Publicado en Madrid el 28/10/2021

Los sistemas informáticos del sector ferroviario, en el punto de mira de los cibercriminales

Según el último estudio realizado por S2 Grupo, sobre la ciberseguridad del sector ferroviario, se extrae que una de las consecuencias de un ciberataque a esta industria podría afectar a sus sistemas OT (tecnología de las operaciones). Estos sistemas "se han convertido en un blanco muy apetecible para los ciberatacantes" ya que son elementos críticos

Según indica en un comunicado la compañía especializada en ciberseguridad S2 Grupo, en el caso de que los sistemas OT se vieran afectados se podrían "interrumpir las operaciones perjudicando a la continuidad de un servicio esencial como es el transporte". En este sentido, la empresa española señala que la irrupción de las tecnologías de la información y la comunicación en el sector ferroviario han generado nuevas amenazas de seguridad a los sistemas de control industrial (ICS) esenciales para su funcionamiento.

"En todos los procesos que componen el sistema de transporte ferroviario, desde la operación de la infraestructura ferroviaria, la explotación de vehículos para el transporte de personas o mercancías, o la propia construcción de material ferroviario, se han introducido nuevas tecnologías para trabajar de una forma más eficiente. Y junto a ello, inevitablemente, se han incrementado los riesgos de ser víctimas de la ciberdelincuencia", ha explicado José Rosell, socio-director de S2 Grupo.

"Entre aquellos que pueden estar interesados en atacar este tipo de infraestructuras se encuentran no sólo grupos terroristas o grupos patrocinados por estados, sino también delincuentes interesados en el fraude económico. Organizaciones criminales, delincuentes de todo el mundo e incluso muchos ciudadanos son conscientes de las debilidades existentes en los ICS y del daño que pueden causar a una organización o al conjunto de la sociedad afectando a servicios esenciales", ha añadido Miguel A. Juan, socio-director de S2 Grupo.

S2 Grupo destaca que algunas de las consecuencias de un ciberataque a las infraestructuras que forman el sector ferroviario "podrían conllevar daños físicos, ya sea un impacto directo en las usuarios de los sistemas ferroviarios o un daño a las infraestructuras con un impacto indirecto en la población (pérdida de servicios esenciales)". Por ello, el sector del transporte es considerado como un sector estratégico por la Ley de Protección de Infraestructuras Críticas (LPIC).

Otras consecuencias podrían causar perjuicios a las compañías en forma de pérdidas económicas, daños reputacionales, daños al medio ambiente, a la Administración, a las personas, afectar al recorrido de un vehículo llegando a provocar un accidente ferroviario, daños a la sociedad por falta de servicios esenciales.

Tecnología y ciberriesgos en el sector ferroviario

En el sector ferroviario se han introducido nuevos elementos para la conexión remota con los vehículos

para tareas de telemetría, mantenimiento y gestión de flotas, o la introducción de sistemas de entretenimiento para pasajeros dentro del propio vehículo, entre otros. Todo esto hace que "un vehículo esté continuamente comunicándose con el exterior, intercambiando información con otros componentes del sistema de transporte; lo que unido a la complejidad asociada a la coordinación de múltiples participantes (fabricantes de componentes, constructores, operadores, gestores de infraestructuras, etc.), introduce nuevos riesgos", señala el comunicado de S2 Grupo.

Algunos de estos problemas de ciberseguridad en el sector ferroviario son:

Falta de seguridad en el diseño de los sistemas – Desde S2 Grupo se ha insistido en que se debe contemplar la ciberseguridad de los sistemas con una visión integrada IT/OT desde la fase de diseño. Esto permite obtener mejores resultados en la protección de los mismos y reducir significativamente los costes. Cuando las medidas de seguridad se implantan a posteriori, se limita su efectividad

La publicación en RRSS y otros entornos online de la descripción de ciertas infraestructuras o vehículos ferroviarios que pueden contener información sensible y, por tanto, exponerlos ante los ciberdelincuentes.

La eliminación de los equipos que sean sustituidos debe hacerse de forma segura, porque también podrían contener información sensible como en el caso de las memorias.

La conexión continua de los vehículos con el exterior.

El uso de sistemas operativos como Windows en sus ICS y la mala segmentación de sus redes IT y OY.

Datos de contacto:
Nuñez Canal
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Logística Ciberseguridad Otras Industrias