JUAN IGNACIO GARCÍA

DIGITAL LEAD EN ABB ESPAÑA

"EN MATERIA DE CIBERSEGURIDAD, LAS VULNERABILIDADES SON EL PEOR ALIADO"

Redacción Industria Química

La ciberseguridad se ha convertido día a día en una de las claves de desarrollo para las compañías que conforman y compiten en el mercado actual. La firma ABB mantiene en su portafolio un amplio abanico de servicios que permiten cubrir todas las necesidades de ciberseguridad de una empresa, tal como el Digital Lead de esta compañía en España nos describe detalladamente en esta entrevista.

Ya es habitual leer en los medios de comunicación ciberataques a plantas de procesos industriales como el químico, ¿Cómo garantiza ABB la seguridad cibernética de sus clientes? ¿Qué servicios les ofrece?

Es difícil reconocer que todavía hay miles de sistemas en funcionamiento hoy en día sin ninguna seguridad básica. La ciberseguridad ha de tratarse como una prioridad de primer orden en la industria en general y particularmente en el sector químico. Es una tarea primordial concienciar a la alta dirección de invertir para proteger los activos de su sistema de control.

A medida que las tecnologías operativas (OT) se han ido exponiendo cada vez más a Internet, los procesos industriales se están viendo expuestos a las mismas amenazas de seguridad cibernética, como cualquier otro sistema en red. Esto en parte es porque los operadores han adoptado el mismo hardware, software, protocolos de red y sistemas operativos para ejecutar y conectar tecnologías comerciales cotidianas, como servidores, ordenadores y equipos de red.

Las soluciones de seguridad cibernética de IT tienden a centrarse en bloquear los datos cuando existe una amenaza. Esto tiene sentido si se trata de una base de datos (por ejemplo, de tarjetas de crédito), pero no funciona igual de bien si un *firewall* bloquea controladores lógicos programables (PLC), desde su posible apertura, al cierre de válvulas, en una fábrica de celulosa o en una refinería de petróleo.

En ABB protegemos los activos de nuestros clientes de la actual creciente cantidad de amenazas, a través de nuestro amplio portafolio de ciberseguridad, un conjunto de servicios estructurados en tres niveles progresivos, desde un Tier 1 o nivel básico a un Tier 3 o nivel experto en operaciones.

Nivel 1 – Inicio con las prácticas fundamentales de ciberseguridad.

- El Benchmark de Seguridad Cibernética ABB Ability

Es el punto de partida para nuestros servicios de ciberseguridad. Es un servicio con el que nuestros clientes recopilan datos de sus sistemas y los cargan en myABB / MCS para su análisis automatizado.

- Fingerprint:

Servicio que revela el estado de los indicadores clave de rendimiento (KPI).

Los datos recopilados por Benchmark de Seguridad Cibernética ABB Ability se compilan en un informe completo, donde se desglosan los diversos hallazgos y se proporcionan las recomendaciones.

- Risk assesment:

Evaluación de riesgos basado en IEC62443-3-2 (las versiones futuras pueden incluir ISO27000, NIST y otras metodologías). Este servicio clasifica el riesgo de cada componente en el sistema de producción evaluado.

- Servicio SUS (Security Update Service), para actualizaciones de seguridad.
- Malware Protection, como protección contra daños al software.
- Backup & Recovery & Verification.

Para los clientes que tienen un proceso manual o ningún proceso para mantener un inventario de activos de ciberseguridad. El inventario de activos de ciberseguridad automatiza el proceso de inventario para ahorrar tiempo, dinero y proporcionar visibilidad de los activos.

- Asset Inventory:

Automatiza el proceso de inventario de los activos de ciberseguridad y ahorra tiempo, dinero y proporciona una actualizada visibilidad de los activos.

- Analytics:

Recopila automáticamente datos del sistema y los compara con las mejores prácticas de la industria. Identifica, clasifica y ayuda a priorizar oportunidades para mejorar la seguridad general de los sistemas de control.

Nivel 2 - Servicios para clientes que han cubierto el Nivel 1 y desean externalizar su mantenimiento, configuraciones o requieren otros servicios más avanzados.

- Mantenimiento:

Con el servicio de mantenimiento cibernético de ABB nuestros clientes pueden externalizar el trabajo, asegurándose de que los controles de seguridad funcionen y se mantengan actualizados. El equipo de ABB también informa al cliente si sucedió algo y lo ayuda a remediarlo. El cliente recibe un informe mensual con métricas clave.

- Consultoría:

ABB ha trabajado con sistemas industriales y ciberseguridad durante muchos años, y hay pocos controles y soluciones de ciberseguridad con los que no hayamos trabajado. Nuestra capacidad para comprender tanto la producción como el proceso de los clientes, el sistema industrial y la ciberseguridad, nos convierte en la opción correcta para los proyectos de ciberseguridad. Podemos ayudar a seleccionar el producto de ciberseguridad más efectivo para el proceso, instalarlo de forma segura, redactar un procedimiento de ciberseguridad, auditar los sistemas, y mucho más.

