STORMSHIELD

BUSINESS CASE

Waterworks: secure separation and monitoring of OT networks

PUBLIC

Water and sewage companies belong to a category of public utility and critical infrastructure entities for which uninterrupted operations are of particular importance. It is difficult to imagine a situation in which customers are deprived of access to water.

A specific characteristic of the operations of water and sewage enterprises is the dispersion of their components – they manage water intake and treatment points, as well as sewage pumping stations. The separation of individual parts of the system increases the risk of attack.

In light of the growing scale of cyber threats targeting critical infrastructure, ensuring maximum security remains a key concern for the entities that manage such systems. This is also driven by the implementation of the NIS2 Directive, which impose new obligations on entities in the water and sewage sector.

Water production and sewage collection are processes increasingly reliant on modern technological solutions. The Internet of Things, constant communication between components of overlapping networks – both Internet and industrial – and the use of numerous devices, are now standard in this sector.

"Such a functioning system often requires the application of appropriate safeguards to minimise the risk of hostile actions.

From the perspective of entities responsible for implementing cybersecurity, this is a challenge associated with the need to operate in a way that maintains the continuity of production processes in an industrial environment while ensuring network security and compliance."

Alexander Kostuch
Pre-sales engineer at Stormhield

Appropriate tools

The use of SNi20 devices made it possible to meet numerous industrial and environmental



As part of a security system implemented in one of the operating water utility companies in Poland, the Stormhield and partner teams established a secure and separated IT network environment, along with solutions aimed at protecting operations carried out in OT (operational technology) networks, which operate, among other things, on the basis of programmable logic controllers (PLC).

The client is a company based in one of the largest cities in northern Poland, specialising in water management for the city and surrounding areas, as well as sewage treatment.

It operates across various locations in and around the city, including sewage pumping stations, water treatment plants, and water intake facilities. These sites are equipped with industrial control systems based on programmable logic controllers (PLC) to manage critical processes. Uninterrupted functionality is essential. The convergence of IT and OT networks exposes the organisation to potential cyber threats and risk. Therefore, the primary goal of the project was to establish a secure, monitored, and separated IT network environment, where administrative departments and various domain activities take place, in order to protect specialised industrial operations in OT networks.

Maintaining uninterrupted production processes in an industrial environment, while ensuring network security and compliance, is a challenging endeavour. It is essential to avoid production pump downtimes and minimise network configuration changes.

SOLUTION USED

→ SNI20

The objectives to be achieved

The client wished to implement a robust network security solution that effectively separates and protects OT (operational technology) networks from IT networks across multiple locations, such as pumping stations and water intake points. The implementation period lasted approximately one month. The deployment strategy included the installation of Stormshield SNi20 firewalls at the edges of each OT network. The locations of these firewalls were selected based on a rigorous risk assessment and existing network connections. SNi20 firewalls were placed as close as possible to industrial automation equipment and mounted on the same DIN rail as the PLCs.

This approach facilitates rapid threat detection and response, minimising the attack surface and maximising the protection of industrial infrastructure.

Authorisation of personnel using existing Active Directory mechanisms and integration via the SSO mechanism is of prime importance. All activities within industrial protocols allowed on the devices are then monitored and logged. Events are recorded in a central SIEM system. The entire setup is managed via the management console Stormshield Management Centrer (SMC).

To meet the challenge of uninterrupted implementation within the existing network, Stormshield proposed a solution focused on network segmentation using bridge functionality, while minimising changes to the existing network infrastructure. This approach is based on the use of interface bridging for segmentation, combined with a comprehensive security policy and deep protocol inspection tailored to the specific industrial protocols used in various network segments.

A significant contextual element of the project was also the requirement for compliance with personal data protection regulations. To comply with the General Data Protection Regulation (GDPR), personal data such as usernames, source IP addresses, MAC addresses, and hostnames are not displayed in logs and reports. Instead, this information is anonymised to maintain user privacy. Access to these logs is restricted to authorised personnel, ensuring compliance with data protection legislation.

As part of the implementation, it was also decided to enhance the protection of SCADA systems. In addition to the physical SNi20 edge firewalls, the partner company implemented a virtual firewall directly in front of the SCADA system, which operates in a private cloud running on a large server farm. The Elastic Virtual Appliance (EVA) firewall was deployed on a server platform using HyperV virtualisation, providing an additional layer of protection for Supervisory Control and Data Acquisition (SCADA) systems. This approach ensured that critical infrastructure controlling industrial processes remained protected from potential cyber threats originating both from the Internet and from the internal network.

Network traffic authorisation is performed by verifying access to PLCs. Matching the hardware to the water and sewage industry's specifics involved accounting for various physical constraints (e.g. high humidity, wide temperature range, etc.). The use of SNi20 devices made it possible to meet numerous environmental requirements.

Implementation Outcomes

The preliminary design, detailed design, implementation, as-built documentation, and functional tests were conducted under the supervision, control, and involvement of Stormshield.

The implemented solution successfully achieved the project's main goals in the following areas:

- **Separation:** OT networks were effectively separated from IT networks using SNi20 firewalls, reducing the risk of threats from the internal IT network. Instead of introducing significant changes to the network topology, Stormshield's solution uses interfaces in bridge configuration for segmentation. This technique allows for the isolation of different segments while maintaining the general network structure. This reduces the scope of required modifications, thus minimising the risk of operational disruptions.

- **Centralisation:** each SNi20 firewall in bridge configuration, despite common features, has a custom security policy controlling access to designated resources within a segment. This policy ensures that only authorised devices and entities can interact with critical resources, minimising the potential attack surface. Thanks to the use of the administration platform SMC, variables, and scripting capabilities, all connected SNi20 and EVA firewalls – despite having individual policies in each location – can be centrally managed, reconfigured, and updated with ease.

- **Security:** real-time monitoring via the SIEM system and centralised management of edge firewalls through the SMC facilitate rapid threat detection, response, and reconfiguration.

- **Regulatory Compliance:** the anonymisation of personal data, in accordance with GDPR guidelines, ensure compliance with data privacy regulations.

- **Enhanced SCADA Protection:** the EVA virtual firewall solutions add an extra layer of security to SCADA systems.

- **Reliability:** SNi20 firewalls offer a bypass function, meaning that even during device reboot (e.g. while loading new firmware), data transmission continues

As a result of the implementation, the critical water infrastructure is now protected against potential cyber threats, ensuring the uninterrupted operation of water management and wastewater treatment processes. A comprehensive approach to security – from physical network firewalls to virtual SCADA protection – provides a robust defence mechanism against evolving cyber threats in industrial environments.

Version 1.0 - Copyright Stormshield 2025