Embarque hacia un transporte público seguro. ¡Atentos a la brecha!

ENISA propone directrices para proteger los activos críticos y el intercambio de datos para el Transporte Público Inteligente en ciudades inteligentes.

En las ciudades inteligentes, el Transporte Público Inteligente (IPT, por sus siglas en inglés) depende del IoT y de sistemas ciberfísicos para recuperar, procesar e intercambiar datos. Estas tecnologías conllevan mejoras en el servicio y la calidad de vida de los ciudadanos.

Sin embargo, con estas nuevas tecnologías también han surgido amenazas cibernéticas. Recientemente, un sistema de transporte fue interrumpido durante varios días debido a interferencias con los sistemas de telecomunicaciones; un servicio de metro sufrió cortes de suministro eléctrico por fallos en los servidores centrales; también se han pirateado tickets inteligentes para realizar acciones fraudulentas. Estas amenazas tienen un impacto económico y posibles consecuencias en la salud y la seguridad de los ciudadanos.

Los municipios y operadores del IPT están empezando a aceptar gradualmente las consecuencias de las amenazas cibernéticas. Las limitaciones actuales incluyen la falta de gobernanza corporativa para la seguridad IPT e inversiones asociadas; dificultades para integrar la seguridad en los sistemas de protección, ya que la ciberseguridad en el IPT sigue sin estar clara; así como la falta de un enfoque común de la UE respecto a la seguridad en el transporte público inteligente.

ENISA ha elaborado dos estudios para sensibilizar y facilitar soluciones prácticas para mejorar la seguridad cibernética. En este sentido, ENISA propone varias recomendaciones claves:

- La Comisión Europea y los Estados miembros deben fomentar el intercambio de conocimientos y la colaboración en seguridad cibernética entre industria, Estados miembros y municipios
- Los operadores IPT deben integrar la seguridad cibernética en su gobernanza corporativa
- Los operadores IPT deben definir claramente sus requerimientos de seguridad
- Los fabricantes y proveedores de soluciones deben crear productos y soluciones que cumplan los requisitos de ciberseguridad de los usuarios finales de IPT

Prof. Udo Helmbrecht** , **Director Ejecutivo de ENISA, comentó: «Las infraestructuras y los dispositivos inteligentes ya no son una cosa del futuro; hoy en día se utilizan en toda la UE. ENISA considera la seguridad de estas infraestructuras un factor clave para lograr el éxito. Garantizar la protección adecuada de los ciudadanos eliminará las barreras para su implementación y ayudará a promover el crecimiento económico mediante la innovación».

Mientras las ciudades inteligentes siguen creciendo en importancia, ENISA responde con dos guías que contienen buenas prácticas 1) para proteger los activos críticos de un sistema IPT y 2) para asegurar intercambios de datos entre un operador IPT y otros interesados en ciudades inteligentes y conectadas.

El informe completo se puede leer aquí:

Security and Resilience of Intelligent transportation systems
Cyber security for Smart Cities: An architecture model for public transport

(Seguridad y resiliencia de los sistemas inteligentes de transporte
Ciberseguridad para las ciudades inteligentes: un modelo de arquitectura para el transporte público)

Información técnica:
Dr. Cédric Lévy-Bencheton, experto en seguridad de las redes y de la información (NIS), cedric.levy-bencheton@enisa.europa.eu

Para entrevistas y consultas relacionadas con la prensa, póngase en contacto con **press@enisa.europa.eu , Tel.** +30 2814 409576