BE PREPARED

Andrus Kivisaar *reports on the importance of being ready for the NIS2 Directive*

Picture credit: Adobe Stock

Throughout the last few years, cyber attacks and cyber security threats have become some of the most persistent, critical risks to all kinds of organisations, businesses and governments. In fact, analyst firm Gartner predicts that by 2025, threat actors will have weaponised operational technology environments successfully to the extent of being able to cause human casualties.

Attacks on critical infrastructure are also increasing in frequency and complexity. Colonial Pipeline, the largest pipeline system for refined oil products in the US, fell victim to a catastrophic cyber attack in 2021. Ransomware forced the company to shut down operations and freeze IT systems – a measure that halted all pipeline operations and created a frenzy of consumer panic.

Exacerbated by the 2022 Russian invasion of Ukraine, the European Union itself has faced growing cyber security risks, particularly through ransomware, malware and DDoS threats. In fact, after the European Parliament voted to declare Russia a state sponsor of terrorism in November of 2022, it was hit by one of the most sophisticated DDoS attacks it has faced to date.

To ensure that organisations are prepared to take action against these rapidly advancing threats, the European Union has introduced the NIS2 Directive – legislation specifically designed to strengthen cyber security and cyber resilience in the EU. All EU Member States must incorporate the provisions of the NIS2 Directive into their legal frameworks by September 2024.

NIS2 is the most comprehensive European cyber security directive to date, making it imperative that companies identify and implement the necessary tools needed to comply with and mitigate these ever-growing threats.

The NIS2 Directive is EU-wide legislation to enhance cyber security across EU Member States. The NIS2 Directive provides additional legal measures to further boost the overall level of cyber readiness in the EU, subsequently making the European Union more cyber resilient in general. The NIS2 Directive's primary goal is to enhance the security of networks and information systems, requiring operators to maintain critical infrastructure, implement security measures and report incidents to authorities.

The new NIS2 legislation is an updated version of the original Directive – the first of its kind on cyber security. Since its implementation in 2016, EU policymakers have identified numerous flaws in the original legislation, prompting the need for an updated version. Thus, the new NIS2 Directive modernises the existing framework to keep pace with the ever-changing cyber threat landscape and address the impact of increased global digitisation.

It's predicted that by 2025 threat actors will have weaponised operational technology environments to the extent of being able to cause human casualties

The NIS2 Directive accommodates the aforementioned updates by expanding the minimum cyber security standards and requirements to new entities and sectors, further improving cyber resilience and incident response capabilities of authorities and private and public entities.

Businesses that operate in the EU and provide digital services or critical infrastructure are now subject to the NIS2 Directive requirements. Furthermore, the NIS2 Directive applies the 'cap-size rule', meaning all medium and large-sized entities within specific sectors fall within the Directive's scope. The European Commission estimates that around 110,000 companies fall within the scope of NIS2.

The Directive applies to entities divided into two categories: essential and important. The 'essential' category encompasses critical sectors such as energy, transport, banking, financial markets, health, drinking water, digital infrastructure, ICT sector management, space and specific public administration entities. The 'important' category covers postal services, waste management, food production, chemical production and distribution, digital providers, and research.

While the overall goal of NIS2 is to bolster cyber security throughout the EU, its provisions fundamentally apply to any company providing or operating with digital services and critical infrastructure in today's risk-heavy cyber environment. The previously outlined threats are critical to various businesses and can be seen across all sectors and borders – whether or not one operates in the EU.

There are four key areas that the NIS2 Directive addresses in addition to expanding the requirements to new entities and sectors, including risk management, incident reporting, oversight, and enforcement. Across sectors and organisations, heeding the updated requirements will aid

ORGANISATIONS CAN ADHERE TO NIS2 INITIATIVES BY UTILISING THE RIGHT TOOLKIT

organisations in strengthening their preparation for cyber security threats and risks.

CYBER SECURITY RISK MANAGEMENT MEASURES

NIS2 requires entities to implement specific cyber security risk management policies, including risk analysis and incident response, encryption and cryptography, vulnerability disclosure, cyber security training and ICT supply chain security.

INCIDENT REPORTING

NIS2 requires an initial notification obligation within 24 hours once made aware of certain incidents, a second notification within 72 hours, and a final incident report within one month.

