Valencia Industria Conectada VLC 4.0

HABILITADORES Digitales

Ciberseguridad

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball

FEMEVAL

AIDIMME INSTITUTO TECNOLÓGICO
METALMECÁNICO, MUEBLE, MADERA, EMBALAJE Y AFINES

ITE INSTITUTO TECNOLÓGICO DE LA ENERGÍA

SOBRE LA CIBERSEGURIDAD

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.

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 Kubečka, 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.

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" (Revista Técnica Industrial. Sept 2015. http://www.tecnicaindustrial.es/TIFrontal/a-6476-los-retos-ciberseguridad-industrial.aspx).

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. 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. 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. (Revista Técnica Industrial. Sept 2015. http://www.tecnicaindustrial.es/TIFrontal/a-6476-los-retos-ciberseguridad-industrial.aspx)

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.

Además, 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. Desde INCIBE 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.

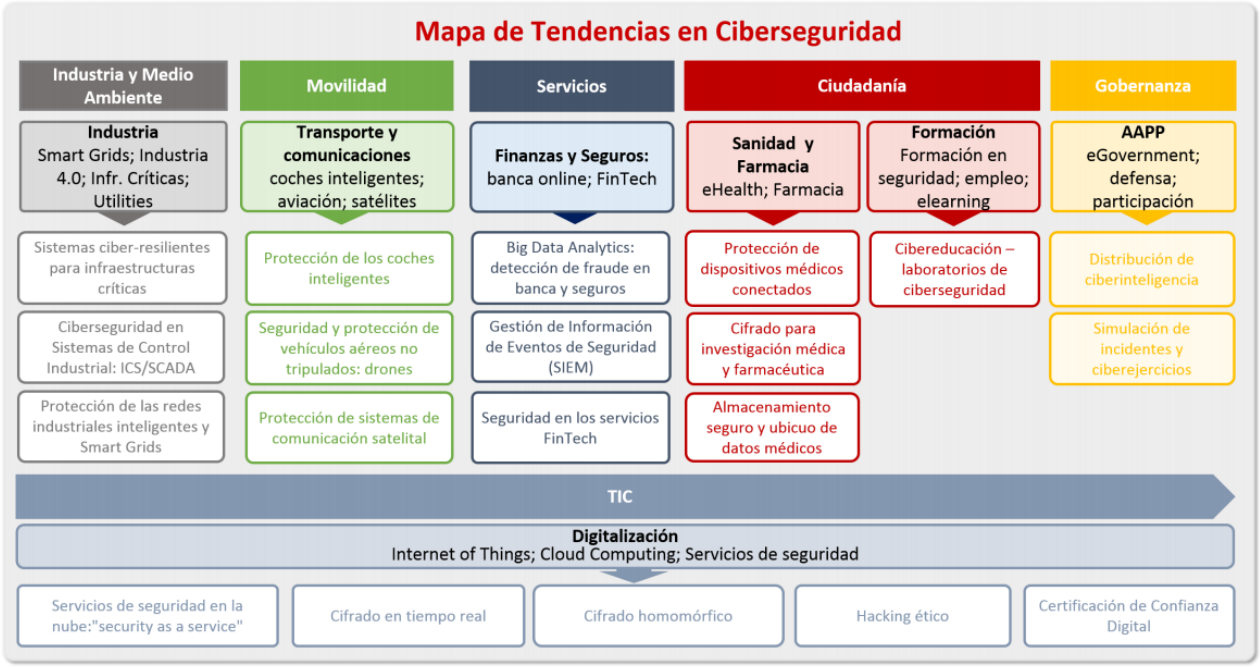
Según INCIBE, el 20-25% de las industrias tienen ya sistemas de gestión de seguridad de la información, certificados con ISO 27001, pero no tienen dentro de su alcance los sistemas de operación, de control industrial (SCI). Los incidentes de seguridad de los sistemas de control industrial se gestionan igual que los sistemas de información, pero esta práctica no es la más adecuada. En la mayor parte de las empresas no hay un sistema estandarizado para gestionar estos incidentes, ni se ha establecido un plan adecuado de recuperación.

