GRUPO OESÍA:

Protecting the technological infrastructure of the Spanish health sector against advanced cyber threats

Abstract

Grupo Oesía is a 100% private and 100% Spanish high-tech company that has been operating for more than 40 years in the fields of Information Technology and Advanced Engineering in Aeronautics, Security and Defense (through its subsidiary Tecnobit). The main lines of activity of the company are IT consultancy services, Cibersecurity, Digital transformation, e-Solutions for the healthcare sector, and Big Data, among others. Headquartered in Madrid, the company has a factory in Valdepeñas (Ciudad Real) and offices in Spain, Colombia and Perú.

The health sector is a preferred target of attack by cybercriminals, mainly because of the valuable data that is managed in hospitals. A Spanish hospital has taken an interest in securing all its technological infrastructure in order to guarantee the privacy and protection of its patients' data against advanced threats and the new vectors of attacks that arise as a result of the Digital Transformation and the deployment of new technologies, to allow the operational continuity of health services to the Spanish society.

oesia grupo Grupo Oesía

Erasmus+
Key competences for an European model of Industry 4.0
i4EU Project

Learn more about us here:
https://www.i4eu-pro.eu

Co-funded by the Erasmus+ Programme of the European Union

Introduction

The healthcare sector, in general, is involved in a digital transformation process to be more efficient and productive with the resources it has available, and to guarantee its users and patients innovative and quality services to prevent and / or improve their health. This digitization process experienced by hospitals implies the deployment of new technologies and new ways of working that allow patients to receive a better response to their health problems for which they attend the hospital; Also, they seek to provide collaboration capabilities among the medical team by offering immediacy and availability of the patient's medical information so that doctors can investigate and diagnose the patient's medical condition and propose effective treatments.

The cybersecurity team has identified that the massive deployment of new technologies and adoption of new processes in the hospital have expanded the attack domain, since IT elements (servers, computers, printers, etc.); OT equipment (security cameras, access control devices, RFID signal emitters and receivers, etc.); uncontrolled medical IoT devices (ERM scanner, medical beds, light bulbs, patient control consoles, etc.) are not secured or inventoried are added, which produces new vulnerabilities to the hospital network, putting in compromise the patients' health, their data and the operational continuity of the medical service. Proof of this, that since March 1 there have been 13,000 cybersecurity incidents in the health sector in Spain.

Challenges

Taking in consideration that guaranteeing the prevention and / or improvement of the patients' health in the hospital and, consequently, the quality of life of Spanish citizens, with innovative methods that guarantee the effectiveness of treatment and the least possible side effect requires the use of new technologies. Also, the interconnection of all medical devices that can generate the greatest amount of symptomatic information from patients to make it available to doctors, who will give the best possible treatment.

> ***The most complicated part, on a technical level, was to analyze and take action in real time, on the thousands of connected IoT devices in the hospital that were not controlled by us and even unknown to their existence***

Co-funded by the
Erasmus+ Programme
of the European Union

A problem arises for the hospital's security team, who find it necessary to propose a project that guarantees, on the one hand, the much-needed Digital Transformation of the hospital and, on the other, its security.

While connecting IoT devices to the hospital offers clear benefits, it also exposes them to new cyber threats. From infusion pumps, patient monitors, and MRI machines to clinical refrigerators and even wheelchairs, IoT devices are vulnerable and easy to hack. Many of these devices run on patchless software, are poorly configured, or use unsafe communication protocols.

After analyzing the capabilities of the current security systems of the hospital and understanding that, it is only capable of monitoring the data flow of IT networks, a real challenge was posed for the team. Technology capable of understanding the “language” of the IoT, was needed; and, to identify its vulnerabilities and take actions to secure it in real time.

Another challenge that the security team faced was the control of the deployment of these IoT devices, since their purchase, deployment and management had no owner, they are devices “born” for the (medical) business and not conceived as technological devices. Therefore, even when they are connected to the network, they are not in the ICT inventory, the configuration is done by the business (without security knowledge), there is no responsible for maintenance (therefore, vulnerable) and their traffic does not understand IT devices. For the medical service, not having these devices is not an option, therefore effective responses are required.

How will solve the problem?

