OSIRIUM

NIS2: your handy cheat sheet

Getting ready for NIS2

What is NIS?

A set of requirements/regulations established in the EU and UK in 2016 to bolster cyber security.

How does NIS2 differ?

It's an update designed to improve the security and resilience of critical infrastructures, such as energy, transport, banking, healthcare, water supply, and digital infrastructure, across the EU. The UK is expected to follow suit as it updates NIS.

NIS2 aims to promote a more coordinated and harmonised approach to cybersecurity and boost resilience of critical infrastructures to cyber threats.

Who does it apply to?

It now covers many sectors, expanding the scope of the original. New sectors include space, waste management, and research and development. It's split into 'critical' and 'important' entities.

Who are the 'critical entities'?

Organisations within the following sectors are regarded as such:

- Energy (electricity, oil, gas, hydrogen)
- Transport (air, rail water, road)
- Banking/ Financial market infrastructures
- Health (including pharmaceutical)
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (managed service providers)
- Public administration
- Space

Important entities

- Postal and courier services
- Waste management
- Manufacturing, production and distribution of chemicals
- Food production, processing and distribution
- Digital providers (online marketplaces, search engines)

What are the key new obligations?

Critical infrastructure operators must now:

- perform regular security assessments
- adopt incident response plans
- appoint a chief information security officer (CISO)
- report significant incidents to the national authorities

What are the penalties for non-compliance?

Maximum fines are increasing. They will now either be:

- up to 10 million euros

OR

- 2% of the company's global turnover

Whichever is higher.

What form will enforcement take?

Organisations will be subject to:

- random checks by trained professionals
- regular security audits by independent body
- on-site inspections and off-site supervisions

Where does Privileged Access fit in?

NIS2 directive points to a number of areas where it is important:

- ransomware attacks
- cyber hygiene
- limiting administrator-level access accounts
- data back-ups
- zero trust principle

How does managing privileged accounts help with compliance?

Reducing ransomware risks: staff workstations are often the key point of attack for cyber criminals. Endpoint management can prevent the user from installing applications and therefore reduce that threat.

Administrator privileges: if they are never available or revealed to the admins, they can't be stolen by malware/ransomware. Making all access to critical IT systems via PAM achieves that.

Spotting possible threats: PAM makes it easy to spot suspicious activity on the network.

Improving cyber hygiene: PAM achieves limitation of administrator-level access accounts and secures, controls and manages admin credentials and passwords.

Protecting back-ups: PAM can help prevent the loss of back-ups in the event of a ransomware attack.

Greater protection of utilities: transport, water, energy etc – are increasingly vulnerable to cyberattacks as they become more digitally connected. PAM reduces the risks of attacks by isolating sessions, managing credentials and enabling just-in-time access.

Zero-trust principle: PAM helps by separating the authentication from the authorisation. PAM authenticates against a variety of sources.

Third party dangers: MSPs often get full VPN access to corporate systems, creating security risks in terms of credential sharing and unnecessary privileged access. But PAM tackles this problem with features such as secure MFA, audit and session recording.

Talk to us to see how Osirium can help meet your compliance needs

Call
+ 44 (0) 118 324 2444

Chat
www.osirium.com

Email
info@osirium.com

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of cyber security and automation technology to create the world's first, built-for-purpose, Privileged Account management and process automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down business risks, operational costs and meet IT compliance needs.

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, www.osirium.com