use case #13

NIS 2

How to adapt to the new directive NIS 2

advenica

NIS 2

The NIS 2 directive is now published, and the deadline for when organisations in the EU have to adopt the directive is getting closer. In October 2024, the directive will come into force and by then everyone affected must have adapted their operations. Among other things, the updated directive applies to more sectors, has more additions, and involves an increased focus on encryption.

What is the NIS Directive?

The NIS Directive aims to promote security measures and boost EU member states' level of protection of critical infrastructure. In other words, it improves information security of operators in sectors that provide essential services to our society and economy.

What is NIS 2?

The initial NIS directive included a process to conduct regular review of itself. This has led to a new directive for countries in the EU about measures for high common level of cybersecurity – this is called NIS 2. In October 2024, the directive will come into force and by then everyone affected must have adapted their operations. Among other things, the updated directive applies to more sectors and more additions.

Based on these deficiencies, new additions have been made, creating the new NIS 2. These are the most prominent new additions:

- Larger scale than NIS, more sectors considered as essential services (list further down)
- Managers are held responsible for securing operations.
- Incident reporting must now be done within 24 hours instead of 72 hours.
- Higher demands on security and reporting, where a minimum requirement list must be followed
- Security of supply chains and suppliers
- Stricter supervisory measures for national authorities
- Elimination of the distinction between operators of essential services and digital service providers
- Stricter supervisory measures for national authorities, firmer enforcement requirements
- Aims at harmonising sanctions regimes across member states, enabling that administrative fines should be issued. The fine will be up to EUR 10 million or 2% of the business's total worldwide turnover, whichever is higher.
- Enhancement of the role of the Cooperation Group, and increasement of information sharing and cooperation between member state authorities

But how do you follow the NIS 2 directive? We have a number of use cases that suggest some solutions to the issues that the NIS 2 Directive mentions.

Encryption

In NIS 2, there are recommendations on using encryption and cryptography. Encryption is mentioned in Article 21 in the NIS 2 Directive, where it is stated that each organisation should have strategies for cryptography, and when applicable, use encryption. Among other things, encryption and other security related functions (access control, integrity preservation and non-repudiation) can be included in efforts to protect networks and information systems. It is also mentioned that public electronic communication networks and available electronic communication services should use encryption and especially such encryption called end-to-end encryption.

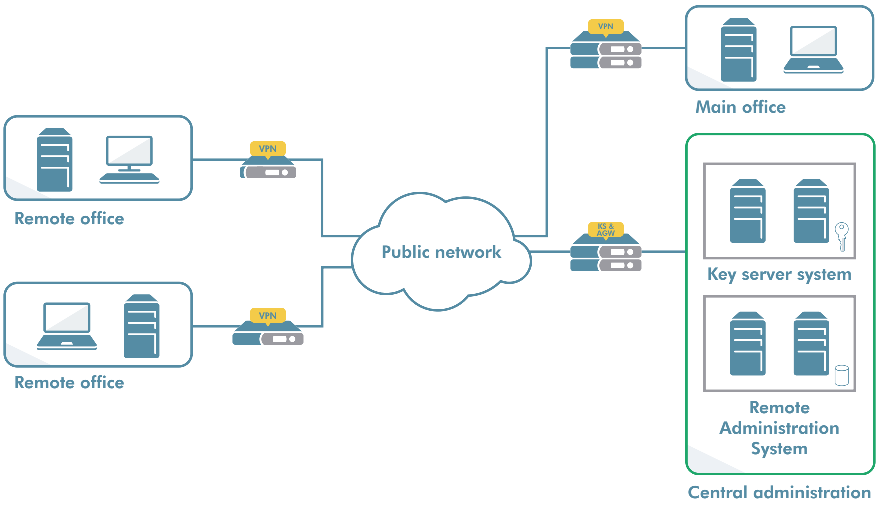
We have a number of use cases as suggestions as to how to use encryption to make your organisation more secure.

Two use cases for encryption

Use Case #1: Secure communication with remote sites

Advenica's SecuriVPN provides sustainable data in motion protection for all end user applications. Optimal deployment is ensured by multiple product models. At the main office, SecuriVPN can be configured to use high availability with failover or dynamic routing. Mobile offices can use the portable SecuriVPN variant. The system supports many features such as NTP, logging and automatic key updates. The system is hardware-based, evaluated and has a central administration system for ease of use.

SecuriVPN is developed and manufactured in-house in Sweden to protect against supply-chain attacks. The system is quantum-secure and holds EU approval for SECRET UE/EU SECRET information exchange.

