09.10.2024 – 11:30 Uhr

Why UK Organisations Can't Afford to Ignore NIS2, the EU Cybersecurity Directive

- **The NIS2 Directive is an EU regulation designed to boost cybersecurity across critical sectors like energy, transport, and digital infrastructure.**
- **Experts warn that UK companies working with EU partners risk operational disruptions if they fail to meet NIS2 compliance standards.**
- **With NIS2 compliance imminent, affected organisations will be expected to implement stronger cybersecurity measures, ensure prompt incident reporting and maintain up-to-date security practices.**

London, October 9 2024 – Although the EU's new Network and Information Security Directive (NIS2) doesn't apply directly to UK organisations, its impact will be felt by those working with EU partners. NIS2, which aims to strengthen cybersecurity in critical sectors, replaces the original 2016 directive and will soon come into force, requiring organisations to improve their security measures. NIS2 expands the scope of affected organisations to include companies with more than 50 employees or an annual turnover of more than €10 million, imposes stricter security requirements, and extends the scope to additional sectors.

According to Bureau Veritas, the impact of non-compliance with NIS2 standards can be significant. Firstly, organisations may experience disruption to their business operations. Financially, important and essential organisations could face hefty fines of up to 7-10 million Euros. In addition, management may be held legally responsible for their failure to meet compliance standards.* "Many more UK organisations than you might expect collaborate with European partners. UK organisations must act swiftly to determine if the NIS2 Directive applies to their operations," explains Keith Poyser, Vice President for EMEA at Horizon3.ai. The NIS2 regulation is set to be adopted soon in the EU, and a recent PwC article reveals that the UK is preparing to implement its own NIS changes in 2024.**

The NIS2 Directive applies to organisations based on three specific criteria. First, any company providing services or carrying out activities within the EU must comply regardless of location. Second, the Directive targets medium-sized and large organisations. Finally, companies classified as “essential entities”, or “important entities” must comply with the rigorous cybersecurity standards of NIS2. This broad scope will require a significant number of UK organisations with EU connections to assess their compliance in order to avoid disruption with European partners. After all, even in a post-Brexit-landscape, the EU remains the UK’s most important trading partner, accounting for 42% of UK exports and 52% of imports.

Ensuring Cybersecurity: NIS2 Compliance for Vital Sectors

The regulations of NIS2 require organisations to implement comprehensive security policies that demonstrate their approach to securing their networks and IT systems. One of the demands involves the establishment of a strong risk management framework to proactively identify and address potential threats. Furthermore, regular risk assessments and a well-defined incident response plan outlining the procedures for detecting and handling security incidents are stipulated. Continuous monitoring of IT system activity through automated tools is also essential to quickly identify and respond to threats.

NIS2 covers a wide range of critical sectors, targeting the so-called "essential" and "important" entities. These include vital industries such as energy, transport, banking, financial market infrastructures, health, and essential utilities such as drinking water and wastewater management. The Directive also encompasses digital infrastructure, postal and courier services, and key manufacturing and food production areas. In addition, sectors like the chemical industry, space, public administration, and broader digital infrastructure are required to comply with NIS2. "It is vital for UK organisations to be aware that the Directive applies not only to companies in the sectors it covers, but also to all of their suppliers and customers along their entire value chain," says Keith Poyser, Vice President for the EMEA region. This comprehensive coverage is designed to ensure that all critical parts of society and the economy are protected from new and emerging cyber threats.

Leadership faces Liability under NIS2

Ernst & Young aptly points out that a key difference between NIS2 and its predecessor, NIS, is the introduction of personal accountability.*** This provision can make CIOs, CEOs and board members of non-compliant organisations personally liable. In the case of UK companies, this could have the effect of separating them from their EU partners. "Take a British cloud provider serving customers in France. If they do not comply with NIS2 standards and a breach occurs, the executives of the French company face significant fines. This could lead to substantial business losses for British firms that have not addressed NIS2. British executives need to improve their compliance now to avoid these serious risks," says Keith Poyser.

Why Pentesting Outperforms Defensive Security Strategies

Despite the very realistic cyber risks we face daily, most organisations still rely on defensive methods such as firewalls to protect their IT networks from cyber attacks, assuming these systems will be effective if the worst happens. In fact, without rigorous testing, it is impossible to guarantee that these measures will withstand an attack.

The most reliable way to ensure cybersecurity resilience is through penetration testing or pentesting. “A pentest is essentially a controlled, large-scale cyberattack, allowing companies to evaluate their security without the risk of real criminal activity,” explains Keith Poyser, Vice President for EMEA at Horizon3.ai. In Europe, the European Central Bank (ECB) has already recognised the importance of pentesting, conducting cyber resilience stress tests on over 100 banks this year. With the EU’s NIS2 Directive becoming legally binding in mid-October, penetration testing is set to become a critical component of cyber resilience across various industries, extending far beyond the financial sector.

Keith Poyser confirms this: “There has already been a significant increase in demand for penetration testing, both in the EU and at a global level, due to the fact that so many EU companies are integrated into global supply chains. A cyber attack on one business partner can impact all connected companies, driving the need for rigorous security measures. Today, penetration testing is not a one-and-done activity. It must become a continuous approach, ingrained within the context of risk reduction and mitigation.”

NIS2 Compliance: A Global Competitive Advantage

Companies can reap significant benefits from adhering to NIS2 compliance, even if they are not based in the EU. One of the primary advantages is establishing a solid competitive edge in the global marketplace. Organisations can build and reinforce trust with European clients and partners by demonstrating a commitment to the cybersecurity standards set forth by the NIS2 Directive. This trust is crucial as it signals a dedication to protecting sensitive information and maintaining high-security standards, which can differentiate an organisation from its competitors. Furthermore, compliance with NIS2 can enhance an organisation’s reputation for reliability and responsibility, potentially leading to increased business opportunities and more robust partnerships with organisations across Europe and beyond.

*https://www.bureauveritas.co.uk/needs/network-and-information-security-directive-nis2

**https://www.pwc.co.uk/issues/cyber-security-services/research/is-your-organisation-ready-for-nis-2.html#:~:text=The%20UK%20will%20not%20be,of%20social%20networking%20services%20platforms

***https://www.ey.com/en_ie/consulting/what-strategic-actions-can-organisations-take-to-be-nis2-compliant

About Horizon3.ai and NodeZero™: Horizon3.ai's NodeZero™ Autonomous Security Platform offers integrated threat detection, autonomous pentesting, third-party risk management, and comprehensive governance, risk, and compliance (GRC) insights. It enhances organisational security by proactively identifying and remediating exploitable vulnerabilities, while strategically deploying deception and threat detection through NodeZero Tripwires™. Founded in 2019 by former industry leaders and U.S. National Security veterans, Horizon3.ai is at the forefront of cybersecurity innovation. Request a free demonstration at: www.horizon3.ai.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information: Horizon3.AI Europe GmbH, Sebastian-Kneipp-Str. 41, 60439 Frankfurt am Main, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, E-Mail: team@euromarcom.de

- - - -

Medieninhalte

Source:
Horizon3.ai

Diese Meldung kann unter https://www.presseportal.de/en/pm/163532/5882467 abgerufen werden.