30/01/2014

EPR08/2014
www.enisa.europa.eu

Energía: en su nuevo informe, la agencia europea de ciberseguridad afirma que la ciberseguridad es fundamental para proteger contra las amenazas a las redes inteligentes, las cuales son elementos clave de la disponibilidad energética.

ENISA, la agencia de ciberseguridad de la UE, señala que la evaluación de las amenazas contra las redes inteligentes es crucial para su protección y, por consiguiente, un elemento fundamental para garantizar la disponibilidad de la energía.

Las redes inteligentes son complejos "sistemas de sistemas" que almacenan, transportan y gestionan la energía desde su punto de producción hasta los consumidores. En la práctica, una red inteligente es una infraestructura crítica, puesto que la energía es un elemento crucial para la sociedad y para el buen funcionamiento de la economía. El hecho de combinar infraestructuras energéticas e informáticas convierte a las redes inteligentes en infraestructuras críticas que deben funcionar de forma segura, respetando la privacidad de los usuarios finales.

El profesor Udo Helmbrecht, Director Ejecutivo de ENISA, comentó: "*Es indispensable comprender el panorama de las ciberamenazas a fin de identificar las medidas de protección necesarias para las redes inteligentes. Este informe responde a una apremiante necesidad de los proveedores de energía y los demás actores implicados: proporciona herramientas para evaluar la exposición a riesgos de los equipos de las redes inteligentes. En materia de ciberseguridad, el esfuerzo conjunto y la coordinación son imprescindibles para reducir los daños*".

Este informe muestra un panorama de las amenazas que afectan a los componentes de las redes inteligentes. También ofrece un compendio de las posibles estrategias de ciberseguridad y protección, así como de las buenas prácticas en este campo. Por último, el estudio describe las amenazas internas que afectan a los equipos informáticos de las redes inteligentes, incluidas varias amenazas originadas por errores y ataques internos.

Conclusiones principales. Del estudio se desprenden las siguientes conclusiones principales:

- *Tener en cuenta las amenazas tanto internas como externas*: en materia de ciberseguridad, las ciberamenazas externas constituyen la principal fuente de exposición externa. Este conjunto de ciberamenazas tiene su origen en agentes amenazantes que utilizan ciberamenazas y lanzan ciberataques.

- *Desglosar y clasificar los elementos de las redes inteligentes expuestos a amenazas*: desde los equipos eléctricos, como cables, interruptores, enrutadores y sensores, hasta los datos, pasando por el software, los sistemas operativos, los servicios, el hardware, las infraestructuras y las personas responsables del funcionamiento de los sistemas.
- *Utilizar los conocimientos disponibles*: reutilizar las buenas prácticas existentes una vez establecido el nivel de protección deseado.
- *Recopilar las **amenazas específicas de las redes inteligentes**, como, por ejemplo:*
    - *Escuchas/intercepciones/piratería: filtraciones de información, intercepción de frecuencias electromagnéticas/radiofónicas, ataques con rastreadores, errores de servicios y sistemas, ciberataques y ataques físicos, etc.*
      *y los **agentes amenazantes**, como empresas, cibercriminales, empleados, hackers, estados, desastres naturales, terroristas y todas las nuevas formas de ciberactivistas.*
- *Evaluar las vulnerabilidades y los riesgos existentes en las redes inteligentes.*
- *Evaluaciones por parte de los propietarios de los equipos*: la Agencia afirma que, en última instancia, la evaluación de la exposición a amenazas y los riesgos de una red inteligente solo puede llevarla a cabo el propietario de los equipos, ya que es él quien domina la complejidad y la interdependencia de la infraestructuras de la red inteligente en cuestión.

Informe completo

Contexto: Informes de ENISA sobre Redes inteligentes (Diciembre de 2012); 10 recomendaciones (Julio de 2012)
Estrategia de ciberseguridad de la UE, propuesta de Directiva de la UE sobre Ciberseguridad

Entrevistas: Ulf Bergström, portavoz, ulf.bergstrom@enisa.europa.eu, móvil: + 30 6948 460 143, o Dr. Louis Marinos, experto de ENISA, resilience@enisa.europa.eu

Traducción. La versión original en inglés es el documento auténtico.
www.enisa.europa.eu