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 – (https://www.cci-es.org/). 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.

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.

TENDENCIAS PARA LOS PRÓXIMOS AÑOS

Según el informe realizado por INCIBE en 2016, las tendencias del mercado se muestran en la siguiente figura. (https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf)



Por otro lado, IT Business Solutions (https://www.itbusiness-solutions.com.mx/cinco-tendencias-en-ciberseguridad-2018) señala que en 2018 los principales retos en este ámbito son:

- Privacidad digital. Se seguirá avanzando en el análisis y protección de los derechos sobre la privacidad de los datos digitales (olvido, la portabilidad y el impedimento a las empresas de crear un perfil con el comportamiento de los individuos en Internet)
- Ataques a criptomonedas
- Ransomware más complejo
- Internet de las Cosas (IoT). La popularidad del uso de sensores y dispositivos de monitoreo conectados a las redes plantea la aparición de más códigos maliciosos para dispositivos móviles, especialmente en el caso del Internet de las Cosas (IoT).
- Infraestructuras de misión crítica. Plantas hidráulicas, de gas, o petroquímica, entre otros servicios críticos de países y gobiernos, se encuentran en la mira de los delincuentes.
- Información y capacitación. Tanto en el ámbito empresarial como particular, la información y capacitación son aspectos clave para la ciberseguridad. En 2018, el entorno será más peligroso, lo que obliga a las empresas a lograr un cambio de mentalidad y crear una estrategia para conseguir un plan de ciberseguridad efectivo para proteger los activos en la red.

NIVEL DE USO. DATOS ESTADÍSTICOS

Según la "Encuesta Mundial sobre el Estado de la Seguridad de la Información" (PWC, 2017. https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html), desde 2012, el presupuesto medio que las empresas dedican a ciberseguridad en el mundo casi se ha duplicado, pasando de 2,8 a 5,1 millones de dólares. En España, la inversión de las compañías en seguridad de la información ha seguido una evolución parecida aunque algo más moderada.

Fuente: PwC, *The Global State of Information Security Survey® 2017.*

Los datos la encuesta en 2018 (PWC, 2018. https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html), revelan que muchas compañías siguen sin estar preparadas todavía para afrontar los riesgos derivados de los ciberataques. El 49% de los directivos españoles entrevistados –el 44% en el mundo- reconocen que sus empresas carecen de una estrategia integral de seguridad, el 53% que no cuentan con programas de formación para los empleados y el 55% que no disponen

de procedimientos previamente establecidos para responder a los incidentes de seguridad. De hecho, cuando se produce un ciberataque la mayoría de compañías reconocen que no son capaces de llegar a identificar su autoría –el 41%, en España y el 39%, en el mundo-.

El Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Energía, Turismo y Agenda Digital, resolvió un total de 123.064 incidentes de seguridad en 2017, un 6,77% más que 2016. Para el año 2018 INCIBE cuenta con un presupuesto de 23.220.000 millones de euros, y focalizará sus actuaciones se focalizarán en cuatro líneas: servicios de ciberseguridad (respuesta a incidentes y concienciación); desarrollo de tecnologías de ciberseguridad para la lucha contra el ciberdelito y cibercrimen; apoyo al desarrollo de la industria, I+D+i e identificación de talento y servicios transversales.

ENLACES DE INTERÉS

Guías sobre ciberseguridad del INCIBE
https://www.incibe.es/protege-tu-empresa/guias

Glosario de términos de ciberseguridad: una guía de aproximación para el empresario
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Cloud computing: una guía de aproximación para el empresario
https://www.incibe.es/protege-tu-empresa/guias/cloud-computing-guia-aproximacion-el-empresario

Decálogo ciberseguridad empresas: una guía de aproximación para el empresario
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Ransomware: una guía de aproximación para el empresario
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Ciberseguridad en la identidad digital y la reputación online. Una guía de aproximación para el empresario
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_identidad_online_metad_0.pdf

Tendencias en el mercado de la Ciberseguridad Julio de 2016
https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

Encuesta mundial de ciberseguridad
https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html