NIS-2 Directive:
How Endian supports your implementation

The global economy is increasingly dependent on digital solutions. Different services and sectors are more and more interconnected and depend on a seamless collaboration. This situation fosters a rapidly growing cybersecurity threat landscape: any single IT security incident, even if it initially affects only a single organization, can cascade to other sectors and companies, negatively impacting the entire EU common market.

The European Union therefore decided that action was required and introduced the NIS-2 Directive (Directive on security of network and information systems). This is based on the original NIS Directive from 2016 and pursues two important goals. On the one hand, it is intended to ensure higher standards in network and information security. In addition, it aims to harmonize the level of security in the EU member states in order to strengthen Europe's overall cyber resilience.

Until October 17, 2024, the EU countries have a deadline for implementing the directive into national law. Companies operating in the EU should therefore familiarize themselves with NIS2 now in order to clarify whether they are affected. The EU not only prescribes technical measures, but also a risk management approach that requires sufficient time to implement.

This article provides an overview of the key points of NIS2 and shows how Endian can support the implementation of the requirements.

With Endian, you have the ideal partner for NIS2 at your side: as an IT security vendor, Endian works according to the principle of "security by design" and has many years of experience in digitalization projects. Endian is independent, owner-managed and based in the heart of Europe.

Who is affected?

Important: The authorities will not tell you whether your company belongs to the critical sectors according to NIS2. You must therefore be proactive and assess whether the directive is relevant to your company or organization based on the specifications.

NIS2 expands the group of companies affected: While there were only eight sectors in the first NIS directive, there are already 18 in NIS2. A distinction is made between essential sectors (essential entities) and important sectors (important entities):

Essential Entities:

- **Energy** (electricity, district heating, oil, natural gas, hydrogen)
- **Healthcare** (healthcare providers, EU laboratories, medical research, pharmaceuticals, medical devices)
- **Transportation** (air, rail, road and shipping)
- **Banks** (credit institutions)
- **Financial services** (trading venues and central counterparties)
- **Drinking water** (suppliers and providers)
- **Waste water**
- **Space sector**
- **ICT service management**
- **Public administration** (central and regional)
- **Digital infrastructure** (Internet nodes, DNS service providers, TLD name registries, cloud providers, data centers, content delivery networks, trust services, communication networks and communication services)

Important Entities:

- **Postal and courier services**
- **Waste management**
- **Chemicals** (production, manufacturing and trade)
- **Food** (production, manufacturing and wholesale)
- **Manufacturers** (medical devices and in-vitro diagnostics, computers, electrical equipment, optics, machinery, automotive and parts, vehicle manufacturing)
- **Digital suppliers** (online marketplaces, search engines, social platforms)
- **Research**

Size Regulation

The NIS2 also introduces a new size regulation: All medium and large companies in the sectors mentioned above are included in the scope. This applies to companies with 50 or more employees or €10 million in turnover, regardless of the performance or threshold levels of their facilities. At the same time, the EU gives member states some room for discretion to also assign smaller companies with a particularly high criticality to the critical sectors.

Measures

The NIS2 includes stricter regulations in risk management. Companies must establish an appropriate level of security and demonstrate that they can prevent, detect and respond to security incidents in an emergency.

The extensive requirements cannot only be met by implementing technical solutions, but also require a close look at the processes within the company.

That is why we present here how Endian's cybersecurity solutions can be complemented by services from consulting companies in order to comply with NIS2 in all respects.

Concepts for Risk Analysis and the Security of Information Systems

The starting point for all further steps is the recording of the current status. Set up a task force to determine the status quo and work out the need for action.

How can Endian help here?

If needed, our system integrators and consultants can assist in this area.

How can consultants help here?

In order to assess the current situation and define a target, a target/actual analysis is done. Appropriate measures can then be planned and implemented based on detailed documentation.

Incident Management

Structured incident management can minimize the impact of a cyberattack and protect your company's data and systems. The prerequisite for successful incident management is to identify the attack itself.

How can Endian help here?

Endian IoT security gateways are equipped with several security features that can detect and stop cyberattacks: Deep Packet Inspection (DPI) analyzes the data packets sent over a network. Unlike traditional analysis methods that focus only on metadata, DPI performs analysis down to the user level and identifies over 300 IT/OT protocols and 2000 applications. This allows the normal state of the network to be determined. If there is an anomaly in the traffic, it is detected using the Intrusion Detection System (IDS). If it is an attack, the Intrusion Prevention System (IPS) intervenes to stop it.

How can consultants help here?

Consultants help implement suitable processes to establish incident management. This covers the entire incident lifecycle, starting with preventive measures to avoid incidents, through detection and response, to the recovery of systems after an incident. In addition, comprehensive training for employees in IT as well as in the business departments is also advisable.

