NIS2 Directive: The complete guide for in-scope entities

BY ANNA HAMMOND · OCTOBER 15, 2024 · LAST UPDATED ON MARCH 6, 2025

NIS2 will take effect across the EU from 18th October 2024, meaning time is running out to comply with its provisions. This Directive, replacing NIS1 (2016), strengthens requirements for in-scope sectors to report security incidents and manage risk.

In this guide, we'll summarize which entities will need to comply with the enhanced legislation and the standards they must meet. Plus, we'll explore the impact this new law will likely have on the bug bounty industry. But first, let's take a moment to understand what's happened since NIS1 was released.

From NIS1 to NIS2

NIS2 stands for 'Network and Information Security Directive 2'. NIS1 was fully transposed into national law in 2018.

NIS2 builds upon the scope of NIS1 by:

- Introducing stricter cybersecurity requirements
- Reinforcing a framework for coordinated vulnerability disclosure
- Promoting greater standardization across the EU
- Bringing in harder-hitting penalties for non-compliance
- Expanding the coverage of sectors from seven to fifteen, split into essential and important entities.

These changes are reassuring, as they emphasize the criticality of proactive cybersecurity measures and promote greater harmonization across sectors and nations.

In-scope sectors for the NIS2 Directive

The NIS2 Directive broadens its scope from the initial seven sectors under the NIS1 Directive to fifteen, defining them as critical or important entities. For essential entities, non-compliance with NIS2 could result in fines of up to €10,000,000 or 2% of global annual revenue—whichever is higher. For important entities, fines can reach €7,000,000 or 1.4% of global annual revenue—again, whichever is higher.

NIS2 in-scope entities

Essential entities

NIS2 considers entities essential if they provide vital services for the maintenance of crucial societal and economic activities, or if they operate critical infrastructure that could significantly impact public safety, security, or economic stability if disrupted. This includes entities where disruption could cause significant cross-border impacts.

Eight sectors are being considered essential entities. These are:

Energy

The NIS2 Directive mandates energy companies—including electricity, oil, gas, district heating, and hydrogen—to protect their networks and systems due to their essential services and vulnerability to cyberattacks.

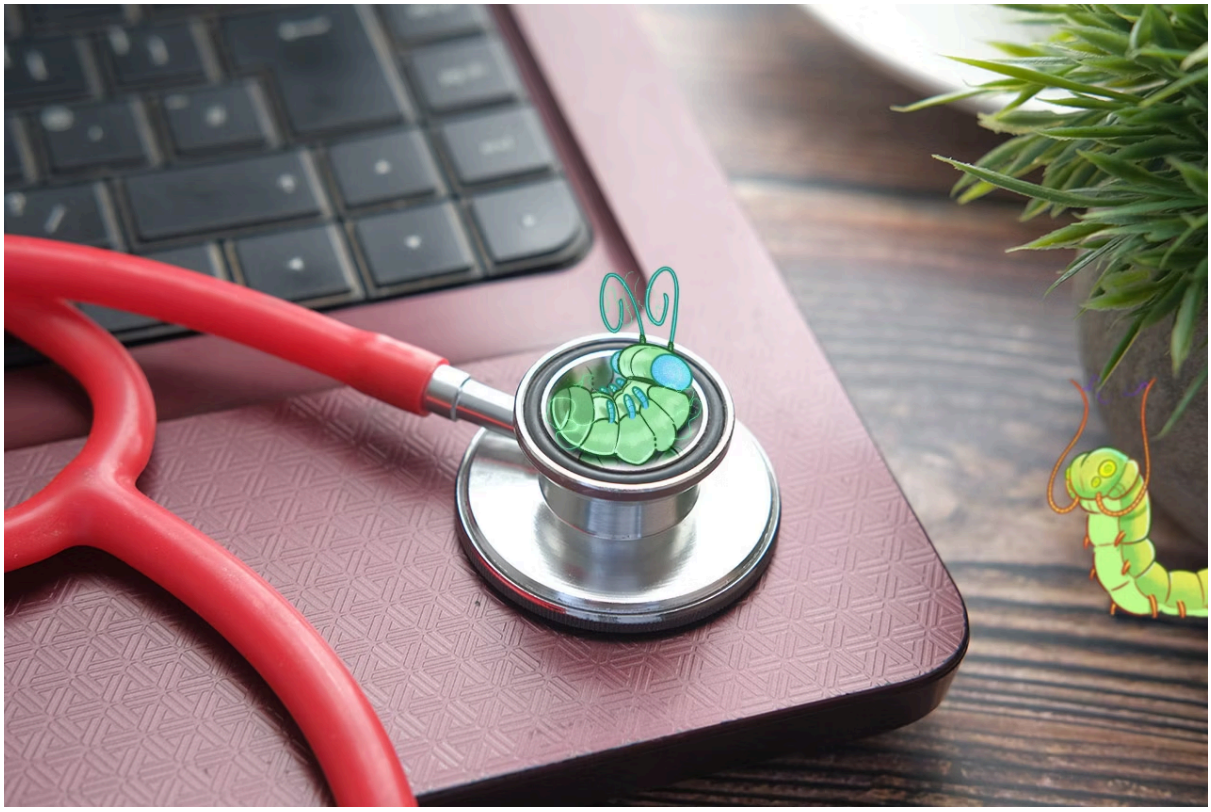
NIS2 and the energy sector

Energy companies must implement robust technical and organizational measures to safeguard critical infrastructure, ensure data protection and privacy, and maintain the availability of energy services. They are also required to appoint a responsible person for compliance, conduct regular risk assessments, and cooperate with national authorities.

By enhancing security and data protection, the Directive could boost consumer confidence, foster market growth, and promote sustainability within the sector.

Health

The healthcare sector, comprising public and private providers, medical manufacturers, insurers, and critical health services, is vital to European society and economy.



NIS2 and the healthcare sector

Under NIS2, healthcare organizations must prioritize patient data protection, implement robust cybersecurity measures to prevent service disruptions, and comply with strict data privacy regulations. The Directive mandates measures such as cyber risk management, incident reporting, regular system testing, staff training, and response planning to minimize cyber threats and ensure continuity of care.

Transport

The transport sector, employing nearly 10 million people in Europe, is crucial for connecting people and businesses, encompassing everything from urban public transport to inter-regional air travel. This sector includes air, rail, water, and road transportation.

NIS2 and the transport industry

The NIS2 Directive will significantly impact the transport sector, mandating enhanced cybersecurity measures. Transportation companies must **evaluate and manage cyber threats** from external suppliers, secure real-time data exchange channels, and safeguard operational technology within supply chains. This includes implementing security standards, encryption, access controls, and intrusion detection systems.

Finance

The finance sector, which includes banks, investment firms, insurance companies, and financial market infrastructure, is integral to the European economy and has been under increasing regulatory scrutiny to **bolster its stability and resilience**. The upcoming NIS2 Directive is set to significantly impact this sector by mandating enhanced security and resilience of critical systems and networks.

NIS2 and the finance industry

Financial institutions must review and upgrade their cybersecurity measures to meet these new requirements, given the sensitivity of financial information and the high value of transactions they handle. Institutions will need to:

- Ensure business continuity through contingency plans
- Protect financial data with robust security measures like encryption and access controls
- Manage third-party risks through regular assessments and compliance agreements.

Effective implementation of NIS2 is expected to lead to a more secure finance market and increased confidence in financial institutions.

Water supply

The water supply sector includes drinking water and wastewater services. The Directive emphasizes the protection of critical infrastructure, such as water treatment and distribution systems. It will require water utilities to invest heavily in cybersecurity measures to ensure resilience against cyber threats. This may involve increased budget allocations for technology upgrades, new security tools, and employee training programs to maintain service continuity and public trust.

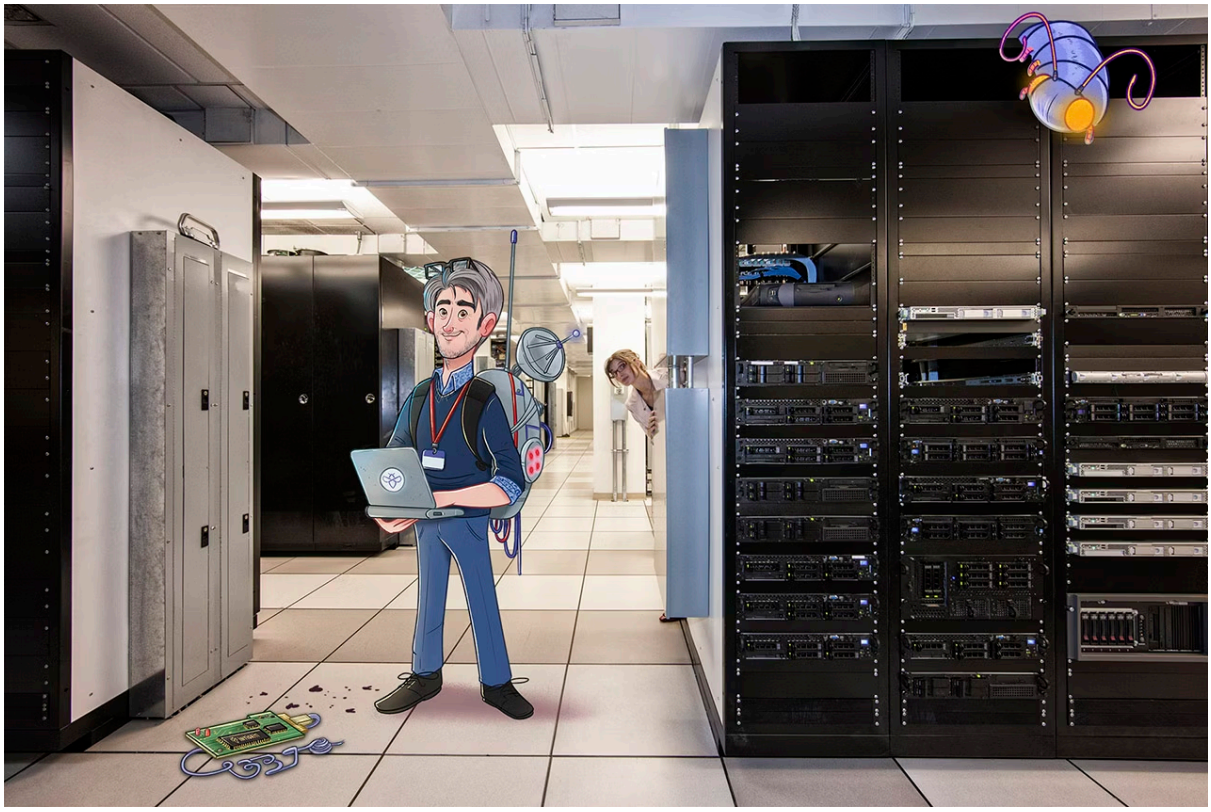
NIS2 and the water supply sector

Additionally, NIS2 mandates coordination with other sectors to develop coherent cybersecurity strategies and compliance with the Directive's requirements.

Water utilities must implement risk management processes specifically for their Operational Technology (OT) systems, which are crucial for managing critical processes like chemical dosing and pressure regulation.

Digital infrastructure

The digital infrastructure sector will face significant changes under NIS2, affecting all operational aspects. Operators may need to upgrade physical security measures, such as installing security cameras, to monitor and control access to sensitive areas. Additionally, they must develop robust incident response and recovery plans, including designated response teams and communication channels for rapid information sharing and evidence-gathering.



