Foto: Shutterstock.

Los retos de la ciberseguridad industrial

La escasa concienciación, la obsolescencia y heterogeneidad de los sistemas de control, la conexión a internet y la falta de personal experto aumentan la vulnerabilidad a los ciberataques en la industria

Joan Carles Ambrojo

El 15 de agosto de 2012 un empleado de la empresa Saudi Aramco abre un correo electrónico. Desconoce que ha facilitado vía libre a un virus demoledor. Unas horas más tarde, el programa maligno (*malware*) deja fuera de combate las unidades de disco duro de 35.000 ordenadores de la compañía y pone en riesgo el suministro del 10% del petróleo del mundo. Aramco había invertido mucho en preservar los sistemas de control industrial de los ataques informáticos y, gracias a ello, las actividades de perforación y bombeo no se vieron afectadas. Sin embargo, el resto de la informática cayó. La empresa regresó a las cuartillas de papel, las máquinas de escribir y el fax para gestionar pedidos millonarios o autorizar el llenado de las cisternas de combustible. Aramco tuvo que comprar 50.000 discos duros y contratar expertos en ciberseguridad. Seis meses le costó poner en línea su infraestructura informática, tras desplegar una red nueva y segura. Una industria con menores recursos habría quebrado irremisiblemente, rememora Chris Kubecka, exasesora de seguridad de Saudi Aramco durante la crisis, a CNN Money en la última conferencia Black Hat celebrada en Las Vegas.

Los expertos claman por mejorar la seguridad de los sistemas de control industrial (SCI), cada vez más expuestos al mismo tipo de ciberamenazas que los sistemas informáticos convencionales. Muchos países han establecido políticas de ciberseguridad para proteger las denominadas infraestructuras críticas (centrales nucleares, plantas químicas, etc.). Sin embargo, muchos SCI en escenarios no críticos están expuestos a incidentes de ciberseguridad que pueden producirse de forma presencial o telemática.

Hay una gran oportunidad para profesionales del ámbito industrial y de la informática de formarse en ciberseguridad

Países como Estados Unidos tienen un nivel muy alto de madurez en la protección de los SCI, con numerosas iniciativas gubernamentales y privadas e importantes presupuestos para su desarrollo. Europa lleva al menos cinco años de retraso. España, cinco años más, según el Centro de Ciberseguridad Industrial (CCI). “En España más de la mitad de los incidentes son motivados por código dañino y, en segundo lugar, las intrusiones en los sistemas”, afirma Héctor Puyosa, doctor en ingeniería industrial e investigador del departamento de Ingeniería de Sistemas y Automática de la Universidad Politécnica de Cartagena (UPCT).

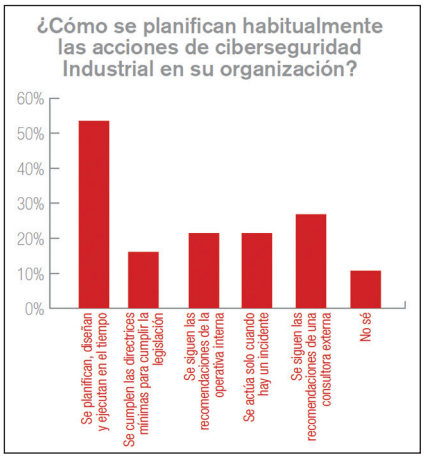
Uno de los grandes mitos es pensar que un ataque a un sistema de control industrial tendrá un impacto menor que si fuera un incidente físico (el robo de cableado o un incendio). “En los últimos dos años hemos estado haciendo una labor de concienciación sobre los riesgos de las ciberamenazas. España es uno de los países donde hay más conciencia en ciberseguridad, aunque todavía se tenga que plasmar en la toma de medidas”, dice José Valiente, director del CCI.

