STORMSHIELD

INDUSTRY

URBAN AREA WATER BOARD

OPTIMISING CYBERSECURITY TAKING INTO ACCOUNT OPERATIONAL CONSTRAINTS

1.3 million
INHABITANTS

60
MUNICIPALITIES

100
WATER TOWERS

Increasingly interconnected networks

The security of water installations is a major issue for urban areas. The exchange of information becomes permanent between the computer and operational networks. However, this optimisation of infrastructure management increases the attack surface. For example, in March 2016, a hacker targeted a U.S. drinking water plant. Malevolent people had altered the amount of chemicals in the water. More recently, in April 2020, the Israeli government made public a series of cyber-attacks on its water supply and treatment facilities. Israel's cybersecurity agency has instructed all staff of companies operating in the energy and water sectors to change the passwords of all systems connected to the Internet.

The context

The main urban centre, with some sixty municipalities and more than one million inhabitants, of a large French region has launched a call for tenders to streamline the management of its drinking water network. For several years, this water distribution had been managed by three private distribution operators. The aim is now to have only one single operator. In addition to this streamlining of service, the city also wanted to modernise its IT architecture by raising the level of security.

The three existing operators then found themselves in competition to manage the public service of producing, transporting, storing and distributing drinking water over most of the area.

Also, to strengthen the security of its operational networks, the city wanted an architecture that would allow independent protection through the implementation of firewalls:

- the IT office network,
- central VPN hubs,
- industrial and security computing,
- remote sites.

The chosen solution

This call for tenders was won by the leading operator on the French market, who called on Stormshield to assist it in securing this industrial environment.

The main functionalities expected and enabled on this global architecture are the control and filtering of each communication with DPI (mainly the Modbus protocol) as well as the implementation of an IPsec VPN solution to protect communications.

Strong industrial constraints managed via a single solution

The security of the central site has been reinforced by the installation of firewalls between the office network and the business installations. These installations are located on two separate networks (security and industrial), each protected by a cluster of firewalls designed to act as VPN hubs. This architecture interconnects these same applications to the various water towers.

In detail, the operator chose a cluster of SN3100 firewalls to secure the operational and safety network and prevent any interruptions thanks to the dual power supply and RAID disks integrated into this equipment.

Three SN710 firewall clusters were also deployed for the VPN hub area (IT/OT communication). Thanks to customisable interactive reports, the customer has instant access to essential information on network activity and security-related events. The Intrusion Protection System (IPS) is based on several behavioural detection methods and is directly integrated into the core of the products, providing effective protection against zero-day threats while maintaining high-speed performance.

Finally, 100 water towers have been individually equipped with two clusters (one for security and the second for the industrial part) with SNi40 hardened firewalls to secure flows between the different sites and applications. These are specifically designed to protect PLCs (Programmable Logic Controllers) and also allow IPsec VPN tunnels to central sites.

The industrial offer proposed by Stormshield perfectly met the various needs expressed by the operator. In addition, the adaptability of the proposed solution made it possible to manage both standard sites and environments with high industrial constraints (temperature, humidity, DIN rail, industrial power supply). This, with the same firmware deployed across the entire Stormshield Network Security range and a single management console, Stormshield Management Center, to manage the entire fleet of firewalls.

In addition, beyond the functionality/price ratio and independently of standard functions (VPN, segmentation, etc.), the customer was strongly attracted by the IPS functionality of the industrial protocols, with the most advanced granularity on the market and which allows the security of these sensitive systems to evolve as the infrastructures are modernised.

A range of services adapted to complex industrial environments

As concerns maintenance and operations, the customer was confronted with issues of accessibility and sensitivity of certain sites to guarantee service availability to users. To overcome these constraints, Stormshield and the selected operator have implemented an adapted support system, with:

- The implementation of a procedure allowing a technical agent with no network/security skills to replace a failing firewall and return the site to operation with the right level of security,
- An activation of the security mode (bypass) for 5% of sites that are not equipped with a cluster but with just a single firewall. This is to prioritise the availability and safety of the industrial systems over security,
- A range of professional services to support the local area in its process of industrialising the configuration of the initial pilot sites.

The whole of the project and its rollout was successful and on time from end to end thanks to strong involvement and cohesion between the operator and publisher. The end client also greatly appreciated the implementation of the procedures for responding to the business requirements in this industrial environment.

And the relationship continues, since Stormshield has carried out other projects and answered calls for tenders alongside this operator, who also gets in touch internally regarding the modernisation of its activity and adjusting its offering to this IT/OT security environment. As this issue is becoming increasingly vital when we are talking about sensitive and critical infrastructures whose cyber risks could have grave economic, environmental and human consequences.

STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. To find out more: **www.stormshield.com**