“El verdadero desafío es que **cada vez más sistemas de tecnologías de operación** están conectados a redes **corporativas y externas”**

Entrevista a ***Alexandre Peixoto,*** Cybersecurity Expert for Control Systems (Emerson)

Para el experto, responsable de ciberseguridad de una de las empresas de automatización más grandes del mundo, ya no se trata de empresas grandes o chicas: todas son susceptibles de recibir ataques.

¿Qué es la ciberseguridad y por qué está creciendo en importancia en la industria de petróleo y gas?

La seguridad cibernética involucra la tecnología, las técnicas, los procesos y las estrategias que utilizan las entidades para proteger el acceso y la modificación de los sistemas electrónicos y la información sin permiso. Para implementar la ciberseguridad se requiere de una estrategia, y esta estrategia se aplica por medio de reglas o políticas y procedimientos, para que los usuarios puedan cumplir y seguir en consecuencia.

La estrategia recomendada para la ciberseguridad es la defensa en profundidad (*defense-in-deep*), que requiere de múltiples capas de protección, cada una dependiente una de la otra, para crear barreras cada vez más complejas, que eviten que un atacante obtenga acceso al sistema.

La seguridad cibernética está creciendo en importancia en todos los segmentos del mercado de control de procesos, no solo en petróleo y gas. Sin embargo, debido a la importancia de los bienes producidos por las compañías de hidrocarburos para personas de todo el mundo, los riesgos ambientales y de seguridad planteados por las operaciones energéticas, así como el papel esencial de esta infraestructura en las economías y naciones; esto aumenta la seguridad cibernética dentro de la industria de petróleo y gas. Pero de ninguna manera excluye otras industrias como las ciencias de la vida y los productos químicos que también priorizan la adopción de enfoques más ciberseguros para los sistemas de control y las tecnologías operativas.

Hasta ahora se realizaban ataques a la tecnología de la información (TI) y las comunicaciones. ¿Desde cuándo y cómo cree que comenzaron a involucrar a la Tecnología Operacional (OT)?

La seguridad cibernética ha sido común en los sistemas de TI durante mucho tiempo. El motivo principal de la temprana adopción de la ciberseguridad por parte de las TI se debe a la exposición de las redes corporativas, en particular las instituciones financieras, a Internet y a los sistemas conectados que brindan a sus usuarios un mayor acceso.

Tradicionalmente, los sistemas de OT se han aislado y controlado más, limitando las opciones de conectividad a lo que se necesita para respaldar el control y la supervisión del proceso. Muchos sistemas de control fueron "bloqueados por el aire", esencialmente desconectados de las redes externas, hasta hace muy poco tiempo.

Las interferencias son problemáticas porque obligan a que actualizar y agregar parches a los sistemas operativos y de control sean manuales y más difíciles, lo cual significa que algunas organizaciones ejecutan continuamente versiones de *software* inseguras u obsoletas.

Las necesidades comerciales actuales de OT están cambiando. Las nuevas tecnologías industriales de *Internet of Things* (IoT, Internet de las Cosas) crean oportunidades para mejorar la producción, el rendimiento y la rentabilidad mediante la conexión de datos del sistema de control a expertos remotos, servicios en la nube, dispositivos móviles y niveles superiores dentro de la organización. Con las nuevas oportunidades surgen nuevos riesgos y aumenta la necesidad de ciberseguridad.

Al mismo tiempo, las técnicas de piratería han evolucionado y se ha vuelto más fácil crear, obtener y explotar contra las redes de IT y OT. El verdadero desafío aquí es que cada vez más sistemas de OT están conectados a redes corporativas y externas; y las organizaciones aún se están ajustando a esta nueva norma que les exige mantener sus protecciones de seguridad cibernética al día.

Pero el desafío de la seguridad cibernética no debe evitarse, porque los beneficios de las nuevas tecnologías claramente superan el costo y las complejidades de mantener una posición fuerte en materia de ciberseguridad.

¿Qué áreas de la industria de O & G involucra principalmente? ¿Cómo pueden los piratas informáticos entrar en la red de OT? ¿Puedes dar ejemplos extremos del daño que los hackers pueden hacer en las empresas de O & G en todo el mundo (parada de la planta, daños al equipo, interrupciones de servicios públicos, cierre del círculo de producción, etc.)?

