09/10/2013

EPR12/2013

www.enisa.europa.eu

Ciberseguridad: Libro blanco de ENISA ¿Podemos aprender de los incidentes de seguridad en los Sistemas de Control Industrial/SCADA?

La agencia de ciberseguridad de la UE (ENISA) ha publicado hoy un libro blanco en el que ofrece recomendaciones con relación a la prevención y la preparación de una respuesta ágil e integrada a los ciberataques y los incidentes contra Sistemas de Control Industrial (SCI) o sistemas de Control de Supervisión y de Adquisición de Datos (SCADA, por sus siglas en inglés). El reciente aumento de la cantidad de incidentes de seguridad contra SCI/SCADA plantea interrogantes acerca de la capacidad de muchas organizaciones para responder a incidentes críticos y analizarlos. Por esta razón, la Agencia subraya la necesidad imperiosa de crear un entorno de aprendizaje proactivo a través de análisis posteriores de incidentes.

Los SCI son de uso común en el control de los procesos industriales de la fabricación, la producción y la distribución de productos. A menudo suele emplearse software comercial de serie no actualizado. Entre los tipos más conocidos de SCI cabe mencionar los SCADA, que constituyen el mayor subgrupo de SCI. Los recientes incidentes en SCI/SCADA demuestran la importancia que tienen la buena gobernanza y el control de las infraestructuras SCADA. **En concreto, y según subraya la Agencia, la capacidad de responder a los incidentes críticos y de analizar los resultados de un ataque con el fin de aprender de dichos incidentes es un factor crucial**.

El objetivo de los análisis posteriores de incidentes es conocer en mayor profundidad el incidente, lo cual facilitará la capacidad de:

- basarse en conclusiones sólidas con el fin de responder a la naturaleza cambiante de las amenazas tanto internas como externas; y
- asegurarse de que haya un aprendizaje suficiente que permita desplegar sistemas más flexibles y resistentes.

Hemos identificado cuatro puntos clave en la creación de un entorno de aprendizaje proactivo que, a su vez, garantice una respuesta rápida a los ciberincidentes y sus análisis posteriores:

- La complementación de la base de conocimientos técnicos existente mediante una especialización de los análisis posteriores y la comprensión de los solapamientos entre equipos de respuesta contra ciberincidentes e incidentes físicos críticos;
- La facilitación de la integración de procesos de respuesta física y cibernética con una mayor comprensión de dónde pueden encontrarse las pruebas digitales y cuáles son las medidas apropiadas que cabe tomar para su preservación;
- El diseño y la configuración de sistemas de manera que permitan la retención de pruebas digitales; y
- El incremento de los esfuerzos de colaboración entre organizaciones, así como a nivel interestatal.

El profesor Udo Helmbrecht, Director Ejecutivo de ENISA, comentó: "Los sistemas SCADA suelen estar integrados en sectores que forman parte de la infraestructura crítica de una nación, como por ejemplo la distribución de energía y el control del transporte, lo cual los convierte en atractivos objetivos de ciberataques llevados a cabo por nacionales descontentos, grupos disidentes o estados extranjeros. Dichos sistemas deberían utilizarse de modo que posibiliten la recopilación y el análisis de las pruebas digitales que, a su vez, permitirán la identificación de lo sucedido durante una violación de seguridad".

Informe completo y recomendaciones: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

Contexto: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Entrevistas: Ulf Bergstrom, portavoz, ulf.bergstrom[at]enisa.europa.eu, móvil: + 30 6948 460 143, o Adrian Pauna, Experto, resilience[at]enisa.europa.eu

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