NIS2 and the digital infrastructure industry

The Directive will also bring heightened regulatory oversight, with EU authorities enforcing stricter security standards and holding companies accountable for protecting their critical systems. This increased scrutiny is expected to drive demand for innovative cybersecurity solutions, fostering competition and innovation within the digital infrastructure market. Overall, NIS2 aims to enhance the security and resilience of this vital sector, ensuring the continuity and safety of digital services.

Public administration

The public administration sector, which provides essential services like social services, public safety, and economic regulation, is crucial to European society. Given the vast amounts of sensitive information it manages, this sector is at high risk of cyberattacks.

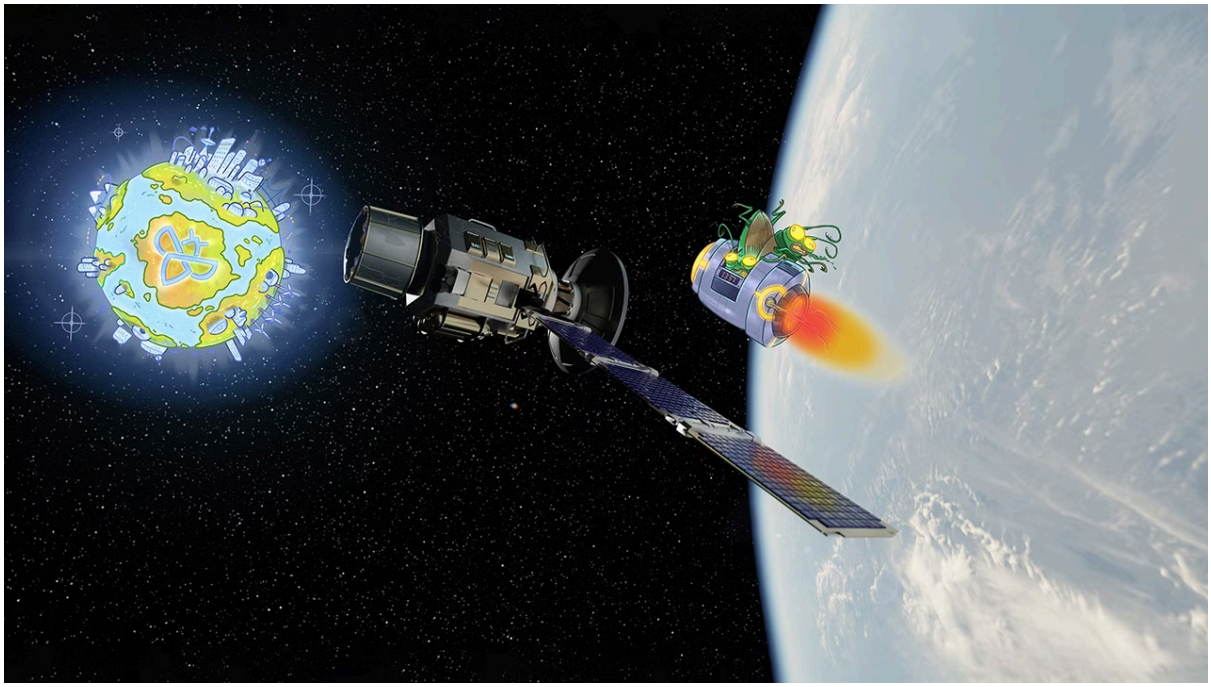
NIS2 and public administration

The NIS2 Directive designates public administration as an "essential entity," emphasizing the need to **safeguard it against cyber threats** to ensure the stability of European infrastructure. The Directive requires public administration organizations to implement enhanced security measures to protect sensitive information, conduct regular risk assessments, and report on their cybersecurity posture.

To comply with NIS2, public administration organizations must invest in employee cybersecurity training to raise awareness levels, given the varying degrees of cybersecurity knowledge among staff. The Directive aims to strengthen the sector's defenses by mandating best practices, ensuring essential services remain available to citizens. Regular risk assessments and incident response planning will help the industry stay vigilant and prepared against evolving cyber threats and vulnerabilities, ultimately enhancing the security and resilience of public administration services.

