S2 GRUPO

Case study

Comprehensive Cybersecurity Assessment of a Clinic-Hospital

01

Brief presentation of the company:

Our client is an international insurance company that provides medical services in different countries around the world.

Aware of the cybersecurity risks in the healthcare sector, the company commissioned S2 Grupo some time ago to prepare a Corporate Security Guide. With a comprehensive approach, the document brings together information security controls for Communications Networks (IT) as well as for Medical Devices and Building Management Systems (OT).

Distributed in a series of Domains, the document has up to 69 control points for healthcare infrastructures.

02

Problem/challenge

It is proven that in recent years there has been a progressive increase in cybersecurity incidents in clinics and hospitals around the world with leakage of sensitive data, reputational damage and blocking the provision of medical services. With obvious damage to patient safety and the privacy of their personal information.

The company intends to extend this cybersecurity framework to the entire organization. As an immediate practical case, it was decided to perform a complete assessment of one of its infrastructures taking the Corporate Security Guide as a reference document.

Based on the results obtained, it will be possible to have a diagnosis of the real state of one of the organization's facilities, which can be extended to other healthcare infrastructures of the company until a representative sample of the general state is obtained.

03

Action performed

The available documentation of the communications networks, medical devices and facilities of the evaluated infrastructure is compiled and analyzed.

A visit is made to the hospital under evaluation with interviews with the heads of the different departments. In addition, meetings and interviews are held with the heads of suppliers and external companies that support the operation of the clinic's services.

The center has emergency services, hospitalization floors, surgery, ICU, diagnostic imaging, clinical laboratory and complementary auxiliary services.

During the development of these stages our experts can understand the functioning of the different departments and their services. Identifying cybersecurity risks with potential impact on patient safety, with special attention to medical devices and OT systems of the healthcare infrastructure (power supply, air conditioning, security, ...).

In the final stage, a series of technical visibility tests were performed on the different communications networks and the interconnected medical devices.

It was found that the communications networks were not segmented, with IT equipment, radiology and medical imaging devices and OT equipment sharing the same network. Aspects related to credential management, visibility between devices, WiFi network and management with providers could clearly be improved.

The systems in charge of patient information management shared the same infrastructure with the Radiology, Laboratory, medical devices and other facilities in the building.

As a result of the tests carried out, many points were detected that needed to be corrected and improved. They did not comply with the specifications of the Corporate Security Guide. A report was drawn up listing the operations performed, the deficiencies observed and a series of recommended corrective measures.

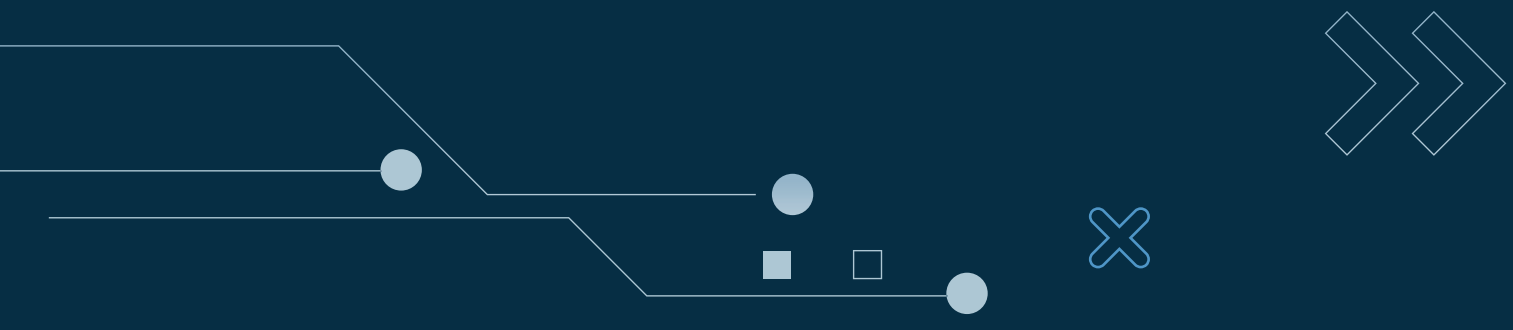
Benefits obtained

With the realization of this project, the client:

1. Will be able to verify the actual state of one of its infrastructures, revealing the deficiencies with respect to the organization's cybersecurity framework.

2. Can correct the problems observed in this facility by adopting the proposed measures and significantly improving the exposure level of this facility. As many as 54 recommended actions were listed, classified as both quick wins and with "high", "medium" and "low" priorities.

3. In addition, from this first assessment in one of their sites, they can extend the measures proposed here to the rest of the organization's facilities. Having noted the presence of these deficiencies allows you to understand where the most critical points of the company's security are located and to easily and immediately identify common problems. It also allows to test the corporate reference document and, if necessary, improve it for future evaluations.



S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLE
SAN SEBASTIAN

SANTIAGO DE CHILE
C.D. MEXICO
BOGOTA
BRUSSELS
LISBON
ROTTERDAM

Follow us: • @s2grupo • s2grupo.es