Case Study

Cybersecurity of a Smart City

01

Context

More than 80% of the world's population lives in cities. Citizens demand more and more quality services: energy and water supply, public lighting, urban mobility, waste collection, sanitation, leisure and tourism, purchase of clothes and food, ….

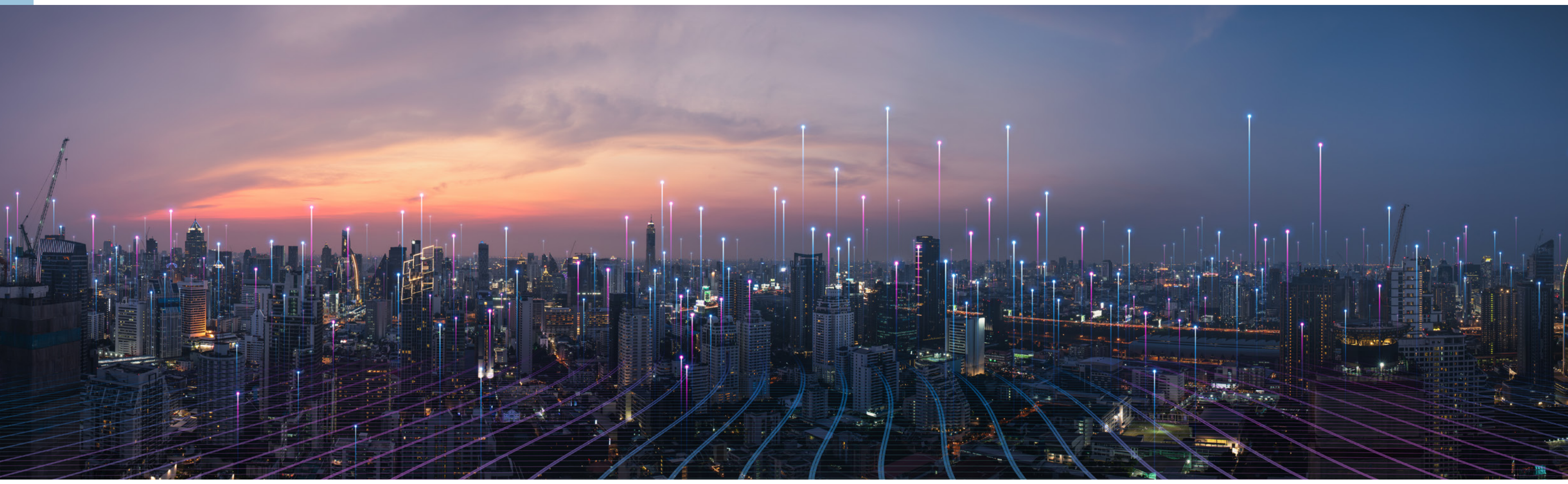
The providers of these services have also been incorporating **digitization into their business processes.** In this way, the quality of the services is considerably improved and both the citizen and the infrastructure managers have information in real time and **can optimize their time and public resources.**

All the big capitals are evolving towards the **smart city model.** With the incorporation of distributed IoT sensors and actuators, citizen interaction apps and a wide variety of applications working interconnectedly on communication platforms.

Aware of the risks posed by this wide range of digital devices distributed throughout our cities, our client, **one of the main capitals of the country,** commissioned us to **assess the level of security** of its urban infrastructures.

03

Problem/challenge



Description of the problem/challenge

The usual architecture consists of a wide variety of sensors and actuators distributed throughout the city. Individually or grouped by zones, the devices communicate with the city control center.

These are microphones that measure the noise level, CO x and NO x level meters, light sensors, vehicle number counters, traffic control cameras, garbage container fill level detectors, filling stations, electric vehicle charging, regulated parking payment cabinets and a wide variety of devices of all kinds.

All installed on public roads, of different types and configurations, sending and receiving data to the control center wirelessly or with a cable or fiber connection. It is not possible to guarantee 100% that they are not accessible and that they can be manipulated. Or they can be used as a gateway to the rest of the platform.

Action carried out

Description of the action carried out

Accompanied by the client's technical staff, our experts carried out a series of inspection visits to different "type" elements. It was necessary **to understand how each analyzed system worked,** how it was connected to the control center, if the devices were accessible to a greater or lesser extent...

The security conditions of different devices in the S2 Grupo industrial laboratory were evaluated: OS, communication protocols, ports, default passwords, encryption capacity, user access, etc. By performing an intrusion test. As well as other procedural and organizational vulnerabilities in the work methods used.

In the case of unauthorized external access, what degree of visibility and what capacity for interaction would an intruder have: could he access the rest of the devices in that installation? Could the operation of that infrastructure be modified? And the rest of the facilities?

As a result of the assessment, **a complete report** was prepared describing the set of actions carried out, the vulnerabilities detected and a series of proposals, of different degrees of complexity, that would improve the general state of the platform's security.

Benefits Obtained

With a series of objectives achieved:

1 Our client has a **vision of the general security status** of their systems: vulnerabilities and the corresponding degree of risk.

2 Identifies its **organizational shortcomings:** the procedures and measures that should be implemented, their complexity, estimated cost and expected scope.

3 Depending on the cost and complexity, **you can plan the next steps** to improve the security of your smart city facilities.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
BRUSELAS
LISBOA
RÓTERDAM

Síguenos en: ● @s2grupo ● s2grupo.es