STORMSHIELD

BUSINESS CASE

How a hospital group is organising itself to reinforce its cybersecurity

HEALTH

The leading hospital player in its region, with 100,000 professionals and 8 million patients per year, the group faces vital cybersecurity challenges. This sector, which is prey to increasingly frequent and virulent attacks, is structuring itself to better protect its information systems. Here's why.

100,000
Healthcare professionals

39
Hospitals in France

8 million
Patients per year

Aware of the challenges to be met, the hospital group that we are assisting has orchestrated numerous changes to guarantee its security and harmonise the information systems of the six University Hospital Groups.

Focus on network infrastructure

Indeed, all of the connected equipment in each of the hospitals, whether industrial or biomedical (e.g. radio, MRI, pharmaceutical robot, etc.), was on the same network, with little or no security. Some of these devices were controlled by control stations running in Windows XP, Windows 2000 or Windows 7. This is a definite source of vulnerabilities as Windows 2000 and XP operating systems are no longer supported by the publisher since July 2010. These obsolete control stations thus contained significant vulnerabilities, indirectly endangering the PLCs that they controlled.

> ***“We had to partition the flows, protect the control stations and secure the machines so that they only accept legitimate and authorised communications.”***

The objectives to be achieved

In order to implement a proactive security policy and reduce the risk of impact from cyber attacks, Stormshield Network Security firewalls were chosen. Why? The combination of a high level of qualification by the ANSSI and functionalities that meet all the expected specifications.

Stormshield’s proposed solutions include in particular:

→ Resilience of firewalls to conditions outside the data centre(presence of humidity and dust, electromagnetic radiation,extended temperature range, etc.)

→ Ergonomic and easy-to-use centralised administration

→ Ability to monitor and protect PLCs (Programmable Logic Controller) by monitoring certain systems (including the real-time supervisory control and data acquisition system, SCADA)

→ Monitoring and analysis of standard IT protocols

→ Continuity of service in the event of firewall failure through the use ofthe bypass mode.

More than 500% of cyber attacks worldwide aimed at healthcare establishments

Cybersecurity: hospitals on the front line

More than 500% in one year: this is the increase in cyber attacks worldwide targeting healthcare establishments (PwC). This figure is indicative. For a long time, the health sector was spared by cybercriminals, who were more concerned with targeting individuals and companies. This truth begins to change in November 2019, with the attack on the Rouen University Hospital. And it is continuing with the Covid crisis in 2020.

Initially, five SNi40 firewalls were deployed at three sites. The aim of this installation is to partition the flows, protect the control stations and secure the PLCs so that they only accept legitimate communications from authorised equipment.

> ***“The SNi40 firewall,we particularly appreciated the technological breakthrough offered by the bypass Smode as well as the supervision of industrial protocols.”***

In addition, to ensure a single administration of both IT and OT networks, the Stormshield Management Center (SMC) platform has been deployed. Through this solution, all of the hospitals in the group are interconnected centrally and by UHG. Each ISD can access the management of the rules related to its perimeter, without the risk of modifying those of other establishments.

Team testing

To carry out this project successfully, Stormshield’s technical teams performed various tests, which quickly proved positive. This led to implementation of the solutions at the various sites.

THE SOLUTIONS MOBILISED

→ SNi40 FIREWALLS

→ SMC PLATFORM

The next steps

01

INSTALL THIRTY ADDITIONAL SNI40S

Install thirty additional SNi40s to ensure the protection of biomedical single-PLC environments (radio, MRI, pharmaceutical robot, etc.).

02

EXTEND THE DEPLOYMENTS

Extend the deployments to all hospitals grouped in the various University HospitalGroups.

03

SECURE THE EQUIPMENT

Secure the equipment linked to the technicalmanagement of buildings (automatic ventilation, air conditioning, lighting, heating, fire alarms, video protection systems, etc.).

STORMSHIELD