'MANAGEMENT BODY' OVERSIGHT

NIS2 imposes direct obligations on management bodies to approve and supervise the utilisation of the cyber security risk management measures. Members of the management bodies should undergo regular training on cyber security risks and assessing risk management practices.

ENFORCEMENT

National authorities possess enforcement powers that include suspension of an entity's authorisation to operate, publication of noncompliance, imposing personal liability on members of the management bodies, and administrative fines of up to 10-million Euros, or 2 percent of total worldwide turnover – whichever is higher.

First and foremost, companies abiding by the NIS2 Directive must implement appropriate technical and organisational measures to assess security risks to their network and information systems. Furthermore, the NIS2 Directive requires companies to implement a comprehensive Application Programming Interface (API) security programme to include different measures such as authorisation, authentication encryption, and monitoring.

For most organisations, a significant challenge will be properly implementing additional security controls to ensure that only authorised parties can access the APIs. Finally, companies also must report security incidents to the authorities.

Properly preparing for NIS2 may vary from sector to sector, however. For example, in the energy sector,

key security challenges revolve around supply chain risks, ageing technologies and interconnected systems. Meanwhile, the challenges faced by the transportation sector are ransomware attacks, limited security investments and employee training. Organisations within the finance sector, on the other hand, need to mitigate risks such as phishing, web-based or social engineering attacks.

BUSINESSES THAT PROVIDE DIGITAL SERVICES IN THE EU ARE NOW SUBJECT TO NIS2 REQUIREMENTS

Regardless of industry, a crucial aspect of maintaining a high level of security – particularly under the NIS2 directive – is creating and maintaining security awareness. The human element is the most common threat vessel, representing the root cause of 74 percent of 2023 data breaches and carrying a huge cost implication, with the cost of data breaches predicted to rise to more than $5-trillion in 2024, for instance. Implementing security awareness training programmes is therefore a fundamental part of any security strategy in a landscape inundated with phishing emails, ransomware and social engineering attacks.

Organisations can successfully adhere to NIS2 initiatives and amplify their cyber preparedness by utilising the right toolkit – like cyber range technology and training. Numerous aspects of cyber range technology can help organisations prepare for and implement NIS2 initiatives while reaping organisational benefits such as improved cyber security, enhanced cooperation and increased potential for innovation.

This NIS2 Directive provides more flexibility to EU member states to cooperate and encourages sharing information about cyber security incidents. When an organisation utilises cyber range training, employees and customers have the potential to become well-trained on various facets of cyber security, further enhancing effective knowledge and communication around incidents. This training supports the various parties involved in a cyber attack to be up-to-date with incident details and allows for a more effective approach to handling cyber threats.

Because of the expanded scope of the NIS2 Directive and its complex, strengthened security requirements, the directive aims to increase Europe's overall cyber security level. Across sectors – energy, transportation, finance and so on – implementing cyber range technology to experience real-world threats in a safe yet realistic environment prepares employees for a range of high-stress scenarios relating to cyber attacks and how to best respond to each. Amid numerous benefits of experiencing real-world simulations specific to an organisation, implementing cyber range technology increases preparedness and confidence in responding to various cyber threats.

Another goal of the NIS2 Directive is to further promote the development of cyber security products and services that reflect the needs of the EU market. Cyber range technology has the potential to bolster innovation in the cyber security industry, and prioritising cyber readiness creates new business opportunities and avenues for cyber industry advancement. Cyber range technology also supports companies responsibly scaling as they grow, advancing innovation throughout additional sectors.

The NIS2 Directive will prompt a substantial advancement in cyber security across the EU as it helps businesses prepare for cyber attacks, strengthen cyber resilience, and develop a more widespread security culture. While September 2024 may seem far off, the reality is that it's important to start taking the necessary steps to implement NIS2 now. Any organisation operating in or providing digital services across sectors within the EU should start strategically planning before it is too late. It is vital to know that while NIS2 will officially be implemented in September 2024, the initiative has already come into force ●

Andrus Kivisaar
is a CEO and co-founder of CybExer Technologies. He has close to two decades of experience in managing international, large-scale IT infrastructure projects including in market-leading financial institutions and core national healthcare organisations.

NIS2 is the most comprehensive European cyber security directive to date

Picture credit: Adobe Stock