Las defensas industriales necesitan refuerzos

La empresas no recibe ataques informáticos aleatorios, sino dirigidos y bien planificados. La ciberseguridad exige personal especializado tanto en los procesos industriales como en su seguridad

Pura C. Roy

El primer Congreso Español sobre Ciberseguridad Industrial, celebrado recientemente en Madrid, analizó qué repercusión puede tener para las organizaciones industriales una intrusión en sus sistemas de automatización y control, y dio las claves para estructurar un entorno industrial ciberprotegido. Organizado por Logitek e Intermak Tecnologías, contó con la participación de más de 100 profesionales de la industria interesados en conocer las claves para dotar sus sistemas de fabricación o de gestión de infraestructuras de la robustez necesaria para operar de forma segura en un entorno cada vez más conectado.

A este mundo de redes debe adaptarse una industria que ha tenido sistemas cerrados y, por ello, vigilados por ingenieros y técnicos, pero que no escapa ya a sistemas más abiertos de trabajo y, por tanto, más susceptibles de ser objeto de intrusiones no deseadas que pueden producir consecuencias tangibles como pérdidas de producción, daños medioambientales o peligros para la salud pública, lo que puede reducir la producción y del prestigio.

El cambio de paradigma en la industria como en otros ámbitos se está dando con las tecnologías de la información (TI). El problema para la industria es que las TI han evolucionado muy rápidamente y han entrado en el entorno de los sistemas de control y el personal de planta no está formado adecuadamente en las nuevas tecnologías. Muchas veces ni siquiera es consciente de que existan problemas y, por otro lado, el personal de las TI desconoce los sistemas de la planta. Tiene la sensación de que es algo fuera de su ámbito, aunque la frontera sea cada vez más difusa.

Protocolos

Los dispositivos industriales han heredado los problemas de las TI. Los sistemas de control ya no están aislados. Han pasado de utilizar líneas serie dedicadas a utilizar líneas Ethernet o wifi compartidas. Los protocolos de comunicación industriales empiezan a funcionar sobre TCP/IP. Los dispositivos industriales tienen sistemas operativos de propósito general.

Por todo ello, para Javier Larrañeta, secretario general de la Plataforma Tecnológica Española de Seguridad Industrial (PESI), que abrió la sesión, se mostró categórico a la hora de hacer un análisis de la situación de la seguridad en la industria: "Pese a que está ampliamente extendido en la sociedad y las organizaciones la consolidación de la seguridad física, laboral, privada e incluso una incipiente ciberseguridad, la seguridad integral, entendida como el sistema inmunológico de la organización que abarca transversalmente todas las áreas, no es una apuesta estratégica de las empresas españolas". En ese sentido, superar esta visión atomizada de la seguridad y el establecimiento de buenas prácticas darían a la industria las herramientas necesarias para protegerse.

Foto: Logitek

Samuel Linares, director de servicios de ciberseguridad de Intermark Tecnologías, explicó que se está produciendo un *tsumami:* "La convergencia entre los mundos físico y *cíber* es cada vez más estrecha". Las consecuencias negativas de esta evolución tienen múltiples formas: acceso no autorizado (robo o mal uso de información confidencial, publicación de información en lugares no autorizados) hasta la pérdida de integridad o disponibilidad de los datos del proceso o de la información de producción con perjuicios como la denegación de servicio, la pérdida de capacidad de producción, la inferior calidad de productos, las averías en el equipamiento, riesgos de salud pública o, incluso, pérdidas humanas y amenazas a la seguridad de la nación.

El 85% de los ataques tardan semanas en descubrirse y esto reduce la capacidad de reacción

Las amenazas de virus como Stuxnet y Flame, que son las más famosas, van en aumento y cada vez son más sofisticadas. Stuxnet fue la primera ciberarma dirigida al sector industrial, descubierta pronto quizá porque infectó más PC de los previstos. Fue más allá de su "trabajo" de retrasar el programa nuclear iraní. Salió a la luz en junio de 2010, aunque, en realidad, este programa malicioso ya estaba funcionando un año antes.

El 85% de los ataques necesitan semanas o más para descubrirse, lo que dificulta enormemente la capacidad de reacción ante ellos. Por eso, se necesita romper la cadena del ataque antes de que el adversario pueda ejercer el control sobre alguno de los activos y realizar un sabotaje. Algunos virus pueden estar activos entre cinco y ocho años.

Al pasar, por la irrupción de Internet, de estándares propietarios a estándares abiertos, se permite que estos *malware* complejos avancen. Según Xavier Cardeña de Logitek, más de la mitad de las vulnerabilidades se encuentran en el nivel de supervisión. Para resolverlas, dio detalles acerca de cómo es posible proteger algunos de los sistemas industriales más vulnerables frente a un ciberataque con *firewalls* embebidos para proteger el acceso a dispositivos de la zona de control, considerar la utilización de protocolos industriales que incluyen la autenticación basándose en estándares existentes, uso de redes inalámbricas seguras como TETRA, o la evolución desde OPC a OPC UA son algunas de las soluciones que planteó.