Grupo Oesia, being conscious that medical care IoT devices are essential for the hospital, and that IT security solutions have become obsolete, with limited visibility and control over IoT devices and their associated risks, proposes a cybersecurity solution for medical IoT devices, based on a managed security service, which guarantees the security of any device connected in the hospital network. The service has technology that prevents IoT-related attacks and continually minimizes IoT areas of attack. Everything done in a way that is easily scalable and non-harmful to critical medical processes.

Co-funded by the
Erasmus+ Programme
of the European Union

The main points intended to be protected:

• IoT vulnerability analysis: the service contemplates continuous scanning of all connected IoT devices, to identify any known or unknown vulnerabilities on the devices.

• Automatic segmentation: minimizes risk exposure with automatically generated IoT policies, which allows the network segmentation and separating IoT devices from the networks where patient information is located.

• Threat prevention: monitors the network in 24x7 format to identify any irregular behavior that may put hospital security at risk and respond to any incident.

The service works as follows:

1.- IoT vulnerability analysis - to expose all hospital risks associated with IoT devices.

The solution performs continuous vulnerability scanning on IoT devices to expose all risks associated with hospital devices at any given time. This analysis is performed from the Grupo Oesia Security Operations Center (SOC), from where you can see all the connected devices classified according to their risk level and even deepen for a risk analysis by device.

The vulnerability analysis on IoT devices is based on three sources:

a. IoT Discovery: By integrating with third-party IoT discovery platforms, the Oesía team identified all connected devices in the hospital, tagged them based on their attributes (e.g. device type, manufacturer, model, firmware version, and MAC address), and analyzed its behavior in real time to detect any anomaly.

b. Firmware Risk Assessment: The idea was to expose the security flaws associated with the firmware of each connected device (and with integrated third-party components) including:

• Weak passwords: credentials easily decrypted by basic force, available from public sources, or cannot be changed.

• Known vulnerabilities: list of all CVEs classified according to their severity and attack vector (physical / network attack).

• Suspicious domains listed

• Encrypted security flaws, such as incorrect operating system settings.

• IoT-Specific Threat Intelligence - The service identifies the latest threat trends from connected IoT devices and looks for malicious patterns through various engines.

Co-funded by the
Erasmus+ Programme
of the European Union

c. IoT-Specific Threat Intelligence: The service identifies the latest threat trends from connected IoT devices and looks for malicious patterns through various engines.

2.- Automatic segmentation – It was intended to minimize the risk exposure of other networks by adopting defined and standardized security policies on the hospital's IoT devices, current and new, these policies are automatically generated.

Based on the vulnerability analysis conducted, the best practices in the market, the experience of our team and the hospital's security policies, the technology automatically generates and applies the policies for each IoT device connected to the hospital, for both; those that are already connected, and the new devices that were being deployed in the hospital.

Some examples of policies that were configured:

- Prevent medical imaging devices from communicating with nursing workstations.
- Prevent high-risk devices (eg, MRI, CT) from communicating using insecure protocols (eg, HTTP).

3.- Threat prevention - The objective of this point was to block attacks directed at IoT devices.

Our technology was monitored from the SOC of Oesía where the team of expert professionals analyzed all the connected devices in order to detect any irregular behavior and to be able to identify security incidents to act on them.

Co-funded by the
Erasmus+ Programme
of the European Union

References

- Reference 1 https://ciberseguridad.oesia.com
- Reference2 http://grupooesia.com/
- Reference3https://www.elespanol.com/omicrono/20200503/ciberdelincuencia-ceba-espana-coronavirus/487201459_0.html
- Reference4https://www.interempresas.net/TIC/Articulos/262175-Ciberseguridad-en-la-sanidad-conectada-2020.html
- Reference5https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/2-uncategorised/6429-encuentro-ciberseguridad-sector-salud.html
- Reference6https://apisa.com.es/wp-content/uploads/2018/05/Seguridad-IoT-en-Sanidad-Estamos-Preparados.pdf

This showcase has been collected in the framework of the Erasmus+ project Key competences for an European model of Industry 4.0 (pr. n° 2019-1-FR01-KA202-062965), funded by European Commission.
For more information: www.i4eu-pro.euLegal notice: This publication / communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.