Una empresa puede convertirse en un objetivo por varias razones: las defensas inadecuadas, los materiales que produce y las relaciones geopolíticas son solo algunas.

Las empresas que se consideran parte de la infraestructura crítica de una nación tienden a ser más relevantes para este tipo de iniciativa ilegal. Sin embargo, según los estudios realizados por el Departamento de Seguridad Nacional de los Estados Unidos, una gran parte de los sitios afectados por amenazas de ciberseguridad vieron iniciados los ataques desde el interior de la instalación. Los datos continúan demostrando que incluso las medidas de seguridad más sofisticadas pueden volverse ineficaces por error humano o falta de conocimiento.

Aun así, estos riesgos pueden mitigarse fácilmente mediante un desarrollo y cumplimiento efectivos de políticas y procedimientos, como la implementación de políticas sobre el uso adecuado de medios extraíbles.

Figura 1. **Porcentaje de incidentes de Sistemas de Control Industrial 2014 y 2015 potencialmente mitigados por cada estrategia.**

En el informe del Departamento de Seguridad Interna (DHS, Department of Homeland Security DHS de los Estados Unidos llamado "Siete estrategias para defender los Sistemas de Control Industrial (ICS Industrial Control System)" (Figura 1)[1], los datos recopilados en 2014 y 2015 indicaron que las siete iniciativas cibernéticas clave que habrían evitado los incidentes informados son los siguientes:

1. Implementar listas blancas de aplicaciones.
2. Asegurar la configuración adecuada/administración de parches.
3. Reducir el área de superficie de ataque.
4. Construir un entorno defendible.
5. Administrar la autentificación.
6. Monitorear y responder.
7. Implementar acceso remoto seguro.

¿Las víctimas de estos ataques son solo grandes corporaciones o también han llegado a compañías medianas y pequeñas de O & G?

Nadie es inmune a la amenaza, y la amenaza nunca desaparece. Tenemos que estar al tanto de la ciberseguridad todos los días porque los "chicos malos" no van a desaparecer. Por ejemplo, estamos ante una "nueva normalidad".

Los sistemas de control son utilizados por todas las compañías de petróleo y gas. ¿Qué estrategia recomienda para protegerlos contra los ataques?

Recomendamos adoptar un enfoque basado en riesgo de ciberseguridad con una estrategia de defensa en profundidad.

La estrategia debe priorizarse en función del riesgo evaluado de las diferentes áreas de sus operaciones, y definir políticas y procedimientos que mantendrán a las protecciones de ciberseguridad para el control del sitio de producción, y los sistemas operativos para proteger las áreas de riesgo. Podemos ayudar a evaluar el riesgo de sus operaciones y sistemas e identificar problemas que deben resolverse y oportunidades de mejora. Al adoptar un enfoque basado en el riesgo, las organizaciones pueden identificar –y resolver más fácilmente– las vulnerabilidades potenciales que son más críticas para sus operaciones.

Empresas, como Emerson, ofrecen un conjunto de soluciones para abordar las necesidades de los clientes y sistemas de control seguros con protección, monitoreo y recuperación.

¿Los boardings de estas empresas tienen conciencia de la dimensión de este riesgo? ¿Cuáles son sus consejos para las empresas de hidrocarburos que aún no han entendido la gravedad de esta amenaza?

La seguridad cibernética es una iniciativa que lo incluye todo, y todos son responsables de ella: no importa quién es usted ni qué trabajo desempeña: puede afectar directa o indirectamente la ciberseguridad de un sistema.

La inquietud para mejorar la seguridad cibernética proviene, en la mayoría de los casos, de la alta gerencia de los sitios clave de producción, o de parte de equipos de toda la empresa que lideran los mandatos corporativos, para cumplir o superar los últimos estándares de ciberseguridad.

Cuando la presión por la seguridad cibernética no proviene de la parte superior, las inquietudes se inician desde sitios que han experimentado ciberataques recientes. De cualquier manera, la llamada a la acción consiste en tener un plan para mejorar la seguridad cibernética de los sistemas, y recomendamos encarecidamente realizar una evaluación de ciberseguridad que, alineada con un análisis de riesgos, pueda ayudar a priorizar una estrategia de mejora continua.

Referencias

1. https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf