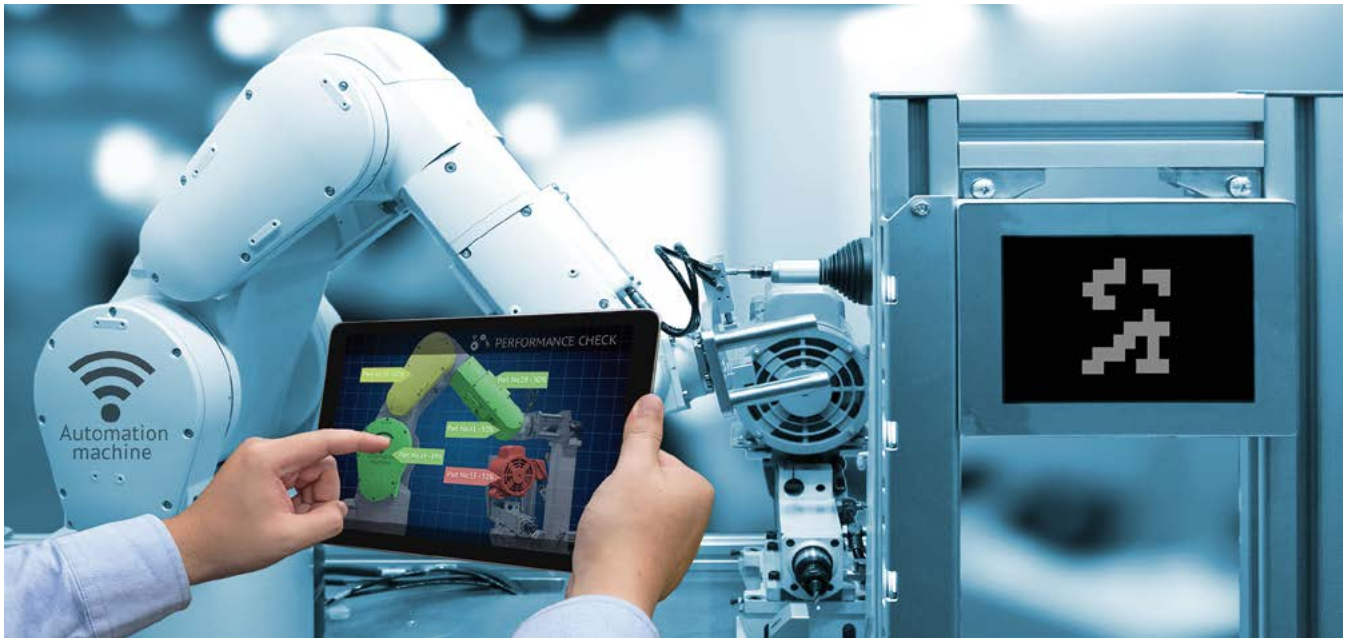

Foto: Zapp2Photo / Shutterstock.

La brecha de seguridad del internet industrial

La consolidación del internet industrial de las cosas, que da a las empresas industriales más flexibilidad e ingresos, está limitada si las organizaciones no mejoran la seguridad frente a los ciberataques

Joan Carles Ambrojo

Los principales beneficios del internet industrial de las cosas (*Industrial Internet of Things, IIoT*, en inglés) son lograr mayor eficiencia, generar nuevas fuentes de ingresos y dotar a las empresas de una mayor flexibilidad. Estos logros requieren la digitalización de sistemas industriales, la interconexión de activos operacionales y empresariales y mayor integración con entidades externas. Pero sin una seguridad adecuada, los dispositivos conectados de las industrias no son fiables, lo que supone un gran riesgo para las organizaciones e incluso los usuarios. Los expertos demandan realizar una implementación adecuada de la seguridad para contrarrestar las crecientes y cambiantes amenazas que están surgiendo.

En el contexto de la fábrica 4.0, hacia donde los nuevos métodos de producción se dirigen, el Internet industrial es una infraestructura en continuo desarrollo. Está construido en distintas etapas sobre una maquinaria que, en su gran mayoría, no había estado previamente conectada a la red. El denominado ecosistema IIoT está compuesto por una creciente legión de dispositivos interconectados, desde sensores hasta sistemas de automatización, que se están introduciendo de forma paulatina en áreas como el mantenimiento, el seguimiento y el control de fabricación. Estos equipos recolectan y transmiten ingentes cantidades de datos de todo tipo, que pueden ser interceptados o filtrados en su camino hacia los sistemas empresariales si no se utilizan los controles y las barreras apropiados. Como buena parte de estos dispositivos no fueron concebidos en su momento para la seguridad digital, al ser innecesario, no integran sistemas de autentificación o autorización.

