El *Informe de Amenazas IA-04/16* del CCN-CERT está disponible en la parte pública de su portal web

Amenazas y análisis de riesgos en Sistemas de Control Industrial

- **Ofrecer de manera muy práctica herramientas que ayuden a llevar a cabo una aproximación inicial a la situación en la que se encuentran los ICS de una organización en materia de ciberseguridad, principal objetivo del Informe.**

- **El documento se enmarca dentro de una serie de actuaciones del CCN que intentarán facilitar la realización de análisis de riesgos empleando MAGERIT/PILAR con el fin de apoyar a las diferentes empresas en la redacción de los Planes de Seguridad de Operado (PSO) y Planes de Protección Específicos (PPE).**

Madrid, 9 de febrero de 2016.- El CCN-CERT ha hecho público un nuevo Informe de Amenazas IA**-04/16 Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS)**, en el que se presenta una selección de amenazas que, según el criterio y experiencia de los autores, son más frecuentes y características en el ámbito industrial y que por tanto deben constituir el principal objeto de atención a la hora de abordar un análisis de riesgos de un sistema de control industrial.

El documento, que recalca que los conceptos de Sistema de Control Industrial (ICS) e Infraestructura Crítica (IC) no son intercambiables, plantea que uno de los mayores problemas es la barrera cultural que existe entre el mundo de la ciberseguridad IT (*Information Technology*) y ciberseguridad OT (*Operation Technology*). Se parte de la idea de que la ciberseguridad de los sistemas de control industrial se encuentra en un terreno a caballo entre dos culturas profesionales y que lo más frecuente es que no los diseñen, construyan ni exploten expertos en seguridad.

El Informe recoge una pequeña introducción a los distintos conceptos, así como una metodología, con un punto de partida y referencia y una clasificación por subsectores. Además, se añade un catálogo de Escenario de Riesgo (ER) en ICS como pueden ser: dispositivos portátiles, trabajo de terceros, interconexiones de redes, copias de seguridad, concienciación del personal, gestión de cambios, gestión de incidentes y continuidad, gestión de la información y del software, gestión de la seguridad, gestión de usuarios y contraseñas y gestión técnica de la seguridad y sistemas.

Análisis de Riesgos

El informe se enmarca dentro de una serie de actuaciones previstas en materia de seguridad de sistemas industriales que emplean sistemas de información de forma muy

específica. En particular se publicará una guía de cómo se puede utilizar la herramienta PILAR de análisis de riesgos para valorar el estado de seguridad de un sistema ICS, permitiendo desarrollar y monitorizar planes de mejora técnicos, así como integrar un entorno de procedimientos operacionales para completar los puntos tecnológicamente débiles.

PILAR, en su versión MICRO permitirá a las diferentes empresas realizar un análisis de riesgos que facilite la redacción de los Planes de Seguridad de Operador (PSO) y Planes de Protección Específicos (PPE).

El Informe puede descargarse desde la parte pública del portal del CCN-CERT.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/

@CCNCERT

http://youtu.be/5XxS9mZZfKs