Cultura reciente

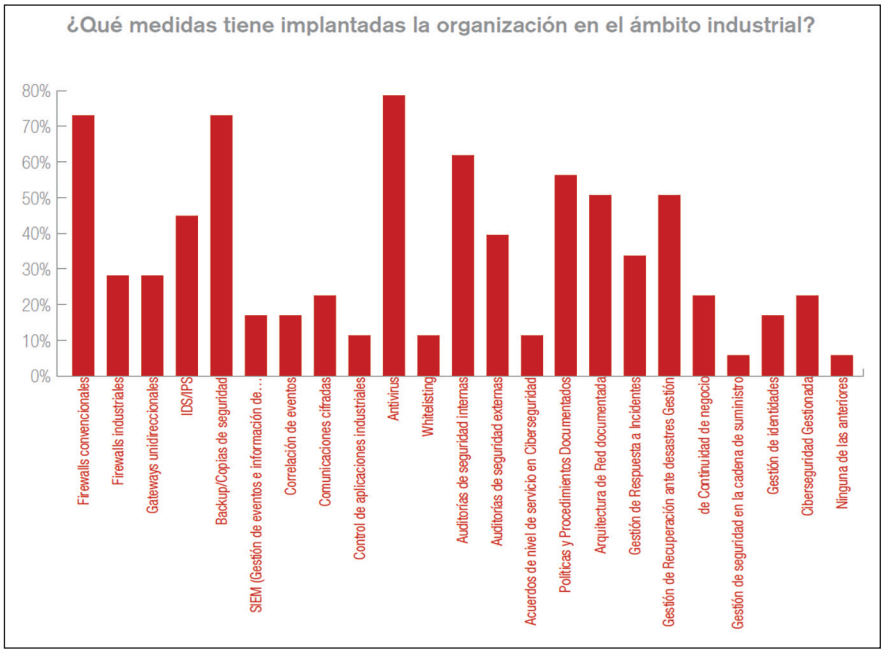
La cultura de seguridad informática en el entorno de los sistemas de control es muy reciente, “ya que en sus orígenes esos sistemas fueron diseñados asumiendo que todos los usuarios eran de confianza y los sistemas operativos y protocolos de comunicación eran propietarios”, añade Héctor Puyosa. Los SCI comerciales que se utilizan en España son de los mismos fabricantes y marcas que se utilizan en Europa y el resto del mundo, por lo que no existe una diferencia tecnológica en ese aspecto. El diferente tratamiento de la ciberseguridad está asociado al sector industrial (regulaciones, buenas prácticas), al tamaño de la empresa (recursos, políticas de seguridad y gestión del riesgo), y al mayor o menor grado de conocimiento que tenga la gerencia media en temas de tecnología de la información, dice Puyosa.

La ciberseguridad industrial aborda la prevención, monitorización y mejora de la resistencia de los sistemas industriales y su recuperación, ante acciones hostiles o inesperadas que puedan afectar al correc-

Evaluación del riesgo en las organizaciones industriales. Fuente: *Informe sobre el Estado de la Ciberseguridad Industrial en España 2015* del Centro de Ciberseguridad Industrial.



Planificación de acciones de ciberseguridad en las organizaciones industriales. Fuente: *Informe sobre el Estado de la Ciberseguridad Industrial en España 2015* del Centro de Ciberseguridad Industrial.



Medidas de seguridad en las organizaciones industriales. Fuente: *Informe sobre el Estado de la Ciberseguridad Industrial en España 2015* del Centro de Ciberseguridad Industrial.

to funcionamiento de los procesos industriales, explica José Valiente. La ciberseguridad se aplica en todos los entornos que contengan SCI, que controlan procesos físicos (desde la producción y distribución de energía a la automoción).

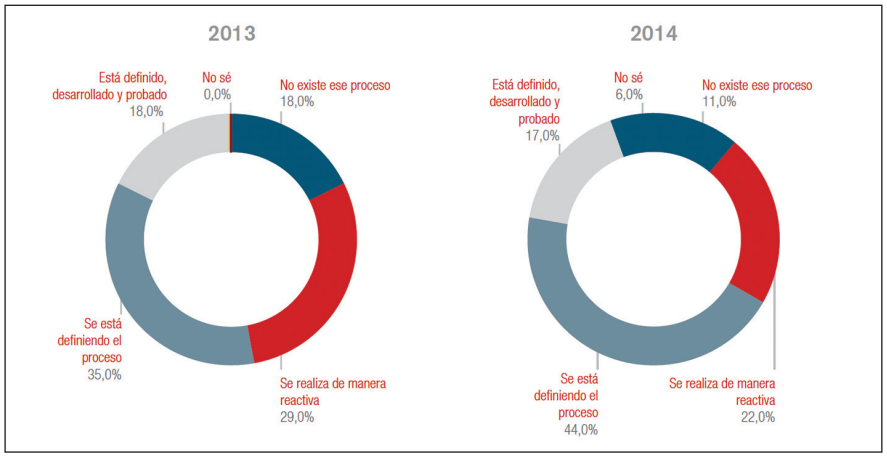
La ciberseguridad son un conjunto de prácticas, procesos y tecnologías diseñados para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, explica José Valiente. Es necesario complementar estas medidas con sus versiones equivalentes en otras dimensiones de la seguridad, "como lo son la seguridad medioambiental, la seguridad física y la seguridad de las personas y el equipamiento, sin olvidar el patrimonio tecnológico de las industrias (activos tangibles e intangibles derivados del trabajo intelectual: idea, invención, secreto industrial, proceso, programa, etc.), dice este experto. Este patrimonio puede ser o no catalogado como una infraestructura crítica (según el sector en el que se enmarque), pero siempre será el principal activo que proteger por las industrias.