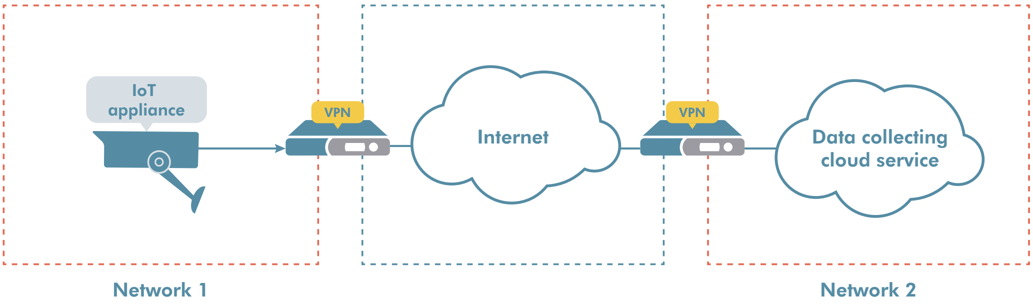


Benefits

- Evaluated by several authorities
- Uses state of the art methods such as key server, PKI and combines symmetric and asymmetric encryption.
- Uses patented three domain separation to ensure proper role separation and privacy.
- Long-term sustainable communication privacy
- Easy to configure and deploy
- Multiple product models for optimal deployment versatility
- Full central logging of system events

Use Case #2: Protection of sensors

The deployment and protection of bandwidth-hungry sensors and more video, data and voice traffic can put pressure on available bandwidth and be expensive. Data protection by encryption comes with a cost of increased traffic escalating the issue. SecuriVPN can be configured to compensate for the low bandwidth and automatically compress all data. It can also be configured to act as unidirectional security gateway, allowing data to travel only in one direction. The devices can operate in harsh environments e.g., operation temperatures 5°C to +40°C.



Benefits

Sustainable data privacy, easy to configure and deploy, unidirectional traffic, full traceability of transferred information.

Network segmentation

Network segmentation is mentioned in one of the reasons for NIS 2 (89) as a necessary and basic cyber hygiene factor, and again (98) to secure electronic communication services and networks. We have gathered a few use cases as to how network segmentation can be used to increase your overall information security and protect your systems and networks.

Three use cases for network segmentation

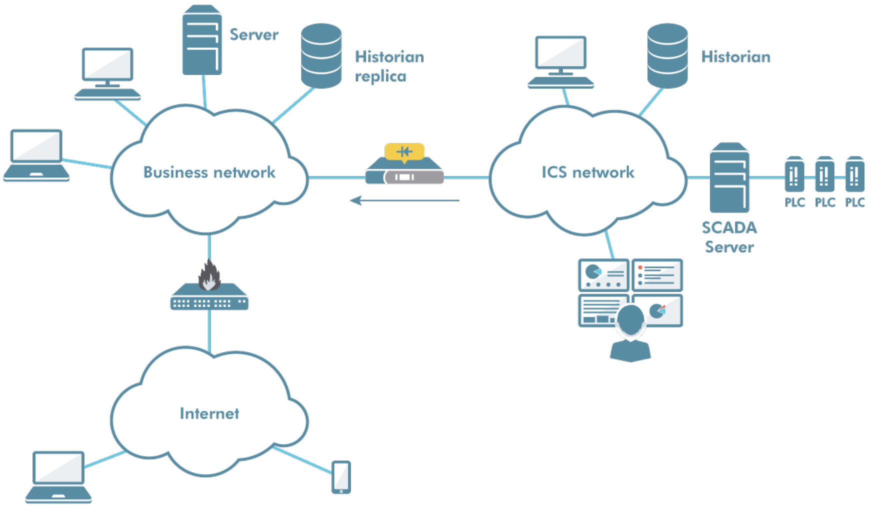
Use Case #1: Secure IT/OT integration

Physical separation of IT and OT using zoning

Separating IT and OT into separate segments helps avoid vulnerabilities or disruption in IT affecting OT. To avoid risks because of mistakes in configuration or function, physical segmentation (zoning) should be used. This means that separate hardware is used for IT and OT.

Use data diodes in the zone border for outbound data flows from OT

The most secure way to connect an integrity sensitive data network to other systems is to use **data diodes**. All data flows from OT that can be managed with data diodes involve a simplified security analysis, quite simply because a data diode is so secure and easy to analyse. Or, more correctly, because it has such high assurance.



Benefits

Using data diodes to protect the collection of log data, you achieve very good protection:

- It is impossible to carry out attacks from the log system on any of the zones.
- You can use a shared log system regardless of the number of zones

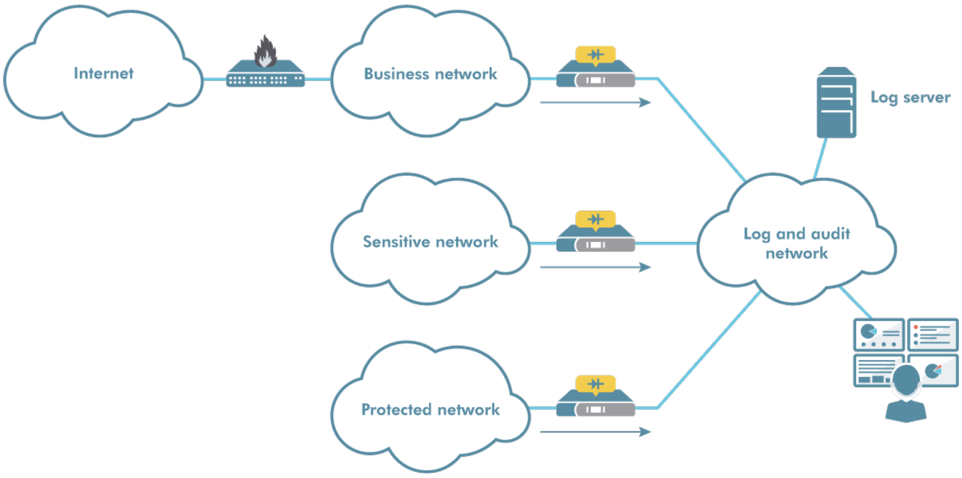
connected. This avoids the additional costs of having to maintain several log systems in parallel.

