PacketFront Software

PacketFront Software and NIS2, EU Cybersecurity Directive

Ensure compliance with NIS2

PacketFront Software

Are you ready for EU's new security directive?

In January 2023, the EU introduced an updated Network and Information Systems Directive (NIS2), which all member states were required to have incorporated into their national laws by October 2024. Its aim was to strengthen security requirements, streamline reporting obligations, and introduce stricter supervisory and enforcement measures.

The directive now also affects more sectors, such as providers of public electronic communications networks or services. Fines for violating the directive can reach up to EUR 10 million or 2% of annual revenue.

How does NIS2 impact your organisation?

PacketFront expects that many of our existing customers fall under the NIS2 directive and are therefore required to comply with the stricter cybersecurity regulations.

The directive applies to companies with more than 50 employees and a turnover exceeding 10 MEUR. However, certain entities, such as DNS service providers and those whose services, if disrupted, could significantly impact public safety, are subject to NIS2 regardless of their size.

Another important addition is the accountability NIS2 assigns to the management of organisations. It is now obligatory for management to take responsibility for their organisation's cybersecurity maturity. This includes conducting risk assessments and approving risk treatment plans to be implemented, among other tasks.

So, what measures should affected organisations take today?

Information security policy

Organisations must assess their risk level and evaluate the potential impact of a cyber-attack against their most valuable assets. After identifying vulnerabilities, they need to proactively introduce strong information security policies.

Incident prevention, detection and response

Organisations must develop plans, implement procedures, and train all relevant parties for incident prevention. The directive specifically highlights the following:

- The use of cryptography and encryption.
- The use of multi-factor authentication.
- The security procedures for employees with access to important data, including policies for data access.

Companies should also agree on methods for detecting potential incidents and establish an incident response plan with a clear chain of command for implementation.

Vsaagatan 10
P.O. Box 575
SE-101 31
Stockholm, Sweden

Phone: +46 8 633 19 90 /
+46 8 633 19 90
Email: sales@pfsw.com
Email: info@pfsw.com

www.pfsw.com

Business continuity and crisis management

One of the goals of NIS2 is to ensure that a business can continue its operations in the event of a cyberattack. This means organisations must have a solid plan for how they will react and recover as quickly as possible, minimising any disruption.

Supply chain security

NIS2 requires organisations to consider not only their own vulnerabilities and practices, but also those of their suppliers and service providers. This includes, for example, maintaining close relationships with suppliers and continuously updating security measures to ensure the best possible protection.

Vulnerability disclosure

NIS2 requires transparent vulnerability disclosure and management. For example, if an organisation identifies a vulnerability within its network, it must report it to ensure the issue cannot be exploited elsewhere.

Incident reporting

In the event of a significant incident, organisations must submit an initial report within 24 hours, a full report within 72 hours, and a final report within one month, to the relevant authorities and, where necessary, to affected customers.

Vsaagatan 10
P.O. Box 575
SE-101 31
Stockholm, Sweden

Phone: +46 8 633 19 90 /
+46 8 633 19 90
Email: sales@pfsw.com
Email: info@pfsw.com

www.pfsw.com

PacketFront Software and NIS2

PacketFront Software is dedicated to assisting our customers with NIS2 compliance. Given the comprehensive nature of the directive, support is being rolled out in stages. Fortunately, much of the required functionality is already in place.

Using centralised systems

Using a centralised system for customer, service, and network orchestration increases control and minimises the risk of errors, as less information is handled manually. It is challenging to comply with NIS2 requirements without such systems, due to the lack of control, traceability, and documentation.

Network audits and back-ups

BECS is an intent-based system, meaning it knows the desired state of the network at any given moment. This state can be used as a method to check whether the configuration of a device has been tampered with. For this purpose, PacketFront has implemented functionality that can perform network-wide audits by comparing the actual and desired device configurations and reporting any deviations.

The desired state of the network also serves as a configuration back-up for devices under BECS control. In the case of a cyberattack, the network can be restored either from the online BECS system or, if compromised, from the BECS back-up.

Encryption

Increasing the use of encryption is one of the main objectives of NIS2. Naturally, a large part of the communication is already encrypted using protocols such as SSH and HTTPS. To further enhance internal security, our customers can now encrypt passwords and parameters stored in BECS..

Additionally, communication between Core and Cell servers can be encrypted to further reduce plaintext traffic.

BECS® - OSS Software

BECS is our cutting-edge network orchestration platform designed to streamline the complexities of network management, including those presented in multi-vendor environments. It provides seamless, end-to-end automation for enterprises, Tier 1 carriers, and smaller networks. With BECS organisations can achieve:

- Lower operational costs
- Streamlined network management processes
- Improved work productivity
- Optimised compatibility with UK TSA and EU NIS2 regulations

Vsaagatan 10
P.O. Box 575
SE-101 31
Stockholm, Sweden

Phone: +46 8 633 19 90 /
+46 8 633 19 90
Email: sales@pfsw.com
Email: info@pfsw.com

www.pfsw.com

User access

One of the cornerstones of network security is limiting and monitoring access to BECS and BBE. Both products offer advanced user rights management, helping our customers determine which employees have access to what.

In the latest BBE release and in the upcoming BECS release, we are addressing the next key area: access audits. In other words, who did what, and when?

Vulnerability management

A key part of vulnerability management is the ability to roll out security-related patches as quickly as possible. BECS automates firmware (FW) management and makes it easy to both ensure that the desired FW versions are in use throughout the network and to carry out rapid upgrades when new releases are introduced by suppliers.

PacketFront Software as a supplier

We understand that BECS and BBE are cornerstones of our customers' service delivery. To be regarded as a trustworthy supplier, we are updating our working methods, tools, and documentation to meet NIS2 requirements. This is an ongoing effort that we are fully committed to, as cybersecurity threats continue to grow in sophistication.

PacketFront Software

PacketFront Software and UK Telecom Security Act

PacketFront Software is analysing the effects of the Telecom Security Act (TSA) in close cooperation with several carriers and legal experts.

As a result of this analysis, we have concluded that the functionality already available in the BECS Network Orchestrator fulfils many of the requirements outlined in the Statutory Instruments (SI). However, we also recognise the need to complement this with new features. For example, BECS has a unique capability to store the desired state of all devices under its control.

To fully utilise this for TSA compliance, we have implemented functionality that enables network-wide configuration audits, allowing operators to identify and address any unauthorised changes.

Read more about PacketFront Software and UK TSA by visiting our website:

PacketFront
Software

Learn more about us and our cutting-edge network orchestration solutions by visiting our website:

www.pfsw.com

PacketFront Software

Get compliant:

Contact us for a demo, consultancy or enquiries:

Head office

Street:
Vasagatan 10, 111 20,
Stockholm, Sweden

Postal address:
P.O. Box 575,
SE-101 31, Stockholm

Phone:
+46 8 633 1990

Email:
sales@pfsw.com

UK representatives

Phone:
+44 7718 175 652

Email:
sales-uk@pfsw.com

Poland office

Street:
Jana Pawla II 22,
00-133 Warszawa, Poland

Phone:
+48 22 487 56 25

Email:
office@poland.pfsw.com
info@pfsw.com