Business Continuity, Backup Management, Disaster Recovery and Crisis Management

Companies need to take steps to prevent business interruptions that can result from a system failure (for example).

How can Endian help here?

Endian offers several features that can prevent business disruption and data loss. Comprehensive firewall capabilities as well as Deep Packet Inspection (DPI) enable defense against cyber attacks. The high availability (HA) system strengthens resilience by providing an additional EndianOS in standby mode that can immediately take over operations in the event of a system failure. However, if systems are compromised, the backup function enables rapid recovery.

How can consultants help here?

Establishing optimal processes and business procedures is an important point to strengthen resilience. Risks need to be identified and appropriate mitigation measures implemented to ensure business operations remain stable. A business impact analysis is conducted with the company to assess the impact of potential disruptions on operations. The introduction of business continuity management ensures that a company remains capable of acting even in crisis situations.

Secure supply chain

NIS2 also incorporates supply chain and supplier relationship security because comprehensive IT security cannot be established without secure suppliers. With the NIS-2 directive, individual companies are required to address IT security risks in supply chains and supplier relationships.

How can Endian help here?

EndianOS protects networks from security threats coming from external suppliers. The Endian Firewall as well as DPI prevent malware from entering via suppliers and can thus block cyber attacks. Thanks to the integrated virus protection, the networks are also protected against other malware.

How can consultants help here?

The security level of suppliers can be verified via various methods. Targeted reviews and self-assessments ensure that suppliers are taking appropriate security precautions and meeting customer requirements. A structured and efficient management of all documents and contracts is a valuable effort to keep track of the agreements made. Establishing effective document and contract management and the associated processes helps to ensure smooth operations.

Procurement

The NIS-2 directive requires organizations to ensure security in the procurement, development and maintenance of networks and information systems. Vulnerability handling and disclosure are included here. Therefore it becomes even more important to choose reliable suppliers for IT infrastructure and network systems.

How can Endian help here?

Endian develops its products according to the principle of „security by design“, i.e. security is thought about and planned for from the very beginning. The Endian Secure Digital Platform complies with IEC 62443, the standard for industrial cybersecurity. In addition, Endian is an independent, European manufacturer.

How can consultants help here?

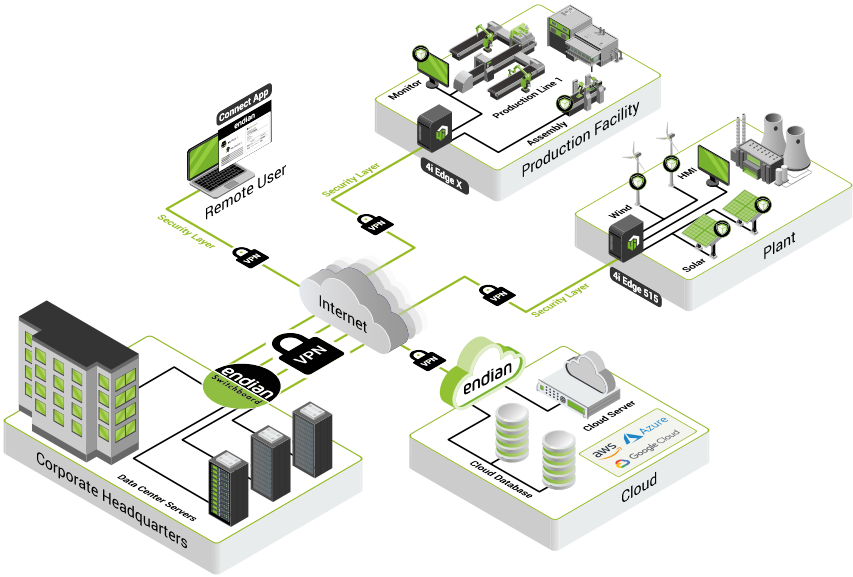
All systems need to be permanently updated in order to be safe from cyberattacks. A structured and well-coordinated approach is important for regularly updating and patching systems, applications and infrastructure. Consultants work with companies to establish effective patch and update management and implement the necessary documentation processes. They also assist in developing policies and processes to ensure that updates are implemented in a timely manner, taking into consideration potential impacts.

Cryptography

The Company shall take appropriate steps to ensure the confidentiality of network communications and data access. This requires developing policies and processes for the use of cryptography and deploying encryption procedures wherever necessary.

How can Endian help here?

Using a Virtual Private Network (VPN), communication on the networks is encrypted. Thanks to the use of modern cryptographic algorithms, data exchange is secured at all times.



How can consultants help here?

Consultants can make a valuable contribution to the development of cryptographic strategies and guidelines for a company's individual requirements. To achieve a high level of security as part of a general security strategy, they can help integrate cryptographic procedures into business processes and IT systems.

