**The road to digital security: a look at the EU’s NIS2 Directive**

**Cyberthreats and the European response**

Growing digitalisation doesn’t just bring progress. It also poses an increasing risk: cyberattacks. To address this, the European Union introduced the NIS (Network and Information Security) Directive in 2016. The aim was to strengthen cybersecurity in strategic, essential sectors: specifically energy, transport, banking, financial markets, healthcare, water, and digital infrastructure.

Since then, however, there have been fundamental changes in society, particularly post-COVID. The mass deployment of video conferencing tools (such as MS Teams, Zoom or Google Meet) paired with increased demand for e-commerce and delivery services have intensified the transition to the digital world. In fact, McKinsey estimates the pandemic accelerated digitalisation by 3 to 4 years. Such developments brought new cybersecurity challenges – and so the EU had to update their Directive.

**NIS2: Tighter rules for a safer world**

The EU adopted the new NIS2 Directive in November 2022. This Directive significantly expands the scope of the original legislation and tightens security measures. In addition to the seven original sectors, NIS2 now covers new areas such as manufacturing, postal/courier services, science, research, and education.

NIS2 requires companies and organisations in all these sectors to identify and manage cyber risks, secure information systems, and regularly train staff. One of the new regulations even states the obligation to report serious security incidents within 24 hours of discovery, with a detailed report within 72 hours, and a final report within 30 days.

The directive also divides organisations into two categories - 'essential' and 'critical' entities, with each category having specific obligations. Penalties for non-compliance with the rules can be very severe. Essential entities face fines of up to €10 million or 2% of worldwide annual turnover, whichever is higher. Major entities can be fined up to €7 million or 1.4% of turnover.

NIS2 thus plays a key role in ensuring cyber security across the EU. The organisation is committed to introducing new measures and adhering to strict rules to protect critical infrastructure such as energy grids, water and healthcare. This ensures that essential services that people rely on remain functioning and secure in the event of a cyber-attack.

**How is 2N preparing for NIS2?**

2N must comply with NIS2: It qualifies as an obliged entity (over 250 employees and an annual turnover of more than €10 million) and falls under multiple regulated sectors such as "Manufacture of electronic devices and equipment," "Provision of publicly available electronic communications services" and also "Cloud computing service provider".

The company has been active in the issue of cybersecurity for a long time and holds ISO 27001 certification, which it regularly upholds in surveillance and recertification audits. This year, 2N has also obtained the security certification IEC 62443-4-1, which applies to its elevator products.

But what’s next? 2N must comply with the strict NIS2 rules and thoroughly and regularly review existing security measures. As such, they are conducting a gap analysis to determine which NIS2 obligations it already meets (through the ISO 27001 certification) and what still needs to be implemented. With cybersecurity being one of 2N's top priorities, the company expects compliance with the remaining requirements to go smoothly and by the legally required deadline. You can be assured that when you choose 2N, you’re not risking non-compliance with EU directives.

**Knowledge, trust, and transparency: key values**

2N has long built on the extensive cybersecurity knowledge and experience of its parent company AXIS. Experts from both companies are in daily contact and share best practices and ideas for secure development.

One of the key tools that 2N has adopted is the Axis Security Development Model (ASDM), which outlines 13 processes and security practices that focus on implementing (and subsequently verifying) security measures at every development stage. This approach minimizes the risk of security incidents and strengthens the trust and satisfaction of its customers.

Trust and transparency between the company and its customers are key values for 2N. The company publishes all cybersecurity-related materials and information on its website - which not only ensures the security of its products and services but also strengthens your confidence in their reliability.

**Banner – trend article**

2N’s Insight into the NIS2 Directive

Are you getting more and more questions about the EU’s upcoming NIS2 Directive and its impact on businesses? Find out what it means, who it affects, and how 2N, a leading access control systems supplier, is preparing for it in this insightful article

>>Read on

**Email – hardening guide**

**Subject:** Strengthen Your Network Security with the 2N Hardening Guide

**Preheader:** Download

Dear [Recipient's Name],

In today’s rapidly evolving cybersecurity landscape**, ensuring the security of your IP-based devices is no longer optional—it’s essential**. With cyber threats becoming increasingly sophisticated, the need to safeguard systems has never been more urgent.

To help you stay ahead, we’re offering the 2N Hardening Guide—a **comprehensive resource** that **outlines critical best practices** for improving the security of 2N network devices.

Whether you're managing devices in a high-security environment like healthcare or government, or simply looking to secure a residential or multifunctional building, these recommendations are designed to minimize vulnerabilities and strengthen your defences.

What You’ll Learn

* **Setting Strong Passwords:** Establishing robust credentials to prevent unauthorized access
* **Regular Firmware Updates:** Patching known vulnerabilities to stay ahead of threats
* **Secure Communication Protocols:** Ensuring safe communication between devices
* **Enabling Encryption**: Protecting sensitive data during transmission
* **Disabling Unnecessary Services:** Minimizing potential attack surfaces
* **Limiting Network Access:** Reducing exposure by restricting access to trusted users
* **Network Segmentation:** Isolating critical devices from broader network traffic to enhance security

Don’t wait until a breach happens. Educate yourself and protect your system now. The 2N Hardening Guide is your essential resource for maintaining a robust, secure network.

[Download it]

Best regards,