S2 GRUPO

Caso de éxito

Ciberseguridad de una Smart City

01

Contexto

Más del 80 % de la población mundial vive en ciudades. Los ciudadanos demandan cada vez más servicios y de más calidad: suministro de energía y agua, alumbrado público, movilidad urbana, recogida de residuos, saneamiento, ocio y turismo, compra de ropa y alimentos, ….

Los proveedores de estos servicios también vienen incorporando la digitalización en sus procesos de negocio. De este modo se mejora considerablemente la calidad de los servicios y tanto el ciudadano como los gestores de las infraestructuras disponen de información en tiempo real y pueden optimizar su tiempo y los recursos públicos.

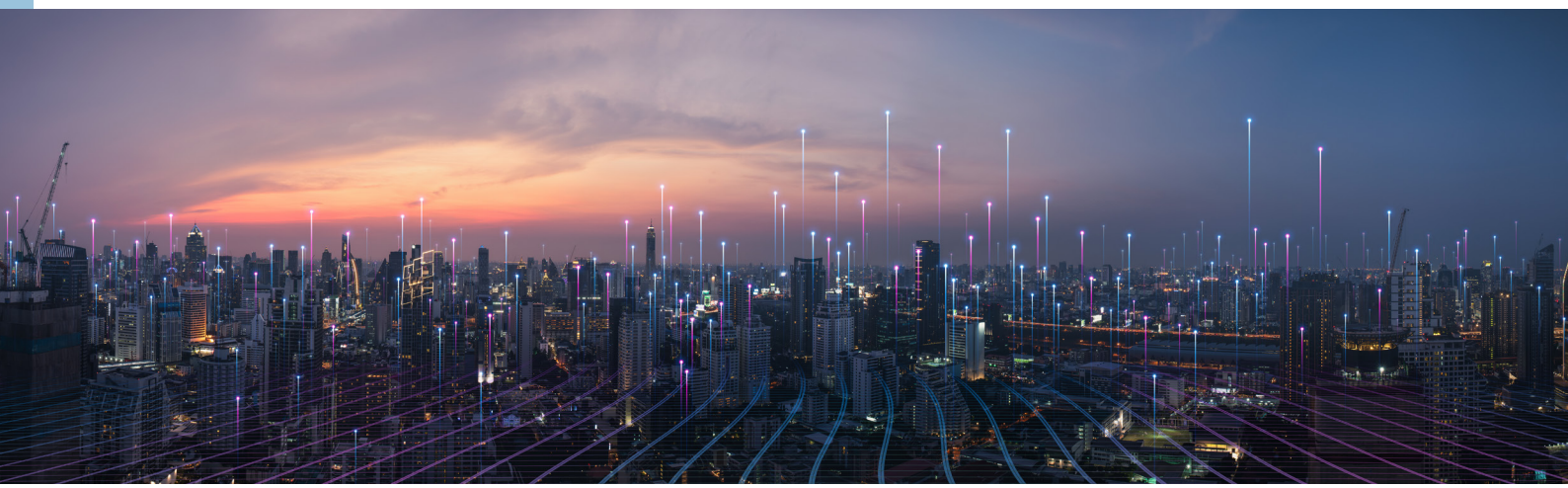
Todas las grandes capitales están evolucionando hacia el modelo de ciudad inteligente. Con la incorporación de sensores y actuadores IoT distribuidos, apps de interacción con el ciudadano y una amplia variedad de aplicaciones trabajando de forma interconectada en plataformas de comunicaciones.

-. Consciente de los riesgos que plantea esta amplia serie de dispositivos digitales distribuidos por nuestras ciudades, nuestro cliente, una de las principales capitales del país, nos encarga una evaluación del nivel de seguridad de sus infraestructuras urbanas.

Caso de éxito: Smart City

03

Problemática/reto



Descripción de la problemática/reto

La arquitectura habitual consiste en una amplia variedad de sensores y actuadores distribuidos por toda la ciudad. De forma individual o agrupados por zonas los dispositivos se comunican con el centro de control de la ciudad.

Se trata de micrófonos que miden el nivel de ruido, medidores del nivel de COx y NOx, sensores de luz, contadores del número de vehículos, cámaras de control de tráfico, detectores del nivel de llenado de los contenedores de basura, estaciones de carga de vehículos eléctricos, armarios de pago de estacionamiento regulado y toda una amplia variedad de dispositivos de todo tipo.

Todos instalados en la vía pública, de diferentes tipos y configuraciones, enviando y recibiendo datos al centro de control de forma inalámbrica o con conexión de cable o fibra. No es posible garantizar al 100 % que no son accesibles y que pueden ser manipulados. O pueden ser utilizados como vía de acceso al resto de la plataforma.

04

Actuación realizada

Descripción de la actuación realizada

Acompañados por el personal técnico del cliente, nuestros expertos realizaron una serie de visitas de inspección a diferentes elementos “tipo”. Era necesario **comprender cómo funcionaba cada sistema analizado,** como se conectaba al centro de control, si los dispositivos eran accesibles en mayor o menor medida...

Se **evaluaron las condiciones de seguridad** de diferentes dispositivos en el laboratorio industrial de S2 Grupo: SO, protocolos de comunicaciones, puertos, passwords por defecto, capacidad de cifrado, acceso de usuarios, etc. Con la realización de un test de intrusión. Así como otras vulnerabilidades procedimentales y organizativas en los métodos de trabajo empleados.

En el caso de acceso externo no autorizado qué grado de visibilidad y qué capacidad de interacción tendría un intruso: ¿podría acceder al resto de los dispositivos de esa instalación?, ¿se podría modificar el funcionamiento de esa infraestructura? ¿y el resto de instalaciones?

Cómo resultado del assessment se elaboró un **informe completo** describiendo el conjunto de actuaciones realizadas, las vulnerabilidades detectadas y una serie de propuestas, de diferente grado de complejidad, que permitirían mejorar el estado general de la seguridad de la plataforma.

Beneficios obtenidos

Con una serie de objetivos conseguidos:

1. Nuestro cliente dispone de una visión del estado general de seguridad de sus sistemas: vulnerabilidades y el grados de riesgo correspondiente.

2. Identifica sus carencias organizativas: los procedimientos y medidas que debería de implementar, su complejidad, coste estimado y alcance previsto.

3. En función del coste y complejidad puede planificar los siguientes pasos para mejorar la seguridad de las instalaciones de su ciudad inteligente.

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