Access control

The enterprise defines permissions and roles for access to its infrastructure.

How can Endian help here?

The Endian Switchboard management tool provides very granular roles and permissions management for access to distributed resources according to the Zero Trust Policy. At the same time, it is possible to change rights and authorization in real time.

How can consultants help here?

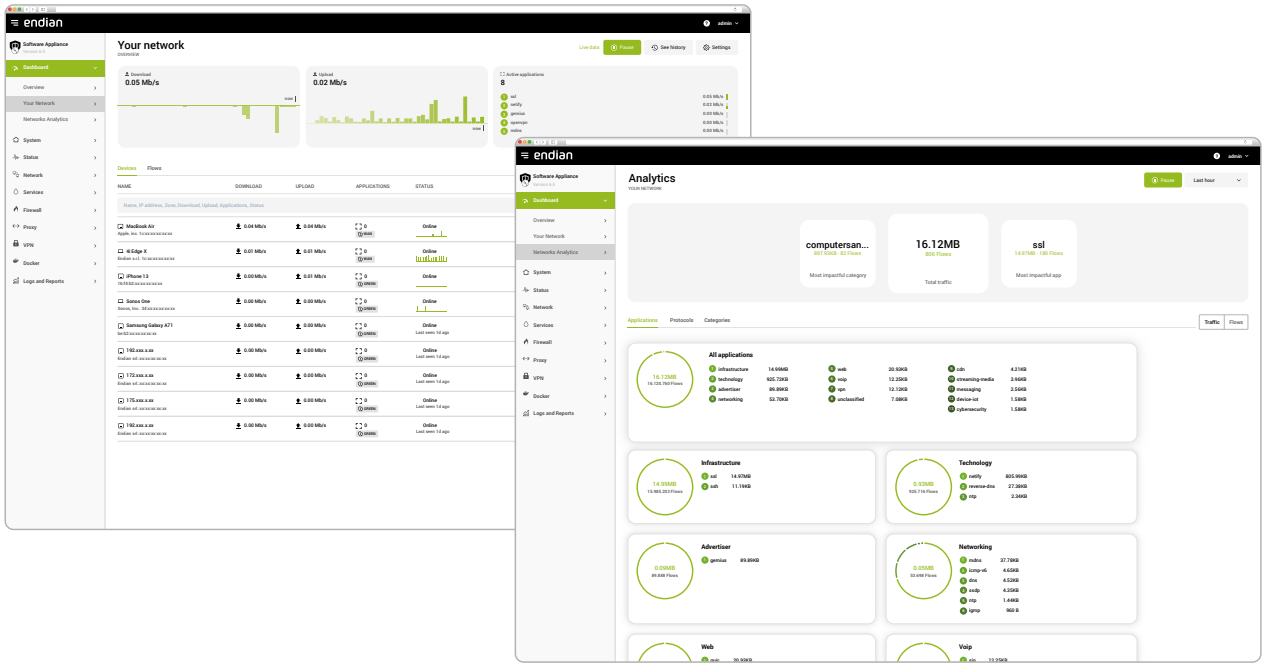
For optimal access management in an organization, authorization strategies and policies need to be designed. Consultants help define clear roles and responsibilities, implement approval processes, and regularly review and update permissions.

Asset Management

The enterprise determines and understands the requirements to ensure essential services in networks and information systems.

How can Endian help?

Endian's Network Awareness solution provides a complete view of IT and OT networks. It shows the assets within the networks and how they are connected to each other, providing the basis for network segmentation.



Authentication

The enterprise takes appropriate measures to authenticate users on its own infrastructure in a secure manner.

How can Endian help here?

Endian provides multi-factor authentication for various services and supports external services, such as Microsoft Active Directory (AD) and Windows New Technology Lan Manager (NTLM). Microsoft users can thus easily authenticate themselves on Endian systems.

Emergency communication

The company defines an emergency communication strategy.

How can Endian help here?

When an emergency occurs, fast action is key. Endian offers an alerting system that automatically sends a notification by mail or SMS as soon as an event occurs, such as a cyberattack or other critical incident. This allows countermeasures to be taken quickly and the incident to be mitigated.

How can consultants help here?

An emergency plan defines clear responsibilities, escalation paths and communication protocols in the event of an emergency. Consultants support the implementation of an emergency plan from the identification of relevant contacts and decision makers to the appropriate communication strategy.

Implementation of NIS-2 Directive: Act now

By October 2024, the EU member states must transpose the NIS-2 regulations into national law. Anyone who is now newly covered by the directive should act quickly. Because consulting, the selection of suitable technologies and their implementation take time.

Endian is happy to advise and support you in implementing the NIS2 directive - feel free to contact us.