Nivel 3 - Este nivel cubre las operaciones, con monitoreo de eventos 24x7, desde un centro experto en operaciones de seguridad (SOC).

- Operaciones colaborativas:

Para maximizar nuestra eficacia y capacidades de ciberseguridad, hemos creado los servicios de operaciones colaborativas. Con nuestros compañeros expertos en ciberseguridad industrial en todos nuestros centros de operaciones colaborativas en todo el mundo, podemos proporcionar servicios de ciberseguridad muy avanzados para nuestros clientes industriales. Monitoreo de eventos, inteligencia de amenazas caza de amenazas, etc.

Esta estructura de servicios permite a nuestros clientes administrar su seguridad conforme a su situación, mientras les permite adoptar nuevas soluciones y otros servicios digitales más avanzados.

¿Qué solución dentro del portafolio de ABB en relación con la ciberseguridad considera más novedosa?

Todas las soluciones y servicios digitales de nuestro portafolio tienen un alto componente de innovación con respecto al mercado. En materia de ciberseguridad, las

» ABB recopila y analiza toda la información existente, tanto a nivel cuantitativo como cualitativo, desde los aspectos organizativos a la propia arquitectura del sistema, o desde las propias características de los equipos y sus funciones, hasta las políticas corporativas

vulnerabilidades son el peor aliado. Nuestro despliegue internacional y nuestra experiencia de más de 30 años como líderes en sistemas de control industrial, junto a la estrecha colaboración en el día a día con nuestros clientes y *partners*, nos posibilita conocer de primera mano sus necesidades, sus objetivos más actuales, y poder ofrecerles las soluciones más vanguardistas.

¿Cómo es el proceso de implementación de soluciones de ciberseguridad en las plantas de procesos industriales?

Cuando hablamos de ciberseguridad, no se debería menospreciar ningún aspecto, ni a nivel cuantitativo ni cualitativo. Cada cliente, cuando afronta la implementación de soluciones de ciberseguridad, debe conocer su situación de partida, cuáles son sus vulnerabilidades y contar con un programa estructurado para planificar su implantación.

La complejidad es distinta en cada compañía, y, aunque el sector de actividad sea el mismo, en cualquier empresa coexisten multitud de aspectos a tener en cuenta: desde las políticas de empresa, sus propias metodologías de trabajo, la normativa vigente, su base instalada de equipos y de aplicaciones informáticas, sus topologías de redes de comunicación, sistemas, control, operaciones, arquitecturas, etc., todo un extenso e importante ecosistema en donde todos sus integrantes son fundamentales; por ello debe ser analizado en detalle, como primer paso.

Bastaría con hacernos una batería de diez preguntas para autoevaluar nuestro nivel de riesgo:

1. ¿Formas regularmente a tus empleados en ciberseguridad?
2. ¿Tienes una lista completa de activos cibernéticos?
3. ¿Has realizado una evaluación de riesgo operacional?
4. ¿Has realizado una evaluación de seguridad cibernética?
5. ¿Has implementado una red adecuada de segmentación?
6. ¿Has implementado herramientas que permitan prevenir los riesgos del trabajo remoto, actualizando firmas a diario?
7. ¿Parcheas tus sistemas de forma regular? ¿Con qué periodicidad de tiempo
8. ¿Estás supervisando los registros de tu sistema? ¿Y los de tráfico de red?
9. ¿Tienes una copia de seguridad de todos tus activos, como switches, routers, firewalls, programas de los controladores (PLC), de las unidades terminales remotas (RTU), dispositivos electrónicos inteligentes (IED) y del resto activos de control digital, a través de un archivo de configuración?
10. Si tu sistema se viera atacado hoy, ¿tendrías preparado un plan de recuperación y de respuesta?

Si en tus respuestas hay más "noes" que "síes" a estas preguntas, significa que necesitas prepararte en materia de ciberseguridad.

En este nivel básico, si no tienes la red adecuada de segmentación, software del sistema actualizado, protección *end-point*, sistemas de protección y hardend, entonces puedes sentirse afortunado de que tu sistema no haya sido aún comprometido.

Hay que resaltar que, para nosotros, entender la situación actual de partida es clave para identificar "dónde, quién, cómo y cuándo" aplicar las soluciones y servicios específicos de ciberseguridad.