Space

The space sector, vital for telecommunications, navigation, and national security, is a prime target for cyber threats due to its critical importance. Space organizations must now report cyber incidents impacting infrastructure like satellites and ground stations, introducing new threat monitoring and response standards.



NIS2 and the space sector

The Directive also mandates closer collaboration with regulatory bodies to share information and improve overall cybersecurity. Additionally, it emphasizes supply chain security, requiring robust risk management practices for suppliers and contractors.

Important entities

The NIS2 Directive also introduces new cybersecurity requirements for 'important entities,' including:

- Digital providers
- Postal services
- Waste management
- Food
- Manufacturing
- Chemicals
- Research sectors

These entities must now prioritize incident reporting, supply chain security, risk assessments, and sector-specific guidelines. While compliance may increase costs and administrative burdens, the Directive aims to foster greater accountability, transparency, and collaboration, ultimately enhancing cybersecurity and resilience across the sectors.

NIS2 Directive will bring opportunities to the bug bounty industry

Based on the provisions and aims of the NIS2 Directive, it is likely that more organizations will adopt crowdsourced security, such as bug bounty programs. Here's why:

Bug bounty aligns with proactive security and incident response planning

The NIS2 Directive emphasizes the importance of proactive cybersecurity measures and incident response planning. Bug bounty programs align perfectly with these goals by encouraging ethical hackers to identify and report vulnerabilities, enabling organizations to fix them before they can be exploited by malicious actors.

Bug bounty programs support most of the in-scope entities

The Directive expands the scope of sectors and entities required to implement robust cybersecurity practices. Many of these organizations will find bug bounty programs to be a cost-effective and efficient way to enhance their security posture. By leveraging the collective expertise of a global community of ethical hackers, organizations can continuously test across multiple assets and improve their defenses.

Collaboration and transparency are at the core of crowdsourced security

The NIS2 Directive promotes a culture of transparency and collaboration in cybersecurity. Bug bounty programs embody this spirit by fostering open communication between organizations and the security research community. This collaborative approach can lead to more innovative and effective solutions for protecting businesses and consumers from cyber threats.

Bug bounty fits with coordinated vulnerability disclosure (CVD)

A pivotal addition to NIS2 is the establishment of a coordinated vulnerability disclosure (CVD) framework. This framework encourages the responsible reporting of security vulnerabilities by researchers and stakeholders, providing a structured process for addressing and resolving these issues—bug bounty programs are a step above this. This collaborative approach enhances the overall security of critical sectors. However, vulnerability disclosure programs can be a great starting point.

Potential challenges for the bug bounty industry

With the NIS2 Directive, we might see organizations rush to implement bug bounty programs without doing their research or getting support from a bug bounty platform. This could lead to several challenges, such as poor engagement on their programs or an influx of duplicate reports, further burdening already-stretched in-house security teams.

Additionally, without clear guidelines on safe harbor provisions and responsible disclosure, there could be increased tension and uncertainty between organizations and ethical hackers. Without a structured

bug bounty platform, organizations might struggle with other legal complexities involved in working with international ethical hackers, such as managing payments.

Overcoming these challenges

To overcome these challenges, companies can work together with a bug bounty platform. For example, Intigriti's platform and services can assist with setup and **maximize the impact** of your program's budget, leading to more insightful results.

The platform has the infrastructure to facilitate payment processing worldwide, making working with international ethical hackers simple and painless. Plus, Intigriti offers a legal framework that both hackers and customers adhere to, ensuring everyone is on the same page.

The release date of NIS2 may be imminent, but it's not too late to empower your proactive cybersecurity measures and incident response planning through crowdsourced security. To speak to a member of the team, **get in touch** today!

Further resources:

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive