10 steps to NIS2

How to prepare yourself properly

1 Check whether the following two criteria for NIS2 validity apply to your company

→ Do you operate in one of the **critical infrastructure sectors defined by NIS2?**

→ Is your company larger than 50 employees or does your annual revenue exceed 10 million or are you the sole provider of an essential or critical service as defined by NIS2?

2 Inform yourself and your management about the NIS2 directives and sanctions

→ NIS2 primarily formulates requirements for cybersecurity risk management and reporting requirements. These are explained in more detail in the following steps.

→ Notify your management about the high fines (up to 10 million euros or 2% of the previous year's annual revenue) and the liability of management bodies on NIS2.

3 Take stock of your network security inventory

→ Assess your employees' security awareness and your current precautions.

→ List your risk management measures and procedures to date.

4 Compare the status quo with the NIS2 specifications

→ Look at the ten NIS2 requirements on risk management:

1. Risk analysis and information security policy
2. Security incident management
3. Business continuity plan including crisis and recovery management
4. Supply chain security
5. Security audited network and information systems
6. Measures evaluation
7. Cyber hygiene processes
8. Training procedures
9. Use of cryptography and encryption
10. Access controls and multi-factor or continuous authentication, and secure communications

5 Determine your need for action and plan necessary expenditures for it

→ Plan the budget for actions you still need to follow up on.

6 Ensure your responsiveness and correct security incident reporting

→ Define and refine your risk management in accordance with NIS2.

→ Establish a network security emergency response team that is always on call.

→ Align your reporting procedures with NIS2 requirements (including initial report within 24h, final report after no more than one month).

7 Whip your internal and external network security into shape

→ **Use secure, backdoor-free network technology and systems**, and emphasize secure network management and maintenance.

→ Secure network access and traffic with up-to-date authentication and encryption.

→ Sharpen your security concepts, policies, and procedures in respect to NIS2.

→ Raise awareness and train employees in regard to network security.

→ Secure your supply chains and connections to suppliers and partners in accordance with NIS2.

8 Ensure your business continuity and crisis recovery

→ Establish a crisis and recovery management plan to maintain business operations.

→ Arm yourself against data loss, extortion, etc. with data backups, geo-redundant servers, etc.

9 Strengthen your own digital sovereignty

→ **Evaluate the status quo** of your own digital sovereignty.

→ Remain capable of action and autonomous with the **following tips**.

10 Rely on good cooperation and support

→ **Use next-generation firewalls with unified threat management** and user-friendly management.

→ **Use cloud-managed security** to support in-house IT.

→ Take advantage of support and training offers for your devices and software.

LANCOM SYSTEMS