS2 defines two distinct types of critical entities: essential and important. The obligations are the same for both, but essential entities are subject to more stringent enforcement measures and sanctions.

NIS2 applies to any entity providing critical services within an EU member country, **regardless of where that entity is located**. In other words, any company based outside of the EU could be subject to NIS2 even if they do not have a physical presence in the EU.

Unlike the original directive, NIS2 cybersecurity requirements apply to not only organisations operating within its expanded definition of 'critical' and their direct employees, but also to the subcontractors and service providers supporting them.

Table 1: NIS2 Industry Sectors

Original NIS Sectors	Additional NIS2 Sectors
• Healthcare • Digital infrastructure • Transport • Water supply • Digital service providers • Banking • Financial market infrastructure • Energy Blue = Essential Entities Orange = Important Entities	• Providers of public electronic communications networks or services • Wastewater • Chemicals • Health (pharmaceuticals, R&D, critical medical devices) • Food producers, processors and distributors • Manufacturing of critical products (medical devices, computers, electronics, motor vehicles) • Digital providers (social networking platforms, search engines, online marketplaces) • Space • Postal and courier services • Public administration

NIS2 introduces more stringent cybersecurity and risk management requirements

NIS2 Article 21 directs member states to ensure that essential and important entities manage risk by implementing robust systems, policies and best practices covering a wide range of cybersecurity measures and disciplines including:

- Risk analysis and information system security
- Incident handling and reporting
- Business continuity, such as backup management and disaster recovery
- Crisis management
- Supply chain security
- Systems acquisition, development and maintenance security
- Basic cyber hygiene practices (see definition below) and cybersecurity training
- Cryptography and encryption technologies
- Human resources security, access control policies and asset management
- Zero Trust access (multifactor authentication, continuous authentication)

'CYBER HYGIENE' ACCORDING TO NIS2 ARTICLE 21

Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices — including software and hardware updates, **password changes, the management of new installs, the limitation of administrator-level access accounts** and the backing-up of data — enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats.

Unlike the original directive, NIS2 cybersecurity requirements apply to not only organisations operating within its expanded definition of 'critical' and their direct employees, **but also to the subcontractors and service providers supporting them**.

MAPPING NIS2 ARTICLE 21 TO ISO27001

You can use standard information security frameworks like ISO27001 or NIST to prepare for NIS2, identify technology and process gaps and scope out compliance efforts. The table below maps the NIS2 Article 21 security areas to corresponding ISO27001 security domains. Ultimately ENISA will recommend additional security standards and frameworks to address specific technical areas such as IEC 62443 for OT and IoT security.

NIS2 Article 21 Security Area	Corresponding ISO27001 Annex
Incident handling and reporting	A.16: Information security incident management
Business continuity	A.17: Information security aspects of business continuity
Supply chain security	A.15: Supplier relationships
Systems acquisition, development and maintenance security	A.14: System acquisition, development and maintenance
Cryptography and encryption technologies	A.10: Cryptography
Human resources security	A.7 Human resource security
Access control polices	A.9: Access control A.5: Information security policies
Asset management	A.8: Asset management
Zero Trust security	A.9: Access control

NIS2 introduces stricter incident-reporting obligations

Critical entities must now:

- Provide initial notification of a significant security incident within 24 hours of detection.
- Deliver an initial assessment of the incident within 72 hours of detection.
- File a detailed final report within a month of detection.

NIS2 imposes costly sanctions

Member states can levy fines of up to EUR 10 million or 2% of annual turnover (revenue) for certain violations or breaches. In addition, critical entity management bodies (i.e., executive teams) can be held personally liable for infringements.

Identity Security And NIS2

Identity Security is a comprehensive approach to protecting an organisation's people, applications and machines. It assumes any user—human or non-human—can become privileged under certain circumstances and penetrate systems, traverse networks and carry out attacks.

Identity Security mitigates risk by:

- Continuously authenticating and authorising internal and external users in accordance with Zero Trust principles.
- Tightly controlling access to on-premises and cloud-based resources.
- Closely monitoring and auditing user activity and providing proof of compliance.

A comprehensive Identity Security strategy is fundamental for defending critical infrastructure against malicious attacks, ransomware, software supply chain vulnerabilities and other threats. An Identity Security program can help organisations address key NIS2 Article 21 requirements related to incident handling and reporting, supply chain security, cryptography and encryption technologies, access control policies and Zero Trust security.

A complete Identity Security strategy includes:

- **Policy-based management of administrative credentials** to safeguard privileged accounts and help satisfy audit and compliance requirements.
- **Privileged session isolation** to prevent malware spread and mitigate risk.
- **Just-in-time access** to limit risks posed by credential theft.
- **Endpoint privilege security** to enforce the principle of least privilege and defend against ransomware and malicious attacks.
- **Centralised secrets management** to secure application pipelines and defend against software supply chain vulnerabilities.
- **Identity and access management** to prevent unauthorized access and enforce role-based access controls.
- **Multifactor authentication (MFA)** to secure remote workers, vendors and contractors and support Zero Trust principles.

A comprehensive Identity Security program can help organisations strengthen security, increase visibility and improve NIS2 readiness. Table 2 summarises the role Identity Security will play in addressing certain NIS2 requirements once they are enacted by member states.

Table 2: The role of Identity Security in NIS2

NIS2 Requirement	How Identity Security Helps
Paragraph 49: Cyber hygiene policies for infrastructure	
Establish good cyber hygiene practices, including password management and admin account management and restrictions.	• Privileged access management secures and controls admin accounts and credentials. • Identity and access management secures and controls user passwords and access. • Endpoint security removes local admin rights and prevents privilege escalation.

