Deloitte.

Nuevos enfoques de protección frente a ciber riesgos

Cada vez parece más claro que conceptos como impresión 3D, internet de las cosas, cloud, robots de nueva generación, movilidad, analytics, industria 4.0, etc., van a introducir cambios relevantes en nuestra industria. De igual forma cuando vemos el acrónimo "ciber" asociado a diferentes conceptos, tendemos a considerar que es algo muy novedoso y no siempre cercano a nuestra realidad manufacturera. No obstante, uno de dichos términos, la ciberseguridad, forma parte de nuestra realidad mucho más de lo que a veces pensamos.

Ser conscientes de los ciber riesgos a los que nuestra industria está expuesta, y establecer mecanismos de protección para mitigarlos, puede resultar muy relevante en el entorno actual para asegurar el éxito en un mercado tan competitivo. La protección de la propiedad intelectual, la protección de la confidencialidad de propuestas económicas a los clientes, los impactos en la imagen de nuestra marca o en la de los directivos, la protección de los empleados en entornos conflictivos o la continuidad de nuestros procesos productivos, cada vez están más expuestas a riesgos ciber, incluso si operamos en un mercado tradicional.

Además, los impactos económicos directos también pueden ser relevantes: se estima que las organizaciones que se dedican a la explotación de estos riesgos obtienen unos beneficios globales anuales de más de 400.000 millones de dólares. Para ello trabajan en ataques preparados para conseguir objetivos específicos en personas o compañías específicas.

Por lo general tendemos a pensar que las inversiones realizadas en materia de seguridad de sistemas de información deberían mantener los riesgos ciber razonablemente controlados. Pero ante la vertiginosa evolución de la tecnología cabe preguntarse ¿estamos protegiendo adecuadamente nuestros activos tanto dentro como fuera de nuestras instalaciones? ¿Qué ocurre con la información en dispositivos móviles? ¿tenemos medios para saber si están intentando robar información confidencial?¿Están suplantando a la compañía o a un directivo en redes sociales? ¿Tenemos capacidad de respuesta si finalmente se produce alguna incidencia? ¿Conocen los empleados las medidas de seguridad que deben de reunir dentro y fuera de la compañía?

Oscar Martín Moraleda
Socio IT ERS

Ahora bien, aunque el paradigma de la seguridad haya cambiado, los ciber riesgos pueden mitigarse a través de un enfoque adecuado, que pasa por no infravalorar la exposición de nuestros negocios, identificar su potencial impacto y establecer los mecanismos de control apropiados al nivel de las personas, procesos e infraestructuras operativas y tecnológicas.

Entrando en algún ejemplo específico para nuestra industria, me gustaría dedicar unas líneas a los ciberriesgos asociados a los procesos productivos y de control industrial.

Ciber riesgos en los procesos de productivos y de control industrial

Volvamos a un concepto ya mencionado: el internet de las cosas. Parece algo que en un futuro no muy lejano cambiará la forma en que interactuamos entre nosotros,

con nuestros clientes, con nuestros familiares y amigos, etc., al disponer de todo tipo de cosas cotidianas conectadas a internet, intercambiando datos y tomándose decisiones en función de dichas conexiones.

Ahora bien, en los procesos productivos y de control industrial, esta situación es ya una realidad. Los sistemas empleados desde hace años para controlar dichos procesos, haciéndolos mucho más fiables, eficientes y eficaces, cada vez se encuentran más interconectados. Con el propósito de reducir los costes de producción y operación, las redes de estos sistemas de control automatizados (ICS) se han ido poco a poco conectando con las redes TI corporativas de las compañías. La idea de aprovechar las redes TI corporativas para gestionar y supervisar las operaciones de los ICS reduce la dependencia de los ingenieros de campo para gestionar y monitorizar estas redes y facilita la integración de las grandes operaciones de producción o distribución, que se encuentran geográficamente dispersas, con el entorno corporativo. Además, el negocio puede obtener información al momento del estado del proceso de producción y desde cualquier parte del mundo, abriendo un mundo de nuevas posibilidades.

Sin embargo, la integración de los sistemas ICS con las redes TI corporativas han hecho que algunos riesgos "ciber" sean ahora totalmente aplicables a las cadenas de producción, con la diferencia de que dichos sistemas no son habitualmente gestionados para mitigar dichos riesgos.

Hay múltiples situaciones reales de explotación de estos riesgos, con graves consecuencias. Sirva como ejemplo el reciente ataque a una empresa Alemana, con un complejo proceso de fabricación de metales y aceros, sufrió considerables pérdidas por un ciberataque que manipuló los procesos de fabricación hasta alterar componentes esenciales de la cadena de producción.

"Aunque el paradigma de la seguridad haya cambiado, los ciber riesgos pueden mitigarse a través de un enfoque adecuado"

La protección de los Sistemas de Control Industrial: la tarea en cuestión

Es necesario adaptarse a la evolución del panorama de seguridad a nivel mundial, con especial atención a la convergencia mutua de las Tecnologías de la Información y Tecnologías Operacionales. En un mundo totalmente hiperconectado, en el que la dependencia con la tecnología hace que hasta los estados se planteen contar con ciber-ejércitos, es necesario proteger adecuadamente los ICS, haciendo especialmente hincapié en:

- Aumento de la concienciación: conocer la existencia de un riesgo es el primer paso para hacerle frente. Operadores, ingenieros, fabricantes, gobiernos, usuarios, todos deben ser conscientes de la nueva realidad.

- Crear controles ajustados a su finalidad: cada industria y cada situación tiene sus fabricantes y sistemas de referencia, y su protección no es igual. A día de hoy existe software y hardware específico para proteger los sistemas ICS que deben tenerse en cuenta desde el diseño inicial.

- Aprovechar la experiencia: los peligros del ciberespacio no son nuevos para las redes normales, y aprovechar la experiencia y maneras de diseñar la red y cómo operar con ella es clave para tener éxito a la hora de proteger una red y reducir costes de implantación y operación de seguridad.

- Evaluar y probar: es imprescindible realizar periódicamente evaluaciones independientes de la seguridad del ICS. Los equipos de seguridad que tienen la suficiente experiencia, tanto en la seguridad de ICS como en la tecnología propia del ICS que están revisando, deben ser contratados para llevar a cabo dichas evaluaciones, en contraposición a las evaluaciones específicas de activos IT realizadas por profesionales de la seguridad de la información.

Lograr un sistema de control industrial seguro -"*safe*" y "*secure*" al mismo tiempo- y resiliente no es trivial y necesita de la colaboración de expertos tanto en los procesos y automatización industrial como en ciberseguridad, y es en la combinación de los dos mundos cuando se logra el éxito.