En España, el Consejo de Seguridad Nacional aprobó el 5 de diciembre de 2013 la Estrategia de Ciberseguridad Nacional con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las infraestructuras críticas. La Ley 8/2011, de 28 de abril, establece las medidas que operadores y Administraciones públicas deben adoptar para proteger las infraestructuras críticas. En general, estas infraestructuras son gestionadas mediante sistemas industriales de control, explica Héctor Puyosa.

Ciberejercicios defensivos

El Instituto Nacional de la Ciberseguridad (Incibe), dependiente de la Secretaría de Estado de las Comunicaciones y de la Sociedad de la Información, está teniendo un papel activo en la mejora de la ciberseguridad, prestando apoyo a la investigación y a la coordinación de actuaciones en este ámbito. El Incibe ayuda a la prevención, respuesta y recuperación en caso de que se haya producido un ataque exitoso y así como a establecer todos los mecanismos y vías para conseguir la colaboración entre empresas privadas y sector público, pero también entre empresas privadas, señala Ignacio González, subdirector del Incibe. También animan a las empresas a participar en "ciberejercicios, para que practiquen y conozcan en casos simulados el nivel de capacidad de defensa frente a las ciberamenazas". España está haciendo los deberes en ciberseguridad, asegura González: algunas industrias están muy avanzadas e invierten en materia de ciberseguridad, "y es nuestro trabajo empujar a las que no lo están tanto para que mejoren las medidas".

El 20-25% de las industrias tienen ya sistemas de gestión de seguridad de la información, certificados con ISO 27001; "pero no tienen dentro de su alcance los sistemas de operación, de control industrial", asegura José Valiente. Los incidentes de seguridad de los sistemas de control industrial se gestionan igual que los sistemas de información, "que no es lo más adecuado. No hay un sistema estandarizado para gestionar estos incidentes, ni se ha establecido un plan adecuado de recuperación", añade el director del CCI. Los departamentos de tecnologías de la información, seguidos por los de seguridad física y operaciones son sobre los que más habitualmente recae la responsabilidad en materia de ciberseguridad industrial, según el *Estado de la Ciberseguridad Industrial en España 2015*, un informe elaborado por el CCI. La mayor parte de los proyectos de ciberseguridad industrial, en general en grandes empresas, están motivados por la regulación, los procesos de mejora continua y la respuesta a incidentes.



Comparativa 2013-2014 en la gestión de incidentes de ciberseguridad industrial. Fuente: *Informe sobre el Estado de la Ciberseguridad Industrial en España 2015* del Centro de Ciberseguridad Industrial.

Las empresas grandes y medianas están empezando a tomar conciencia de la situación. Las primeras acciones suelen ser las de concienciación del personal y las evaluaciones del nivel de ciberseguridad, afirma Óscar Navarro, del área de consultoría de S2 Grupo. A pesar de existir un cierto "divorcio" entre los expertos en control industrial y los informáticos de cara a la ciberseguridad industrial, "algunas empresas como la nuestra ya forman equipos multidisciplinares para trabajar en ciberseguridad industrial", añade Navarro.