NIS2 Requirement	How Identity Security Helps
Paragraph 53: Utility sector security	
Protect increasingly connected digitalised utilities (transport, water supply, energy, etc.) and smart cities against cyberattacks.	• Privileged access management mitigates attacks by isolating sessions, managing credentials and enabling just-in-time access. • Identity Security intelligence automatically detects anomalous behaviour symptomatic of an attack. • Endpoint privilege security defends against cyberattacks by removing standing admin privileges from servers and workstations and by controlling application behaviour. • Identity and access management secures and controls user passwords, mitigating credential phishing and theft.
Paragraph 54: Ransomware protection	
Defend critical infrastructure against ransomware attacks.	• Endpoint privilege security defends against ransomware by removing standing admin privileges from endpoints and controlling application behaviour based on policy. • Privileged access management mitigates risks by isolating, monitoring, recording and auditing privileged sessions and preventing privilege escalation.
Paragraph 85: Supply chain security	
Address supply chain security vulnerabilities.	• Secrets management reduces software supply chain risks by monitoring and controlling secrets. • Secrets management protects passwords, keys and certificates used by applications, scripts and other non-human identities across DevOps environments and CI/CD pipelines. • Secure, just-in-time, remote access and session recording for outside vendors enforces principle of least privilege and simplifies forensics and audits.
Paragraph 89: Cyber hygiene practices for users	
Establish good cyber hygiene practices, including Zero Trust principles and identity and access management; pursue advanced technologies like artificial intelligence (AI) and machine learning (ML) to enhance security.	• MFA positively identifies users in accordance with Zero Trust principles. • Just-in-time access restricts access to specified time windows, further supporting Zero Trust principles. • Adaptive MFA uses AI-powered behavioral analytics and contextual information to determine which authentication factors to apply to a user in a specific situation.

NIS2 Requirement	How Identity Security Helps
Paragraph 98: Public electronic communications network security	
Use end-to-end encryption as well as data-centric security concepts, such as cartography, segmentation, tagging, access policy and access management and automated access decisions.	• Privileged access management uses encryption technologies to secure credentials and secrets used by people, applications and machines. • Privileged session isolation helps reduce the spread of malware between systems. • Identity and access management secures and controls access based on policy. • Endpoint privilege security provides just-in-time privilege elevation, automating access decisions.
Paragraph 102: Mandatory incident reporting	
Critical entities should be required to submit an early notification of an incident within 24 hours.	• Audit trails and privileged session recordings provide documentation of cyber incidents. • Identity Security intelligence automatically identifies and reports anomalous behavior symptomatic of a breach. • Identity and access management uses AI and ML to automatically identify suspicious user activity. • Endpoint privilege security automatically identifies activity symptomatic of an endpoint-originated attack.

Preparing For NIS2

Member states have until October 2024 to incorporate the NIS2 Directive into their national laws. There are **concrete steps you can take today** to prepare for NIS2 as member states flesh out their regulations.

1. **Identify, assess and address your risks.** Management bodies of essential and important entities must take appropriate and proportionate technical, operational and organisational measures, using an all-hazards approach to manage the risks posed to the security of network and information systems and the physical environment.
2. **Evaluate your security posture.** A security assessment can help identify areas of weakness such as unmanaged passwords or misconfigured or dormant accounts that are susceptible to credential theft.
3. **Take steps to safeguard privileged access.** Adversaries can exploit privileged accounts to orchestrate attacks, take down critical infrastructure and disrupt essential services. NIS2 advises critical entities to limit access to administrator-level accounts and to regularly rotate administrative passwords.
4. **Strengthen your ransomware defenses.** Costly and debilitating ransomware attacks are a major concern for EU regulators and one of the primary drivers of the NIS2 Directive. Introduce security solutions and best practices to proactively defend against ransomware. Use endpoint privilege security solutions to enforce the principle of least privilege, control applications and augment next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions.
5. **Move to a Zero Trust architecture.** Traditional perimeter-based security architectures, conceived to defend trusted enterprise network borders, aren't suited for the world of cloud services and hybrid workforces. Adopt a Zero Trust approach, implementing several layers of defense such as least privilege access, continuous authentication and threat analytics to validate all access attempts.

6. **Scrutinise your software supply chain.** Supply chain attacks are a major concern for EU regulators and a prime motivator for the NIS2 Directive. Take a fresh look at your software supply chain and consider implementing a secrets management solution to mitigate risk.
7. **Formalise your incident response plan.** NIS2 calls for faster incident reporting, with the first report due within 24 hours of an incident. Make sure your organisation is prepared. Review your event notification, information gathering and reporting processes.
8. **Educate your people.** Cybersecurity and cyber hygiene training are fundamental to NIS2. Step up your efforts to improve cyber awareness and foster a security-first culture.

Next Steps

Together, PwC and CyberArk can help your organization prepare for the NIS2 Directive and strengthen your identity security posture. PwC has an extensive business relationship with CyberArk and has deep experience architecting and implementing CyberArk solutions.

PwC and CyberArk can help your organisation identify and assess risks, formulate NIS2 plans, and defend your business against ransomware, software supply chain attacks, and other threats.

Learn More

- Get a complimentary risk assessment. CyberArk experts will help you evaluate your privileged access management systems and practices and assess your threat profile as you prepare for NIS2.
- Download CyberArk's Blueprint for Identity Security Success to map out your Identity Security strategy and improve NIS2 readiness.
- Discover how CyberArk's Identity Security Platform can help defend critical infrastructure against malicious attacks, ransomware, software supply chain vulnerabilities and other threats.
- Contact CyberArk or your local PwC office for more information on how we can assist you to get ready for NIS2.

About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 327,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

CYBERARK®
The Identity Security Company

pwc

©Copyright 2023 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 02.23 Doc. TSK-3106

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.