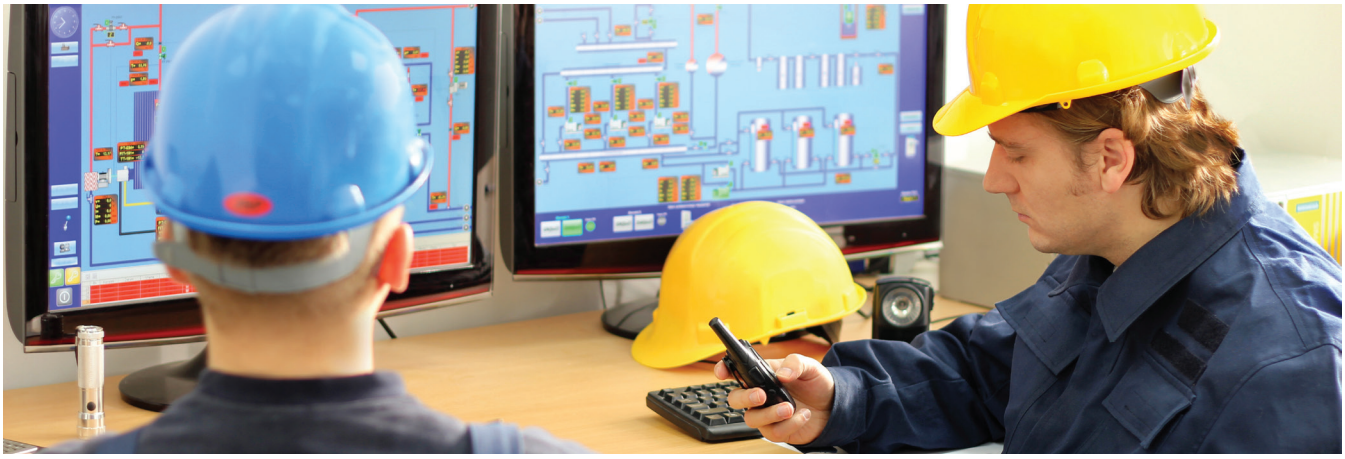

Foto: Shutterstock.

De la falta de intencionalidad a los ataques

J. C. A.

La ciberseguridad industrial exige soluciones personalizadas. Los Sistemas de Control Industrial (SCI), incluso los que no están conectados a la red, están expuestos a las ciberamenazas. Los puntos débiles de los SCI frente a estos ataques están relacionados con una arquitectura de red que no hace una buena segregación de los flujos de comunicación entre las redes de instrumentación, control, operación y gestión. También influyen políticas no retadoras de la configuración de los dispositivos de red, sistemas operativos y aplicaciones que limiten o eliminen aquellos servicios o acceso que sean innecesarios para la operación del sistema industrial de control. O políticas laxas de gestión de cuentas y de confidencialidad de la información y la falta de un sistema de gestión de la ciberseguridad, explica Héctor Puyosa, de la Universidad Politécnica de Cartagena,

El personal con acceso interno es quizá el eslabón más débil, pues puede romper por desconocimiento, error o intencionalmente las medidas de ciberseguridad establecidas. Por ello es imprescindible la formación del personal, disponer de medios para la detección de intrusión y la realización de auditorías para identificar desviaciones y oportunidades de mejora.

Obsolescencia de los sistemas

Un elemento de preocupación es la obsolescencia de los SCI que corren sobre sistemas operativos que ya no están soportados por sus fabricantes, por lo que ya no se desarrollan parches ni actualizaciones de seguridad.

Veamos cómo una aparente acción menor no intencionada puede tener efectos desastrosos. Un operador de una planta industrial intenta en vano imprimir información del proceso de planta. Decide revisar por su cuenta la impresora. Son las 12 horas de la mañana de un fin de semana. El dispositivo forma parte del sistema de control y está conectado a la red vía Ethernet. El operador observa un cable de red suelto al lado de la impresora. “Debe ser la causa del fallo”, piensa, y lo conecta. Lo intenta de nuevo. Sigue sin imprimir y desiste. Varias horas más tarde, el refresco de la información del proceso en las distintas pantallas de operación del DCS es cada vez más lento y se pierde la visualización de lo que pasa en campo. Alarma roja.

Se decide preparar la planta para una parada manual de emergencia y se llama al servicio de retén de instrumentación y control para que intente resolver el problema. No lo consigue y decide reinicializar el servidor de la consola de operación. Parte de los servicios de planta ya estaban parados y ya había entrado el siguiente turno de operación. Las comunicaciones se restablecen pero el tráfico de mensajes es inusual. Al poco se repite la pérdida de visualización. Tras rastrear el tráfico de mensajes, descubre que una impresora en la sala de control está conectada a la red por dos cables. Al consultar la documentación disponible, concluye que el cable frontal no debería estar conectado. Lo desconecta. Al cabo de un tiempo el tráfico de mensajes vuelve a su condición normal. Conclusión: la empresa decide actualizar las políticas de autorización de acceso físico a los equipos y la documentación.

Ciberataques relevantes

¿Qué consecuencias pueden tener los ataques externos y deliberados? A finales de 2014, un ciberataque produjo daños masivos en un alto horno de una acería en Alemania, cuenta Héctor Puyosa. Los *hackers* utilizaron técnicas de ingeniería social y el envío de mensajes personalizados a trabajadores de esa fábrica con los que obtuvieron acceso a sus identificadores y claves de acceso a la red de oficinas y de allí al sistema de producción. El acceso malicioso logró finalmente la denegación del control para realizar una parada controlada del horno que obligó a una parada de emergencia no controlada con resultado de daños masivos.

Otro caso relevante fue la destrucción en 2010 de cientos de centrifugadoras que producen uranio enriquecido en la fábrica de Natanz (Irán) mediante el código dañino Stuxnet. Las investigaciones concluyeron que ese código fue diseñado para interceptar órdenes de un sistema SCADA con comandos maliciosos que produjeron la rotura de las centrifugadoras. Stuxnet fue el primer *malware* conocido que espía y reprograma SCI que corren sobre el sistema operativo Windows. El sistema SCADA estaba completamente aislado del resto de redes de comunicación, por lo que el ataque probablemente se realizó utilizando técnicas de ingeniería social para infectar con el código malicioso dispositivos extraíbles, seguramente llaves USB, de trabajadores de esas instalaciones.