Ignacio Álvarez Vargas

Director del Área de Sistemas de Comunicación y Ciberseguridad Industrial de Siemens España

"Sería necesaria una nueva especialidad universitaria para profesionales en ciberseguridad industrial"

Mónica Ramírez

Ignacio Álvarez Vargas (grado de ingeniería en electrónica industrial y automática e ingeniero industrial en la especialidad de organización industrial) es el director del Área de Sistemas de Comunicación y Ciberseguridad Industrial de Siemens España y presidente de la Asociación española de PROFIBUS, PROFINET e IO-Link. Los últimos 25 años su vida profesional han estado relacionados con la automatización industrial y, concretamente, con las comunicaciones industriales.

Ignacio Álvarez Vargas.

La industria 4.0 afecta a toda la cadena de valor industrial y cada vez existe una mayor conectividad de las máquinas y las plantas. En consecuencia, ¿qué nuevos riesgos han aparecido?

La industria 4.0 y la transformación digital en las organizaciones industriales están provocando un aumento de las necesidades de conectividad tanto horizontales (comunicación entre líneas o máquinas) como verticales (entre máquinas y sistemas de gestión de la producción) en las instalaciones industriales. A su vez, también ha aumentado la necesidad de conectividad remota a través de Internet para ofrecer servicios de mantenimiento y captación de información de las máquinas. Esta situación puede aportar numerosas ventajas y mayor flexibilidad, pero también conlleva la aparición de nuevos riesgos que deben ser gestionados adecuadamente adoptando las medidas de protección adecuadas.

Las empresas industriales deben adoptar modelos de protección y defensa, ¿cuáles son los más habituales?

Para encarar esta realidad con éxito, las empresas deben adoptar un modelo de protección para asegurar la disponibilidad y la resiliencia de las instalaciones. Uno de los modelos de protección más utilizados es el llamado modelo de defensa en profundidad (defense in depth en inglés). Este modelo ofrece una excelente protección con la que se consiguen unas ratios de protección muy altas. El modelo está basado en tres pilares: seguridad de planta, seguridad de red e integridad del sistema; y nace a partir de las recomendaciones del conjunto de normas ISA 99 y el estándar desarrollado a partir de estas: IEC 62443, que es el estándar en seguridad en los sistemas de control industrial.El primer pilar concierne a la seguridad de planta, que utiliza una serie de métodos de protección para evitar que personas no autorizadas obtengan acceso físico a componentes críticos. Esto comienza con el control del acceso a edificios convencionales y se extiende hasta la protección de áreas sensibles por medio de sistemas de seguridad en las instalaciones. El segundo pilar versa sobre la seguridad de la red, cuya misión principal es proteger las redes de control frente a accesos no autorizados e incidentes. Esto incluye la vigilancia de todas las interfaces como las de la red de planta y el acceso de mantenimiento remoto mediante Internet. Suele realizarse mediante técnicas de segmentación de red, mediante *firewalls* o creando una "zona desmilitarizada" (DMZ) protegida. Además, es recomendable la transmisión de datos encriptados usando una red privada virtual (VPN) para proteger las instalaciones del espionaje y de la manipulación de los datos. Finalmente, el tercer pilar es la salvaguarda de la integridad del sistema. Aquí se hace hincapié en la protección de los sistemas de automatización y los componentes de control, así como los sistemas SCADA y HMI contra el acceso no autorizado y el cumplimiento de requisitos especiales como la protección de conocimientos técnicos. Además, la integridad del sistema también implica la autenticación de los usuarios, las autorizaciones de acceso y cambio y el *hardening* del sistema, es decir, la robustez de los componentes contra los ataques. Adicionalmente, me gustaría recalcar la importancia de concienciación de las personas.

¿Cuáles son los riesgos de usar una red pública como Internet para el acceso remoto a instalaciones industriales?

La utilización de redes públicas, como Internet, para realizar accesos remotos a las plantas conlleva una serie de riesgos que pueden ser mitigados adoptando las medidas de protección necesarias. Es indispensable utilizar protocolos de seguridad robustos para encriptar las comunicaciones, como los túneles VPN basados en estándares reconocidos: IPSec e OpenVPN. Por otro lado, los dispositivos que se utilicen como puntos finales deben estar preparados para trabajar en un entorno industrial y, por supuesto, deben estar adecuadamente configurados a nivel de *firewall* en función de la aplicación en la que estén trabajando. Por otro lado, es recomendable utilizar sistemas de gestión de conexiones remotas seguras, capaces de gestionar todos los usuarios los dispositivos de manera centralizada, esta-

bleciendo los permisos adecuados para cada usuario y la posibilidad de activar y desactivar dichas conexiones seguras a voluntad desde este sistema de gestión.

¿Qué papel deben desempeñar los fabricantes de tecnología industrial en el marco de la ciberseguridad industrial?
Los fabricantes de tecnología industrial deben adaptarse a los requerimientos actuales dentro del nuevo escenario. Es necesaria una inversión en I+D para dotar a los sistemas de control industrial de la mayor integridad del sistema posible teniendo en cuenta los nuevos riesgos emergentes en cuanto a ciberseguridad. Es necesario dotar de nuevas funcionalidades de seguridad a los sistemas de control estándar para protegerlos ante un intento de acceso no deseado y evitar, por ejemplo, que un atacante consiga información sobre datos de producción o que un *man-in-the-middle* modifique el valor de consigna de una máquina o que un ataque de denegación de servicio (DoS) me inhabilite la disponibilidad de la instalación. También es necesario diseñar nuevos productos dedicados a la protección de redes industriales y específicamente diseñados para participar en un sistema de automatización.

