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 EU introduced an updated Network and Information Systems (NIS2) directive, which all EU member states must incorporate into their national laws by October 2024. The purpose is to strengthen security requirements, streamline reporting obligations, introduce more stringent supervisory measures and stricter enforcement requirements.

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

How does NIS 2 impact your organisation?

PacketFront expects that many of our existing customers will fall under the NIS2 directive and must thus comply to the stricter cyber security regulations.

The directive will apply to companies with more than 50 employees and a turnover exceeding 10 MEUR. However, certain entities, such as DNS service providers and entities whose services, if disrupted, could have a significant impact on public safety will fall under NIS2 regardless of their size.

Another important addition is the accountability NIS2 assigns to the management of organizations. It will be obligatory for management to take responsibility regarding their cybersecurity maturity. This will include having risk assessments conducted and approving risk treatment plans to be implemented, among other tasks.

So, what measures should the affected organisation take to?

Information security policy

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

Incident prevention, detection and response

Organisations must have plans, implement procedures and train all relevant parties as 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 to detect potential incidents and create an incident response plan with a transparent 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 NIS2 goals 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 soon as possible minimizing any disruption.

Supply chain security

NIS2 requires organisations to consider not only their own, but also their suppliers and service providers vulnerabilities and practices. This means, for example, to maintain a close relationship with suppliers and continually update security to guarantee best possible protection.

Vulnerability disclosure

NIS2 requires transparent vulnerability disclosure and management. This means, for example, that if an organisation identifies a vulnerability within their network, it must disclose it to make sure the vulnerability is not exploited elsewhere.

Incident reporting

In the case of an incident. Organisations must submit an initial report within 24 hours of a 'significant' incident, a full report within 72 hours and final report within a month to authorities and potentially to customers.

PacketFront Software and NIS2

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

Using centralized systems

Using a centralized systems for customer, service and network orchestration increase control and minimize the risk of errors as less information is handled manually. It will be challenging to comply to NIS2 requirements without such systems due to 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 if the configuration of a device has been tampered. For this purpose, PacketFront has implemented functionality that can be used to perform network wide audits by comparing the actual and desired device configurations and report any deviations.

The desired state of the network is at the same time a configuration back-up for devices in BECS control, i.e. in a case of a cyberattack, the network can be restored either from BECS that is on-line, or if compromised, from BECS back-up.

Encryption

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

Also, the communication between Core and Cell servers can be encrypted to further reduce the plain text 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 corner stones of network security is limiting and monitoring access to BECS and BBE. Both products have advanced user rights management helping our customers to decide which employees have access to what. In the latest BBE and coming BECS release we will tackle the next issue, which is access audits, i.e. who did what and when?

Vulnerability management

The big part of the vulnerability management is the capability to roll-out any security related patches as soon as possible. BECS automates FW management and makes it easy to both control that desired FW versions are being used throughout the network and make fast upgrades if new FW releases are introduced by the suppliers.

PacketFront Software as a supplier

We understand that BECS and BBE are cornerstones in our customer's service delivery. To be regarded as a trustworthy supplier we are updating our working methods, tools and documentation to meet NIS2 requirements. This is a continuous work we are fully committed to pursuing as cybersecurity threats get more and more advanced.

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