Desde ABB y para cada uno de nuestros clientes, recopilamos y analizamos toda la información existente (información más general a la más técnica y comprometida), tanto a un nivel cuantitativo como cualitativo, desde los aspectos organizativos a la propia arquitectura del sistema, o desde las propias características de los equipos y sus funciones, hasta las políticas corporativas; siempre con el aseguramiento del cumplimiento del marco normativo vigente, tanto en arquitecturas de referencia como en el tratamiento toda la información. Priorizamos actuaciones y damos soporte 24h. desde nuestros centros de excelencia operativa.

En los últimos años ABB ha firmado algunos acuerdos estratégicos como la alianza mundial de ciberseguridad para la tecnología operativa. ¿Qué supone esta alianza para ABB y qué beneficios aporta a sus clientes?

Sí, es cierto. ABB se adhirió recientemente a la Operational Technology Cyber Security Alliance (OTCSA), una alianza para la ciberseguridad de la tecnología operativa, en cuanto a las brechas de seguridad para la OT, así como infraestructuras críticas y sistemas de control industrial. Para fundar la OTCSA se han aliado con ABB

destacadas empresas de la industria: Check Point Software, BlackBerry Cylance, Forescout, Fortinet, Microsoft, Mocana, NCC Group, Qualys, SCADAFence, Splunk y Wärtsilä.

La OTCSA tiene cinco objetivos clave: primero, reforzar posturas respecto al riesgo ciberfísico de los entornos de OT e interfaces para la interconectividad de OT/IT; segundo, servir de guía a los operadores de OT sobre cómo proteger sus infraestructuras basándose en un proceso de gestión de riesgos y en arquitecturas/diseños de referencia que cumplan de manera demostrable normativas y estándares internacionales, como la IEC 62443; tercero, servir de guía a los proveedores de OT en relación con arquitecturas de sistemas seguras, con interfaces y funcionalidades de seguridad; en cuarto lugar, apoyar la adquisición, desarrollo, instalación, operación, mantenimiento e implantación de una infraestructura crítica más segura y protegida, y, por último pero no menos importante, acortar los plazos necesarios para la adopción de infraestructuras críticas más seguras y protegidas.

ABB dispone de centros de operaciones colaborativas alrededor del mundo para monitorización y soporte continuo 24/7. ¿Podría explicar el funcionamiento de estos centros y qué aporta a sus clientes?

Sin lugar a dudas, las tecnologías digitales han llegado resolver los problemas e incidencias que se presentan en la operación y mantenimiento de las plantas industriales, independientemente del tipo de industria. La digitalización y la creación de nuevos servicios de atención remota ahorra ingentes cantidades de dinero, dota de alta eficiencia todas las tareas necesarias para la resolución del problema y permite un nivel de colaboración y transferencia de conocimiento entre nuestros expertos que prestan el servicio y nuestros clientes.

Nuestros Centros de Operaciones Colaborativas, repartidos estratégicamente por todo el mundo, prestan servicios a nuestros clientes en tiempo real gracias a la aplicación de innovadoras tecnologías digitales para la resolución de las incidencias. Estos centros proporcionan información relevante a nuestros clientes para que puedan incrementar su rentabilidad y su productividad, mejorando el rendimiento de sus instalaciones y consiguiendo una mayor seguridad, menores riesgos y costes más bajos.

Hablando por último de servicios avanzados, ¿cuál es la tendencia y cuáles son los servicios avanzados más demandados en las plantas de procesos industriales químicas?

La seguridad cibernética para sistemas de automatización y control, y en particular para las infraestructuras críticas, es algo cada vez más prioritario en todos nuestros clientes.

Nuestras soluciones mitigan los posibles riesgos, proporcionan confianza a los clientes y aseguran el cumplimiento de la normativa vigente y políticas existentes. Ofrecemos una amplia gama de soluciones de seguridad que minimizan riesgos cibernéticos y proporcionan el más alto nivel de protección para la automatización. Además, es importante destacar que en ABB abordamos la ciberseguridad a lo largo del ciclo de vida, tanto de los sistemas como de los datos, y desde su diseño y desarrollo, pasando por su mantenimiento hasta llegar a las operaciones

Como ya he mencionado anteriormente, en ABB disponemos de un portfolio de gran valor añadido, desde los dispositivos, sistemas, soluciones, servicios que permiten a nuestros clientes conocer más, hacer más y ejecutarlo mejor, de manera colaborativa con ABB. Desde los dispositivos hasta la nube. Todo nuestro portafolio de servicios digitales está creado con el foco puesto en la seguridad de las personas y de los activos, en la fiabilidad y calidad de las operaciones y en la optimización de la producción.

Para este cometido utilizamos nuestra plataforma ABB Ability, plataforma en constante desarrollo e innovación que actualmente cuenta con más de 200 soluciones digitales multisectoriales que permiten a nuestros clientes saber más sobre sus propias instalaciones, optimizar su producción e incrementar la seguridad en sus operaciones y procesos.