NIS2 Directive

What it is and how Quest can help

With cyberattacks on the rise and showing no signs of slowing down, governments around the world have started setting stringent rules for how organizations should — or must — protect themselves and their customers. In particular, in 2023, the European Council and European Parliament updated its Network and Information Systems (NIS) Directive from 2016; the new standard is known as the NIS2 Directive or simply NIS2.

NIS2 applies to all "essential" and "important" entities — generally speaking, if the public relies on an organization's goods or services in their day-to-day lives, it is required to adhere to the NIS2 standards. For example, energy companies, public health, public transportation and public administration organizations are all included, and the mandate may well be found to apply many other sectors, from waste management services to digital service providers that support search engines, social networks or other important services.

But what does NIS2 actually require of these organizations?

What's in NIS2

As with the earlier NIS Directive, organizations subject to NIS2 are required to take technical, operational and organizational measures to manage and protect against risks to their networks and information systems. They're also required to minimize the impact of a potential incident to their employees and users.

New to NIS2, however, is a requirement that organizations must implement a baseline for security measures to ensure a reasonable threshold when security response is required, as well as a plan for what that response should be. This includes, but isn't limited to, baselines for:

- Risk analysis
- Business continuity
- Supply chain security
- Security incident handling

NIS2 also requires that a managing body oversee and approve these baselines and plans, along with the cybersecurity measures and developments in each specific line of business. The personnel of these managing bodies are also liable for significant potential penalties to ensure ongoing security.

Goals of NIS2

Aside from increasing security across many sectors in the EU, a major goal of NIS2 is to streamline reporting of security incidents. Accordingly, NIS2 introduced strict deadlines for various stages of acknowledgment for an incident:

- Within 24 hours of becoming aware of an incident, an organization must provide an "early warning" that indicates whether the occurrence is suspected to have been caused by unlawful or malicious means.
- Within 72 hours of becoming aware of the incident, an organization must provide an "incident notification" that includes information on the severity and impact of the incident, as well as any indicators of compromise (IOCs).
- Within one month of an incident, an organization must provide a "final report" that details what occurred and the root cause.

Since a NIS2 incident equates to a data breach of the EU General Data Protection Regulation (GDPR), the organization must also notify data protection authorities of an incident so they can begin investigating.

NIS2 investigations and penalties

When evaluating a potential NIS2 violation, regulators are provided the following powers of investigation:

- On-site inspections
- Security audits
- Requests for information to assess the entity's security response plans and the measures they have in place
- Security scans
- Access to information to assess the entity's cybersecurity risk management measures, evidence of the implementation of said measures, and any related documents and information

For organizations considered "important" rather than "essential," these measures are allowed only after an incident. But at essential entities, regulators have the power to engage any of these measures that they see necessary as a means to ensure adherence.

The penalties for non-compliance are steep. For essential organizations, monetary fines can be €10 million or 2% of their global business, whichever is higher; for important organizations, fines can be €7 million or 1.4% of their global business, whichever is higher. Regulators also have a list of non-monetary penalties at their disposal.

How Quest can help

The foundation of cybersecurity is keeping identities secure. Simply put, it takes only one account being compromised before you're out of compliance with the NIS2 Directive. And the center of identity for most organizations, across both on-premises and cloud-based apps and services, is Active Directory (AD). That's why it's vital to reduce risks in your AD and Azure AD environment.

That's where Quest can help. The Quest difference is that we provide a complete and continuous strategy to protect identity across its entire lifecycle, thereby strengthening both security and compliance. In particular, we can help meet NIS2's new requirements to establish baselines for:

- **Risk analysis —** Quest can help you build an effective risk analysis process. In fact, we can help you establish a comprehensive risk *management* program. Quest cybersecurity risk management solutions span all five NIST pillars: Identify, Protect, Detect, Respond and Recover. For example, SpecterOps BloodHound Enterprise empowers you to analyze and manage one key risk: the attack paths that adversaries could use to compromise your Active Directory in just a handful of steps. Moreover, the solution pinpoints the key choke points you need to remediate — empowering you to not only analyze risk but significantly reduce it.
- **Business continuity —** Quest is focused not just on cybersecurity, but cyber resilience. After all, cybersecurity is only one piece of a larger goal: keeping your business up and running. Quest cyber resilience solutions enable you to build a comprehensive business continuity strategy so you can effectively defend against and quickly recover from not just malicious attacks, but a wide range of adversity, including natural disasters, power failures, unexpectedly high loads and other threats to your vital IT systems.
- **Supply chain security —** Just how connected organizations are to one another today was vividly illustrated by the 2020 SolarWinds incident: Hackers compromised the private networks of dozens of organizations and spied on them for months by adding malicious code to Solarwinds' Orion software, which the other organizations were using to manage their IT resources. To secure the software supply chain and minimize risks to customers, Quest puts security firmly at the core of its software development lifecycle practices.

  Indeed, although Gartner lists supply chain security as a top security trend in 2022, Quest has invested in supply chain security for years. For example, Quest uses a Zero Trust R&D architecture; performs no development in countries of security concern (COSC); has achieved 93% compliance with NIST SP800-218; and has earned multiple certifications, including SOC 2 Type 2 and ISO 27001, 27017 and 27018. Moreover, to block security breaches like the Solarwinds incident, Quest uses an airgap secured assembly process that exceeds industry standards.

- **Security incident handling —** For Quest, security incident handling is key pillar of a broader cyber resilience strategy. Our solutions help you quickly identify and respond to threats with a consolidated view of across your hybrid IT environment, from on-premises Active Directory, file servers and network-attached storage to Azure AD and Microsoft 365 workloads like Exchange Online, SharePoint Online, OneDrive for Business and Teams. They highlight security vulnerabilities and anomalous activity, and accelerate incident investigations through responsive search and interactive data visualizations. Plus, they can even proactively thwart attacks by preventing changes to your critical security groups and Group Policy objects (GPOs) and blocking attempts to steal credentials by exfiltrating your AD database.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.