23/01/2014

EPR07/2014
www.enisa.europa.eu

Según ENISA, la agencia de ciberseguridad de la UE, los sistemas de control industrial de la energía, el agua y el transporte anticuados y desprovistos de los suficientes controles de ciberseguridad deberían someterse a pruebas de capacidad coordinadas a nivel europeo.

La agencia europea de ciberseguridad ENISA publica hoy un nuevo informe con recomendaciones sobre los nuevos pasos a adoptar con relación a la realización de pruebas de capacidad coordinadas en los a menudo anticuados sistemas de control industrial (ICS, por sus siglas en inglés) de las industrias europeas. De estas recomendaciones se desprende la necesidad de convertir la realización de pruebas en los ICS en una preocupación para todos los Estados miembros de la UE, si bien, según ENISA, es algo que podría abordarse a nivel europeo.

Hoy en día, los sistemas de control industrial (por ejemplo, SCADA) de la energía, el agua y el transporte utilizan ampliamente tecnologías de la información (TI). Las TI mejoran la eficiencia, reducen costes y permiten la automatización de los procesos. Por desgracia, dicha utilización suele acompañarse de una planificación deficiente y de una gran falta de información y de configuraciones de seguridad, además de implicar la incorporación desde el "día cero" en los sistemas ICS/SCADA de vulnerabilidades conocidas o nuevas, sin descubrir o sin parchear.
Los sistemas ICS pueden tener una vida útil de más de 20 años, lo que significa que, tradicionalmente, fueron diseñados como sistemas independientes y desprovistos de los suficientes requisitos de seguridad. A su vez, esto implica que son sistemas que no están preparados para enfrentarse a las amenazas actuales. Superar las actuales lagunas de seguridad requiere tener una comprensión sólida de lo que es la seguridad (es decir, cuáles son las vulnerabilidades, sus orígenes, su frecuencia, etc.). Una evaluación adecuada de la seguridad exige el uso de herramientas y metodologías especializadas. La Agencia destaca la acuciante necesidad de disponer de una estrategia concreta que permita definir los objetivos, la misión y la visión de unas pruebas de capacidad coordinadas en la UE.

Este estudio explora la manera de coordinar las acciones llevadas a cabo en la UE para que las pruebas de los ICS que sean armonizadas, independientes y fiables, lo cual permitiría sacar partido de las iniciativas actuales. La metodología consistiría en investigación de escritorio, una encuesta en línea y entrevistas en profundidad con 27 expertos de la UE, los Estados Unidos, Japón, la India y Brasil.

Principales conclusiones y recomendaciones
Del estudio se desprenden 36 conclusiones y 7 recomendaciones dirigidas tanto al sector público como al privado, con una atención especial a los organismos de la UE:

- 1. Creación de una coordinación de pruebas de capacidad bajo el liderazgo público de la UE y un fuerte apoyo por parte de las autoridades públicas y nacionales pertinentes, así como del sector privado de la UE.
- 2. Establecimiento de una Junta Ejecutiva funcional y de confianza que refuerce el liderazgo.

- 3. Creación o implicación de grupos de trabajo específicos.
- 4. Definición de un modelo financiero que sea adecuado para la situación europea.
- 5. Realización de un estudio de viabilidad con relación a la manera en que deberían organizarse las pruebas.
- 6. Firma de acuerdos de colaboración con otras organizaciones que trabajen en la seguridad de los ICS.
- 7. Establecimiento de un programa de gestión de conocimientos para las pruebas de los ICS.

El profesor Udo Helmbrecht, Director Ejecutivo de ENISA, declaró: "*Existe una clara necesidad de incrementar la seguridad de las infraestructuras críticas de información y los sistemas ICS; los riesgos son cada vez mayores, y tanto los desastres naturales como los cada vez más avezados delincuentes han puesto en evidencia las debilidades de los sistemas*. *Recomendamos enérgicamente a todas las entidades públicas y privadas implicadas que afronten las cuestiones relativas a la seguridad con la mayor firmeza posible".*

Informe completo
Contexto: Estrategia de ciberseguridad de la UE
Entrevistas: Ulf Bergstrom, portavoz, ulf.bergstrom@enisa.europa.eu, móvil: + 30 6948 460 143, o Adrian Pauna, experto, resilience@enisa.europa.eu

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