Certificar la seguridad

Certificar la seguridad industrial es difícil porque cuesta certificar tecnologías que en ningún momento incluyeron la ciberseguridad y lógicamente, el periodo de amortización de esas tecnologías es largo. "Los vectores de ataques explotan distintos tipos de vulnerabilidades. Las más comunes son aquellas asociadas a la obsolescencia y falta de actualización de *software* (incluida la falta de actualización de antivirus), agujeros en las políticas de seguridad y una segregación o arquitectura de redes de comunicación incompleta o con algunos fallos de diseño o mantenimiento", asegura Héctor Puyosa. En los últimos años, muchos de estos sistemas, que no se han reemplazado porque tienen periodos de amortización superiores a los 15 años, se han ido conectando a internet y pueden ser atacados con cierta facilidad, ya que prácticamente todos tienen controles de acceso por usuario y contraseña por defecto o muy débil, precisa Ignacio González. "Cuando se diseñaron los SCI no pensaron necesario incluir requisitos de seguridad [suficientes]".

Sin embargo, la mayor vulnerabilidad que tenemos en España está relacionada con la falta de una cultura en ciberseguridad, sentencia el profesor de la UPCT. "Hace falta cambiar la percepción del riesgo, que se considere que es muy probable que ocurra un incidente de seguridad, que su impacto será inmediato y con consecuencias importantes". En los últimos años se observa cierto avance pero hace falta una mayor difusión del tema para educar y concienciar a las personas y las empresas. Esa sensibilización debe estar acompañada de acciones desde las Administraciones públicas, imponiendo medidas reglamentarias y ofreciendo ayudas para acelerar la implantación de recomendaciones y buenas prácticas. "Es de destacar el desarrollo del primer curso masivo abierto *online* sobre ciberseguridad industrial que tuvo una exitosa primera edición en el último trimestre de 2014. Este tipo de formación de calidad es una necesaria y excelente iniciativa del sector público para crear un ecosistema de profesionales cualificados en la materia", dice Héctor Puyosa. Por su parte, el CCI organiza en Madrid en el mes de octubre el V Congreso Internacional de Ciberseguridad Industrial.

Los principales problemas de ciberseguridad están relacionados con la conectividad, y si en el ámbito industrial no se tienen conocimientos sobre conectividad menos todavía de ciberseguridad, añade José Valiente. De igual modo, en el ámbito de los profesionales de tecnologías de la información existe un desconocimiento sobre cómo son los protocolos industriales, cómo funcionan los sistemas de control, y no se pueden aplicar las mismas técnicas y procedimientos que se aplican a los sistemas de información", dice el director del CCI.

La oportunidad de negocio relacionado con las auditorías, planes de mejora e implantación de soluciones de ciberseguridad ha hecho que diversas empresas españolas estén fortaleciendo sus capacidades para dar este tipo de servicios. "En España se puede conseguir un adecuado nivel de servicio en ciberseguridad de las empresas fabricantes o distribuidoras de sistemas de control que conocen muy bien sus equipos, así como de las empresas consultoras e integradores que pueden ayudar a desplegar elementos de detección y mitigación de riesgos o fortificar los servidores y sistemas de red", señala Puyosa. El CCI publicó en mayo de 2015 un catálogo de proveedores, servicios y soluciones en ciberseguridad industrial.

Hay una gran oportunidad para profesionales del ámbito de la informática tradicional, e incluso industrial, de formarse en ciberseguridad de estos sistemas. El *Informe anual de seguridad de Cisco 2014* indica un déficit de más de un millón de profesionales de la seguridad en todo el mundo para el año pasado. "Con el internet de las cosas y la industria 4.0 la cifra se quedará corta", señala Valiente.

Tendencias

Los incidentes en seguridad informática tienden a aumentar y la ciberseguridad se consolidará como una parte más de los sistemas de gestión, afirma Héctor Puyosa, experto que también forma parte del grupo técnico de ISA que desarrolla la serie de estándares internacionales sobre ciberseguridad industrial ISA-62443. "El desarrollo de normas y recomendaciones como la serie ISA-62443 sobre ciberseguridad de los sistemas industriales de automatización y control y su confluencia con la familia de estándares ISO 27000, sistema de gestión de la seguridad de la información, ayudará a clarificar las diferencias de requerimientos pero asegurará que las buenas prácticas del mundo de las tecnologías de la información se apliquen con éxito en las aplicaciones de operación de plantas industriales", precisa Puyosa.

Desde el punto de vista tecnológico, se espera nuevos desarrollos que mejoren las capacidades de autentificación y autorización, filtrado / bloqueo y control de acceso, encriptado y validación de datos de los sistemas de control, así como herramientas más sencillas de utilizar y que requieran de menos conocimientos específicos para la medición, monitorización y detección de intrusiones, concluye el investigador de la UPCT.