19/12/2014

EPR20/2014

www.enisa.europa.eu

Certificación de seguridad de las redes inteligentes en Europa: retos y recomendaciones

ENISA publica hoy un informe sobre la *Certificación de seguridad de las redes inteligentes en Europa*, destinado a los Estados miembros (EM), la Comisión, los órganos de certificación y el sector privado. El informe contiene información sobre varios métodos de certificación existentes en la UE y otros Estados miembros y países de la AELC. En concreto, describe la situación europea y analiza las ventajas y las dificultades que implicarían unas prácticas de certificación más armonizadas.

El informe intenta atraer el interés de los expertos en redes inteligentes y recibir el apoyo de las autoridades de certificación sobre cuestiones pendientes en materia de certificación de la seguridad en entornos de redes inteligentes. La creciente necesidad de contar con una certificación para redes inteligentes se deriva de la falta de control sobre la cadena de suministro energético (cables, paneles solares, turbinas eólicas, etc.) que ha provocado la automatización de la red inteligente.

Udo Helmbrecht comentó acerca de este proyecto: "*Las energías renovables y las redes inteligentes resultan muy prometedoras para la industria europea, y la certificación de seguridad es un instrumento de gran importancia para incrementar la confianza de los usuarios en la cadena de suministro energético. En este informe, ENISA ofrece recomendaciones que animan a las autoridades de certificación a transponer sus requisitos de seguridad nacional y, al mismo tiempo, allanan el camino hacia una mejor armonización de las prácticas europeas en materia de certificación de redes inteligentes*".

En este contexto, ENISA ofrece estas *diez* recomendaciones a los Estados miembros y a la Comisión Europea:

1. La Comisión Europea debería nombrar un comité directivo europeo para coordinar las actividades de certificación de las redes inteligentes.
2. El comité directivo europeo debería facilitar directrices y un modelo de referencia para instaurar una cadena de confianza.
3. El comité directivo europeo debería llevar a cabo un ejercicio de recopilación de todas las normativas y los programas existentes en la UE.
4. El comité directivo europeo debería fomentar el reconocimiento internacional de programas como SOG-IS.
5. El comité directivo europeo debería fomentar una validación proporcional a la aceptación del riesgo que implica cada caso de uso de las redes inteligentes.
6. El comité directivo europeo debería facilitar la flexibilidad en la actualización de los perfiles de protección, a fin de adaptarlos al cambiante panorama de las amenazas a la seguridad.
7. Los Estados miembros deberían utilizar los perfiles nacionales como especificaciones detalladas de las normativas internacionales, con el fin de cubrir los casos de uso específicos a nivel nacional, así como los métodos y pruebas de certificación aplicados localmente.

8. La Comisión Europea debería solicitar a los comités técnicos, en colaboración con las asociaciones energéticas europeas, la creación de perfiles europeos.
9. El comité directivo europeo debería facilitar herramientas acordes con el marco de certificación propuesto, mientras que los comités técnicos nacionales deberían facilitar herramientas preevaluativas para programas específicos.
10. La Comisión Europea y los Estados miembros deberían promover el cumplimiento y la armonización como ventajas económicas y como una medida de reducción de costes.

El informe está basado en las conclusiones a las que se llegaron en el taller sobre certificación de seguridad de los componentes de las redes inteligentes celebrado en Bruselas en 2012 y organizado por ENISA en colaboración con la Dirección General de Redes de Comunicación, Contenido y Tecnologías (CONNECT). El mensaje clave es que Europa necesita unas prácticas de certificación de seguridad de redes inteligentes más armonizadas para permitir una reducción de los costes de certificación. El informe también es el resultado de las consultas realizadas a expertos en certificación de seguridad de redes inteligentes, y fue validado por expertos en seguridad en un taller celebrado en Heidelberg en septiembre de 2014.

Informe completo: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification/

Consultas: Dr. Konstantinos Moulinos, Agente de Seguridad y Resiliencia de Redes de Comunicación, ENISA, **Correo electrónico:** Konstantinos.Moulinos@enisa.europa.eu, **Teléfono:** +30 2814409629.