- You can easily shield and protect the log system so that no unauthorised person can access its contents.
- Data diodes means simplified security analysis (and thus simplified commissioning) and meet extremely strict requirements from bodies such as supervisory authorities.

Use Case #2: Secure logging

All the zones that supply log data are protected with one data diode each. The data flow is made unidirectional towards the log system. A shared log system can therefore be used regardless of the number of zones supplying data to the log system. If any of the zones contains confidential data, either the log system must be protected at the appropriate confidentiality level, or the log data from such a zone must be filtered so that the log system is not contaminated with confidential data. However, this can lead to the value of the log data decreasing as free text data often needs to be filtered out, which may make it more difficult to interpret log data.

- The data diodes make it impossible to use the log system as a stepping stone.
- The data diodes make it easy to protect the log system so that no unauthorised person can access the data.
- It is much more difficult for an attacker to cover their tracks after an attack.
- It is also possible to encrypt the connection to the log server to prevent corruption of log data.



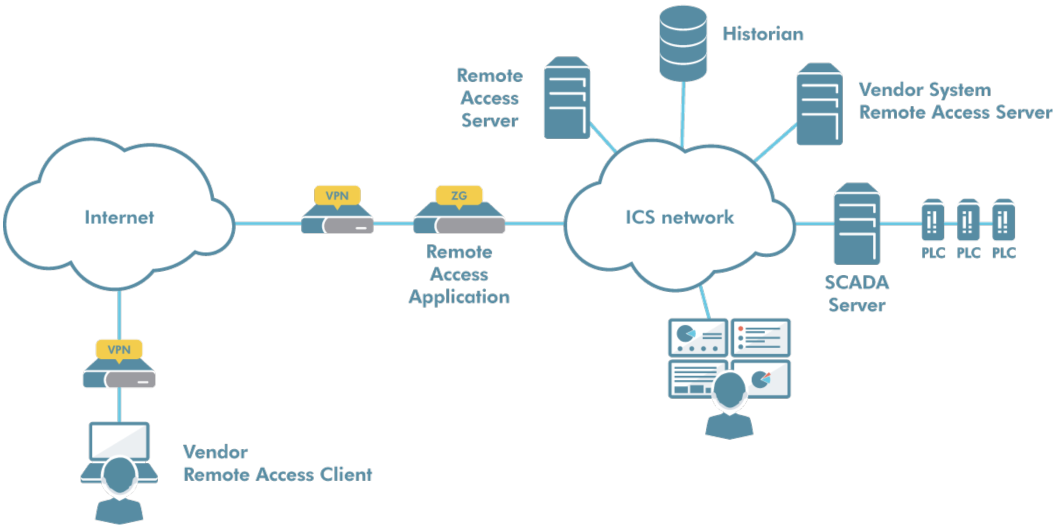
Benefits

By physically zoning IT and OT and using data diodes and **ZoneGuards** in the zone border, you achieve an optimum balance between function and security. Consequently, you can accelerate the digitalisation process without risking the availability of OT, and you also avoid having to spend time and effort on analysing any of the outbound flows from OT.

Choosing data diodes and ZoneGuards gives you a future-proof solution that is considerably less likely to need change over time than a solution based on traditional firewalls and intrusion detection systems.

Use Case #3: Secure Remote Acess

Remote access can be made secure by using RDP and protecting the jump server with an explicit security solution. SecuriCDS ZoneGuard for RDP is such a solution. The connection from the user's PC is established with RDP to ZoneGuard. The user is authenticated and the solution ensures that the connection is to an approved target system at a permitted time. ZoneGuard then ensures that only screen view data may pass from the target system to the user. Only keystrokes and mouse movements are transferred in the other direction. It is also possible to set restrictions, for example that only certain keystroke combinations are permitted. No other information is permitted to pass, eliminating the risks of, for example, general network communication or incorrect configuration of the jump server or its software. This also prevents access to peripheral devices, which would otherwise have meant enhanced risk.


Historian
Remote Access Server
Vendor System Remote Access Server
Internet
VPN
ZG
Remote Access Application
ICS network
SCADA Server
PLC
PLC
PLC
VPN
Vendor Remote Access Client

Benefits

Using RDP and protecting communication with ZoneGuard achieves both security and functionality:

- Only authorised users can use the connection at permitted times.
- The connection can only be made to the systems intended.
- No risk of transfer of malicious code at network level.
- No exposure to peripheral devices.
- Traceability: who did what when?

Want to know about NIS 2? Read our **blog post**!

Interested in our solutions? Read more about our **products and solutions**!

Read our **solution descriptions** to solve your cybersecurity issues!

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

advenica

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED