04/12/2013

EPR/17/2013
www.enisa.europa.eu

Cómo atenuar los ataques en los sistemas de control industrial (ICS): la nueva guía de la agencia europea ENISA.

ENISA, la agencia de ciberseguridad de la UE, ha elaborado un nuevo manual para atenuar de modo más eficiente los ataques en los sistemas de control industrial (ICS, por sus siglas en inglés) mediante un apoyo a procesos industriales vitales, principalmente en el área de las infraestructuras de información crítica (como los sectores energético y de transporte químico), donde a menudo existe una carencia de conocimientos suficientes. Dado que los ICS suelen estar conectados a plataformas de Internet, es necesario tomar medidas de seguridad adicionales. Esta nueva guía proporciona las consideraciones claves necesarias para equipos encargados de ICS con capacidad de respuesta a emergencias informáticas (ICS-CERC, por sus siglas en inglés).

Los ICS son indispensables para diversos procesos industriales, como la distribución de energía, el tratamiento de aguas y el transporte, así como para procesos químicos, gubernamentales, de defensa y alimentarios. Los ICS son objetivos lucrativos para intrusos como los grupos delictivos, servicios de espionaje extranjeros, *phishers*, *spammers* o terroristas. Los ciberincidentes que afectan a los ICS pueden tener efectos desastrosos en la economía de un país y en la vida de sus ciudadanos. Pueden causar largas interrupciones en el suministro de la electricidad, paralizar redes de transporte y provocar catástrofes ecológicas. Así pues, la capacidad de responder a los incidentes en los ICS y atenuar su impacto es un aspecto fundamental a la hora de proteger las infraestructuras de información crítica y optimizar la ciberseguridad a nivel nacional, europeo y mundial. Por ello, ENISA creyó oportuno crear esta guía sobre buenas prácticas de prevención y preparación para organismos con CERC-ICS, poniendo de relieve las siguientes conclusiones:

- Mientras que la prioridad principal de los sistemas TIC es la integridad, la de los ICS es la **disponibilidad** (de la escala «CID»: Confidencialidad, Integridad, Disponibilidad). Esto se debe a que los ICS son indispensables para garantizar el perfecto funcionamiento de las infraestructuras críticas.
- Los principales actores de los ICS no tienen suficientes conocimientos en materia de ciberseguridad. Asimismo, los equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés) ya establecidos no siempre entienden todos los aspectos técnicos específicos de sector de los ICS.
- Ante los posibles daños significativos que pueden producirse en los ICS, el **proceso de contratación** de los ICS-CERC requiere una estricta selección de personal, y deben de tenerse muy en cuenta otros muchos aspectos como, por ejemplo, la capacidad de un individuo de rendir bajo presión y su voluntad de respuesta fuera del horario laboral.
- Debe reconocerse la importancia de la **cooperación tanto a nivel nacional como internacional**.
- Los retos exclusivos a los que se enfrentan los servicios de ciberseguridad de los ICS pueden simplificarse mediante unas **buenas prácticas por parte de los CERT**, la aplicación de las experiencias mundiales y europeas conocidas y un **mejor intercambio de buenas prácticas**.

El Profesor Udo Helmbrecht, Director Ejecutivo de ENISA, declaró: «Aunque, hasta hace unas pocas décadas, los ICS funcionaban en entornos diferenciados y específicos, hoy suelen estar conectados a

Internet. Esto permite la racionalización y la automatización de los procesos industriales, al mismo tiempo que aumenta el riesgo de exposición a ciberataques».

Informe completo: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems/

Contexto: Estrategia de ciberseguridad de la UE. Esta guía se creó a partir de los trabajos previos realizados por ENISA en el campo de los CERT[1]. En ningún caso prescribe a qué entidades de los estados miembros deben confiarse los servicios de los ICS-CERC.

Entrevistas: Ulf Bergstrom, portavoz, ulf.bergstrom@enisa.europa.eu, móvil: + 30 6948 460 143, o Andrea Dufkova, Experta, [cert-relations [AT]enisa.europa.eu

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

[1] *http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities*