

Preparing for NIS2

More than a compliance exercise:
an opportunity to future proof your organization

» What is NIS2?

The Network and Information Systems 2 Directive – commonly referred to as NIS2 – represents the most comprehensive EU cybersecurity legislation that the region has ever seen. Slated to go into effect on October 17, 2024, **NIS 2 covers 15 sectors and over 160,000 companies** – including those with more than 250 employees.

The purpose of NIS2 is to **establish a baseline of cybersecurity measures for organizations that provide essential services**. This includes organizations in the public and private sectors, across industries ranging from finance to transportation to healthcare.

Preparing for NIS2 will require companies to rethink the tools, processes and skills that reinforce their cybersecurity.

Why has NIS2 been introduced?

A significant update to the original NIS directive, NIS2 comes at a time when **Europe's cybersecurity threat landscape continues to quickly evolve**.

Since the war in Ukraine began, nation state attacks have increased, according to Microsoft's Digital Defense Report. These bad actors have become more sophisticated, using automation and remote access technologies to attack a wider set of targets – often looking for a vulnerable point of entry within IT supply chains. And often targeting critical infrastructure.

In fact, **the median time for an attacker to begin moving within a corporate network is less than 2 hours**.

Why should NIS2 be a priority?

NIS2 represents an opportunity for organizations to ensure they have the people, processes and partners in place to **protect operations, ensure business continuity and enable digital transformation**. What's more, working to ensure NIS2 compliance will **help build confidence among customers, partners and shareholders**.

What can I do as a business leader to ensure we approach NIS2 in the most effective way?

While working to achieve NIS2 compliance will require thorough preparation and collaboration across an organization, leaders can think about their approach through three broad tenants: **People, Planning and Partners**.



People

Transform your workforce into cybersecurity champions

» Any kind of successful transformation effort is about people and company culture as much as it is about technology. Optimizing your cybersecurity – and preparing for NIS2 – is no exception. This is not just an issue relegated to the IT department or your cybersecurity team. **Effective security requires teamwork** – from workers on the factory floor to the c-suite.

Skilling and education are important components of empowering your people. **The majority (62%) of supply chain attacks are malware.** And as most malware attacks rely on social engineering, you quickly see why people are so important.

» Further, with people working in a more flexible way, **the right tools can help safeguard against threats** – whether someone is in the office, at home or on the road.

» It's also critical to think about how to best augment the skills and experience of your cybersecurity teams. Currently, Europe faces a shortage of around 200,000 skilled cybersecurity professionals. This means teams are often stretched thin.

AI powered tools offer the opportunity to **help cybersecurity teams move faster** while minimizing strain.

1

Cybersecurity training

Educate employees on cybersecurity best practices using Microsoft 365 Learning Pathways and Microsoft Defender for Office 365.

2

Employee security procedures

Control access to sensitive data and monitor insider threats with Azure Active Directory, Privileged Identity Management, Microsoft Information Protection, and Microsoft Inside Risk Management.

3

Use of cryptography

Secure key management and encryption with Azure Key Vault and Microsoft Defender for Cloud.

4

Multi-factor authentication

Enhance user sign-in security with Azure Active Directory Multi-Factor Authentication.

5

Augment cybersecurity talent

Security Copilot draws on Microsoft's global threat intelligence and more than 65 trillion daily signals. The tool delivers insights that increase the quality of threat detection and decrease response times.

Plan

Build a plan for preventing and responding to incidents

Savvy organizations plan to pre-empt attacks. But they also plan for when breaches occur. It is important to note that **NIS2 will require businesses to have plans in place** both for mitigating risk and managing incidents when they do happen.

Pre-empting attacks requires **understanding where vulnerabilities exist** and **implementing safeguards** accordingly.

Risk assessments

Assess risks and comply with regulations using Microsoft 365 Compliance Manager and Microsoft Defender for Cloud.

Supply chain security

Secure devices and networks against supply chain attacks using Microsoft Defender for Endpoint.

Contingency planning involves implementing tools and processes to protect business continuity. It means **ensuring the organization can report incidents accurately** and with machine speed.

Security incident handling

Manage security alerts with Microsoft Sentinel and data security incidents with Microsoft Purview Information Protection and Insider Risk Management.

Business continuity

Ensure operations during and after security incidents with Microsoft Azure Site Recovery and Backup.



Partners

Team up with a trusted partner to improve your cybersecurity posture

For organizations looking to modernize their approach to cybersecurity, **partnerships are key**. As the threat landscape evolves, no organization can effectively mitigate the threat – and ensure accurate, timely incident reporting – while operating in a silo.

Working with a trusted cloud provider represents an essential step to maximize security controls. **Microsoft takes a 'secure by design' approach** with hardened datacentres, managed services and predictive threat mitigation.

The bottom-line: NIS2 isn't just a regulatory requirement – it's **an opportunity to safeguard your business**, help **protect Europe's sovereignty** and **build trust with your stakeholders**.



in research and development of security technology and a world-class team of cybersecurity professionals, Microsoft is committed to helping increase cyber resilience for our customers. Working together, we can help our customers plan for NIS2, prepare their workforce and ultimately improve their cybersecurity posture.

To learn more about how Microsoft can help your organization comply with NIS2 and improve your cybersecurity posture, please contact your account team today.

