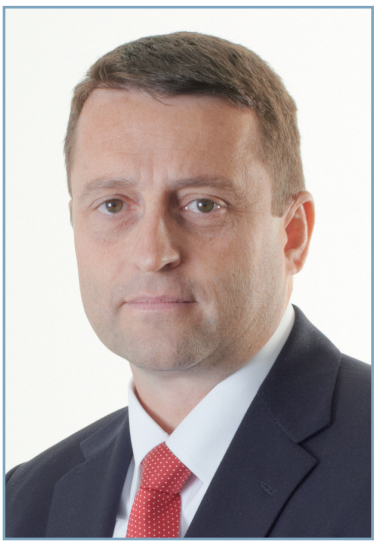

Ciberseguridad: preguntas simples para resolver un problema complejo

Marc Baret
Director, EMEA industrial services, Rockwell Automation

Frente a la convergencia de las tecnologías de información (IT) con las tecnologías de operación (OT) y desde que la industria utiliza sistemas informáticos, la ciberseguridad es una preocupación máxima y creciente para los dirigentes industriales. Los piratas informáticos no dejan de poner a prueba los sistemas industriales buscando la mínima vulnerabilidad para exigir un rescate, sabotear un proceso o robar la propiedad intelectual.

Conseguir que una empresa industrial sea segura y mantenerla así a largo plazo es un proceso continuado que requiere de una concepción de red OT sólida y de servicios de ciberseguridad gestionados. Esta misión puede parecer compleja para los directivos empresariales, sin embargo pueden beneficiarse de la ayuda de empresas con experiencia específica en OT.

UNA PREGUNTA INELUDIBLE

Si bien la digitalización de la industria tiene muchos beneficios tangibles, deben también considerarse los riesgos relativos a la ciberseguridad. La buena noticia es que, con el diseño correcto, las estrategias de seguridad y los servicios de detección de amenazas, los fabricantes pueden evitar el robo de datos y el tiempo de inactividad debido a problemas de ciberseguridad.

Permanecer fuera de la red tampoco es una opción realista, ya que los beneficios de la digitalización y de la industria 4.0 son simplemente demasiado grandes como para ignorarlos.

MANTENERSE FUERA DE LA RED

Permanecer fuera de la red tampoco es sinónimo de seguridad. Incluso los sistemas *offline* presentan vulnerabilidades de red que determinadas personas pueden explotar con dispositivos de consumo como una simple llave USB o una tarjeta Raspberry PI que sea capaz de explorar las redes WIFI locales.

ENTENDER LOS RIESGOS

Ningún negocio es completamente seguro. Sin embargo, existen varias estrategias que pueden reducir significativamente el riesgo, así como medidas preparatorias que pueden mitigar el impacto de un ciberataque. Estos planes de acción y métodos de recuperación deberían ser una parte integral de las operaciones normales de la fábrica. Desafortunadamente, pocas empresas están implementando sistemáticamente estas buenas prácticas de ciberseguridad industrial.

IMPOSIBLE ASEGURAR LO QUE NO SE VE

Todo comienza con la visibilidad. Cada empresa debe tener un inventario actualizado de sus activos inteligentes para ganar visibilidad global. La mayoría de los sistemas industriales conectados en red han ido creciendo orgánicamente con el tiempo. Tal vez no se hayan diseñado pensando en los parámetros actuales y es posible que incluyan sistemas antiguos que se hayan utilizado durante mucho tiempo. Contestar a preguntas sencillas como si se dispone de un inventario de todos los activos inteligentes, cuál es el aspecto de la red OT, si el diseño de red cumple con las pautas de ciberseguridad actuales o si se monitoriza el tráfico de la red OT son claves para lograr una mejor visibilidad de los activos inteligentes.

PROTEGER LA RED

Para garantizar la ciberseguridad de una empresa, es necesario crear una red OT adaptada. Algunas cuestiones importantes que se deben tener en cuenta son: si hay algún sistema en funcionamiento que dependa de tecnología que ya no cuenta con el soporte del proveedor, si los sistemas operativos están actualizados (Windows, Linux), si se realiza una gestión activa de las revisiones, si se monitoriza e identifica el tráfico de red inusual o si se ha considerado combinar todos los activos en una plataforma virtual.

SEGURIDAD A LARGO PLAZO

Tomar medidas para respaldar estos dos factores clave de visibilidad y seguridad hará que la empresa esté mucho mejor preparada ante las posibles amenazas. Sin embargo, mantener este alto nivel de seguridad requiere un enfoque continuo. De hecho, estar a salvo hoy no significa estar a salvo mañana.

Establecer procesos de gestión simples para mantenerse al día, verificar los elementos agregados y eliminados en la red y evaluar regularmente la vulnerabilidad del sistema son tareas que deben convertirse en habituales para permanecer seguros. Pero incluso con un plan de acción que respete las mejores prácticas, los riesgos de seguridad no desaparecen, incluso si se han reducido considerablemente. Las amenazas "zero-day" que aún no se han identificado, pueden afectar la red por lo que es necesario estar preparado.

PLAN DE EMERGENCIA

¿Con qué debe contar una empresa para reducir la probabilidad y los efectos de la cibercriminalidad? Primero, es necesario localizar el ataque mediante un sistema activo de detección de amenazas en tiempo real para identificarlo y aislarlo, con un plan de recuperación de desastres o de incidentes y disponer de soluciones de salvaguarda y recuperación apropiadas.

SOCIOS DE CONFIANZA

Aunque ninguna de estas soluciones es difícil de implementar, es necesario contar con la experiencia adecuada para asegurar el entorno industrial. Y no es necesario que esta experiencia esté disponible internamente, lo que es demasiado costoso para muchas empresas. Con socios confiables, procesos operacionales y servicios de soporte *ad hoc*, una empresa puede protegerse eficazmente de las amenazas de ciberseguridad.

Es imprescindible tomar en consideración los riesgos de la ciberseguridad por lo que acudir a una compañía que comprenda estos riegos, diferentes a los del mundo IT, es fundamental.