El 'firewall' y otros mitos

Quizás uno de los mayores errores de las empresas industriales, según detalló Rens de Wolf, de Fox-IT, es creer que son imbatibles. Mitos como "nuestros *firewalls* nos protegen automáticamente", "los procesos de control están asilados de otras redes" llevan a una situación de desprotección a las empresas que puede tener devastadoras consecuencias. Para el experto, la respuesta está en desplegar medidas críticas de protección donde los errores de indefensión son inaceptables (niveles de 0 al 3 de ISA-99), además de la utilización dispositivos y soluciones de alta seguridad.

Durante la jornada, E.on y Metro de Londres explicaron cómo gestionan su entorno de ciberseguridad. En el caso de la empresa eléctrica, una de sus plantas de generación de ciclo combinado, ubicada en Suecia, cuenta con un sistema basado en tecnología de industrial Defender, que incluye la integración de todos los dispositivos de las instalaciones con el fin de tener un total control sobre las amenazas. En el caso del suburbano británico, el entorno de ciberseguridad abarca los sistemas de control de señalización, control de potencia, gestión de las comunicaciones y los responsables de la gestión de las estaciones. La estructuración de redes cerradas, la circulación de datos de manera unidireccional, el diseño de zonas "desmitarizadas" o *gateways* unidireccionales son las bases de un sistema que les permite ofrecer plenas garantías de seguridad.

"Los planes de seguridad deben basarse en un análisis de riesgos para actuar y tener en cuenta la prevención, la detección y la reacción", recomendó Carmelo Zerpa, consultor senior de Seguridad de Tecnocom.

Bioplásticos, una de las grandes apuestas de la industria europea

Su polivalencia los consolida como materia prima alternativa a las convencionales derivadas de fuentes no renovables

Foto: European Bioplastic

La producción mundial de bioplásticos rozará los seis millones de toneladas en 2016. Estas son las últimas previsiones efectuadas por la asociación European Bioplastics con la ayuda del Instituto para Bioplásticos y Biocomposites de la Universidad de Hannover. Los incrementos más importantes se registrarán en los no biodegradables. Sobre todo, en las soluciones denominadas *drop-in,* de bioplásticos a granel como el PE y el PET, que, básicamente, se diferencian de sus equivalentes convencionales en la fuente base de material renovable o procedente de la naturaleza.

Por otra parte, también los plásticos biodegradables crecen. Así, según European Bioplastics, su capacidad de producción se incrementará en dos tercios para 2016. Como asegura su director general, Hasso von Pogrell, los líderes que contribuirán al crecimiento de este grupo serán el PLA y el PHA, con capacidades productivas de 298.000 toneladas (+50%) y 142.000 (+550%) toneladas, respectivamente.

La I+D en este campo es constante. Científicos europeos han creado nuevos materiales compuestos nanoestructurados que combinan bioplásticos y fibras de celulosa para su uso en una amplia variedad de industrias como las del embalaje, el transporte, la construcción, el juguete, el menaje y las artes gráficas. Para obtener prestaciones similares a las de los materiales no renovables, los investigadores del proyecto SustainComp han recurrido a la generación de nuevos materiales a través del uso de nanotecnología. SustainComp es un proyecto coordinado por la compañía sueca de investigación Innventia.

Desde el Centro Fedit Itene (Instituto Tecnológico del Embalaje, Transporte y Logística) se ha trabajado conjuntamente con la empresa italiana Novamont y con Innventia en la evaluación de la sostenibilidad de los nuevos materiales desarrollados para diferentes aplicaciones tales como un sistema de amortiguamiento para aparatos electrónicos, un componente de asiento para autobuses urbanos, bloques para juguetes, un panel *display* para aplicaciones de publicidad y un *set* de cubiertos para *catering*.

Ventajas ambientales

Los resultados de la evaluación de los nuevos materiales, según Itene, confirmaron la mejora ambiental sobre algunos efectos tales como el cambio climático, o la disminución de recursos no renovables. En el caso de su desarrollo industrial se espera que estos materiales sean económicamente competitivos, si se tiene en cuenta un escenario futuro en el que se produzca un incremento del precio del petróleo y la implementación de políticas ambientales más restrictivas en muchos países.

Por ejemplo, la sustitución de las fibras de vidrio por las fibras de madera es clave para el éxito de la aplicación del componente de asiento para autobús urbano (aplicación duradera), mientras que la recuperación a través del reciclado orgánico es la característica que marca las diferencias para la aplicación del *set* de cubiertos biodegradables (aplicación desechable).