¿Qué consecuencias puede tener un ciberataque para una empresa?
Esta pregunta no es fácil de contestar en pocas líneas, ya que las repercusiones pueden ser múltiples, dependiendo de que el ataque sea dirigido (como Industroyer: interrupción del suministro de energía en Ucrania) o sea un ataque no dirigido (como Wannacry) o qué fin persiga conseguir el atacante: desde los que quieren robar dinero, a los que quieren arruinar nuestra reputación, pasando por los que usan las vulnerabilidades como armas. En cualquier caso, las principales consecuencias van a ser casi siempre las siguientes: pérdida de la propiedad intelectual implementada en estos sistemas y máquinas, privación de la disponibilidad y de la productividad de la planta industrial, pérdida de la integridad de los productos acabados en sí misma y pérdida de la reputación de las compañías.

¿Qué diferencias hay entre la ciberseguridad en la red OT (red industrial) y en la IT (red corporativa)?
Las redes de comunicación industrial (OT) y empresarial o corporativa (IT) son considerablemente distintas, y sin embargo tienen una cosa en común: su conexión segura es decisiva para crear valor añadido en una empresa (especialmente en la era del Big Data y el aumento del volumen de datos). Solo aquellos que entiendan las necesidades de las redes IT y de las redes industriales pueden establecer una conexión confiable y mantener las comunicaciones funcionando. La comunicación se configura de forma diferente para cada una de las dos redes: mientras que la tradicional red IT transmite telegramas, la comunicación industrial se centra en aplicaciones, buscando adicionalmente tiempos de transmisión óptimos. Por tanto, los componentes de red y las topologías de ambas deben adaptarse a los respectivos requisitos. Un equipo terminal en la oficina, por ejemplo, generalmente se comunica con uno o más servidores, la topología de red es vertical y está diseñado para un mayor ancho de banda. Si un cliente falla de forma esporádica, generalmente no tiene un impacto en el negocio y, por tanto, no son considerados críticos.

> "El perfil de especialista en ciberseguridad implica un gran conocimiento del mundo IT y del de la automatización industrial, y especialización en redes industriales"

Sin embargo, en la automatización, el foco de la comunicación es la comunicación máquina a máquina (M2M) y es diferente: un intercambio de datos integrado (sin pérdidas, ni retrasos) es un requisito previo vital para evitar paradas en la producción y, en consecuencia, en la planta, las cuales originan elevadas pérdidas financieras. Todos los equipos requieren un intercambio de datos continuo. Por esta razón, la transmisión de datos en las comunicaciones industriales debe ser realizada y completada dentro de un tiempo de respuesta definido (o lo que es lo mismo debe ser determinista).

¿Cómo deben actuar las organizaciones industriales cuando sufren incidentes de ciberseguridad?
Antes de contestar a la pregunta, me gustaría alabar la gran labor que están haciendo en este campo, tanto el CNPIC, como INCIBE y, por ende, el CERT de Seguridad e Industria, en el campo de respuesta a incidentes de ciberseguridad a nivel nacional. Mi recomendación comenzaría en momentos anteriores a sufrir un incidente de seguridad, ya que cualquier tipo de empresa, y más en concreto empresas vinculadas a sectores industriales, deberían tener implementado e implantado un plan de contingencia frente incidentes de ciberseguridad y continuidad de negocio. Una vez sufrimos el incidente, el trabajo estaría en su gran medida procedimentado y lo único que deberíamos hacer es seguir el plan y contactar con el CERT de referencia. En caso de la industria nacional, ya sea considerada infraestructura crítica o no, sería el CERTSI, a través de sus diferentes canales. Además, INCIBE, a través de su web, tiene diversos recursos para su público objetivo que puede facilitar el conocimiento y la realización de procedimientos para actuar en estos casos.

El puesto de especialista en ciberseguridad es una de las nuevas profesiones emergentes más demandadas, ¿qué perfil profesional ha de tener?
Realmente es un puesto muy demandado y hay muy pocas personas preparadas para él. Mi recomendación pasaría por los siguientes puntos: gran conocimiento del mundo IT y del de la automatización industrial, y especialización en redes industriales y ciberseguridad industrial.

¿Qué papel pueden desempeñar los ingenieros técnicos industriales y graduados en ingeniería de la rama industrial en el campo de la ciberseguridad?
Tendrían parte de la formación necesaria para el puesto. Desde mi punto de vista, sería necesaria una nueva especialidad dentro de las universidades que estuviera orientada a formar profesionales en el campo de la ciberseguridad industrial.

¿Cómo se imagina el sector de la ciberseguridad dentro de 10-15 años?
Debido a que las empresas están cada vez más expuestas a una creciente fuente de riesgos como criminales, *hackers*, agentes estatales y competidores desleales cada vez más sofisticados en el aprovechamiento de las vulnerabilidades de las modernas tecnologías, creo que el sector de la ciberseguridad continuará con su auge ascendente tanto a corto, como a medio y largo plazo.