STORMSHIELD

ARTÍCULOS DE OPINIÓN

EMPRESAS INDUSTRIALES: LA SOBERANÍA, COLUMNA VERTEBRAL DE SU ESTRATEGIA DE CIBERSEGURIDAD OT

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Hoy en día, los ciberdelincuentes apuntan cada vez más al sector industrial, y sus ataques tienen consecuencias de gran alcance. Sin embargo, esto no solo afecta a los operadores de vital importancia y a los servicios esenciales: la preocupación es común. Además de las regulaciones que "obligan" a algunos a elegir soluciones soberanas, los actores industriales tienen la responsabilidad de aplicar estas mismas normas y actuar a lo largo de la cadena de seguridad. Pero, ¿por qué es tan importante este concepto de soberanía? Columna de invitados de Vincent Nicaise, Jefe de Asociaciones Industriales de Stormshield, y Yoann Delomier, Jefe de Equipo de OT, Wallix.

Los nuevos usos de la tecnología digital en la industria en los últimos años han contribuido en gran medida al desarrollo y a la modernización de dicho sector. Y ha sido así no solo en términos de rendimiento y competitividad en un momento de fuerte globalización, sino también en lo que respecta al cuidado del medio ambiente y a la trazabilidad con respecto a los consumidores y a la normativa europea.

Sin embargo, estas nuevas prácticas han generado que el mundo industrial esté cada vez más expuesto a los riesgos cibernéticos. Por ejemplo, los operadores de infraestructuras críticas (transporte, energía, agua, etc.) llevan a cabo procesos industriales que utilizan datos que circulan -a veces sin cesar- en tiempo real, y que se exponen ahora a ataques desde múltiples direcciones. Igualmente, y, de forma más general, todos los puntos de entrada están siendo explotados por hackers cada vez más profesionales, cuyos objetivos incluyen el espionaje industrial y la detención de la producción para exigir rescates o con fines políticos. Y dado lo que está en juego a nivel financiero, humano y medioambiental, el sector industrial tiene un fuerte incentivo para pagar...

A tenor de esta realidad, y de los crecientes ciberataques que sufren estas infraestructuras críticas, la protección de las empresas industriales, que garantizan la seguridad de los bienes y las personas, debe ser una obligación. No obstante, los actores industriales no siempre dan prioridad a las consideraciones de ciberseguridad cuando elaboran sus planes de modernización, y es un tema crítico que debería aplicarse a la hora de diseñar los proyectos de TI/OT, con el fin de garantizar una seguridad óptima de los procesos. Y la soberanía de las soluciones de ciberseguridad es crucial en estas consideraciones.

LA CONFIANZA: PRINCIPAL CRITERIO PARA ELEGIR LAS SOLUCIONES DE CIBERSEGURIDAD

Elegir soluciones de ciberseguridad soberanas significa, ante todo, garantizar la transparencia y evitar cualquier riesgo de que los datos puedan ser explotados con fines maliciosos. Esta es la única manera de garantizar una defensa en profundidad sin eslabones débiles, y evitar cualquier riesgo de interferencia o espionaje industrial, como se ha visto recientemente con el grupo de hackers chino Winnti, que fue citado en una investigación por haber llevado a cabo una importante operación de espionaje en Estados Unidos, Europa y Asia en nombre del Estado chino.

Mantener la independencia digital es también el único modo de permitir una respuesta local y autónoma con respecto a los problemas de producción y las actividades críticas cuando se resuelven incidentes cibernéticos; por ejemplo, con el fin de minimizar las interrupciones de la producción. Las soluciones europeas son capaces de ofrecer esta respuesta local en términos de soporte técnico rápido, asistencia a los equipos locales, o procesos de respuesta a incidentes.

Y, por último, la elección de soluciones soberanas también garantiza el cumplimiento nativo de la normativa y los estándares vigentes. Esto se traduce en requisitos normativos para ofrecer un acceso seguro a los sistemas de información y a los sistemas operativos (autenticación, segmentación, trazabilidad de los datos, cifrado, etc.).

En resumen, se necesitan soluciones europeas más fiables. Sobre todo, porque, dada la proliferación de centros de producción en todo el mundo, las fronteras ya no son un problema cuando se ataca a una empresa industrial europea.

INVERTIR EN LÍDERES EUROPEOS EN CIBERSEGURIDAD INDUSTRIAL: UN ENFOQUE RESPONSABLE Y CON CONCIENCIA SOCIAL

Para que la industria pueda tomar las decisiones correctas, los principales proveedores de soluciones de ciberseguridad europeos disponen de varias herramientas para construir un entorno fiable y resistente. La primera de ellas es ampliar la gama de soluciones de protección disponibles a nivel local, garantizando que los clientes finales tengan la posibilidad de elegir una solución soberana como mínimo. Esto va de la mano de la labor de concienciación de los fabricantes industriales en la implementación de componentes de seguridad soberana en el diseño de sus productos.

De manera más general, es importante apoyar a las empresas de nueva creación y al ciber-sector a través de las organizaciones nacionales, la inversión en la ciber-economía local a través de fondos específicos y la educación. Estas son las condiciones para que las empresas se instalen en Europa y se queden allí, y también para mantener y desarrollar la experiencia europea.

Con la implicación de todo el ecosistema y una cooperación eficaz entre los actores europeos, será posible aumentar el control soberano en la industria, garantizando al mismo tiempo una protección óptima de nuestra economía, de los ciudadanos y del medio ambiente.