Adaptación y respuesta

Un ciberataque en el entorno de producción puede interrumpir las operaciones y tener un impacto inmediato en una organización. José Valiente, director del Centro de Ciberseguridad Industrial, opina que son cada vez más las voces que defienden que la seguridad en la era de la transformación digital no debe estar basada de forma exclusiva en medidas de prevención o defensa, sino también en la capacidad de adaptarse y dar respuesta. Una idea que explica a través del investigador en ciberseguridad Jeimy Cano: "Tarde o temprano las barreras definidas van a caer, tarde o temprano la organización será objeto de un incidente y, para ello, la postura de seguridad por vulnerabilidad habilita a la organización para responder de manera ágil y efectiva, pues no estará distraída en el que dirán del incidente, sino tomando acciones concretas que permitan entender, contener, recuperar y comunicar lo que ha ocurrido, para aprender rápidamente y aumentar su capacidad de resiliencia frente a eventos futuros".

En la mayoría de ambientes industriales existen debilidades de diseño: ausencia de segmentación, de autentificación y de cifrado, como reconocen importantes directivos de organizaciones que participaron en el documento *Beneficios de la ciberseguridad industrial para las empresas industriales*, publicado en febrero de 2017 por el Centro de Ciberseguridad Industrial (CCI). "Los atacantes tienen multitud de posibilidades de causar daño a una organización industrial alterando las especificaciones", añade José Valiente. Por ejemplo, un incidente tecnológico también podría alterar la producción, incluso producir un accidente laboral. "Cualquier empresa industrial puede ser un objetivo fácil para quienes han convertido los ciberataques en una fuente de

ingresos. Gestionar el riesgo tecnológico se ha convertido en una necesidad".

La ciberseguridad es una de la mayores preocupaciones para el 62% de los directivos de grandes fabricantes, según el informe *Cibersecurity, Data Security & Privacy* presentado en el Industry of Things World 2017. Son amenazas que no solamente pueden dañar las líneas de producción y los equipos industriales, sino también la imagen corporativa.

"Las grandes empresas son las primeras que están adoptando el internet de las cosas, las pequeñas vendrán más tarde", asegura Oriol Patau, director tecnológico de Accent Systems, una ingeniería electrónica pionera del IoT en España que tiene un centro de producción en Castellar del Vallès (Barcelona). Tiene en su haber diversos proyectos IoT, como el seguimiento de activos, "un segmento de negocio interesante". Por ejemplo, un cliente que deseaba realizar el control de piezas de aviación en almacén. En los productos que desarrollan y fabrican "incorporamos nuestras capas de seguridad, desde la autentificación extremo a extremo, y en otros dispositivos que necesitan más seguridad les añadimos cifrado", añade Patau.

Los proveedores de circuitos integrados están sacando nuevos productos para la industria conectada. Hasta ahora, se podían almacenar las claves dentro de un microcontrolador, "pero los nuevos requerimientos de seguridad en el mundo IoT nos obligan a utilizar unos circuitos integrados específicos certificados que contienen estas claves, que están más protegidos que un microcontrolador. Son circuitos que impiden su acceso a alguien no autorizado porque tienen muchos tipos de protecciones", afirma.

Miles de millones de dispositivos

Profesionales de seguridad de tecnologías de la información encuestados dijeron que esperaban que los dispositivos de IoT representaran un riesgo para sus redes, dado que el 71% no monitorizan estos componentes en tiempo real. Ahora ya existen unos 6.400 millones de dispositivos IoT conectados en todo el mundo y se calcula que en 2020 serán más de 20.000 millones. Pero en 2018, dos tercios de las empresas que los utilicen pueden tener brechas de seguridad. Las enormes cantidades de datos que los dispositivos están recolectando y transmitiendo podrían ser interceptados (seguridad) o filtrados (privacidad) sin controles adecuados.

Habilidades en ciberseguridad

El sistema educativo es insuficiente para cubrir las demandas de perfiles profesionales de IoT. La industria conectada trae consigo la necesidad de nuevos perfiles y habilidades, cuya demanda crecerá asimismo fuertemente en los próximos años, según el informe de Cotec sobre el Internet de las cosas en España. La escasez de técnicos puede suponer una barrera importante para el despliegue de IoT, como ya identifican las empresas (cuarto inhibidor en términos de relevancia, tras la seguridad, privacidad y falta de casos empresariales). De hecho, en 2017 el 25% de los proyectos de IoT será abandonado antes de su implantación debido a la falta de capacidades en IoT, según el informe *España 4.0. El Reto de la Transformación Digital de la Economía.*

Una de las competencias profesionales que va a tener mayor crecimiento se refiere a la infraestructura de seguridad de los objetos IoT y la ciberseguridad. Algunos de los nuevos puestos demandados por estas plataformas son arquitecto IoT, encargado del diseño global del sistema y el especialista en conectividad y redes. Existen cuatro *títulos de técnico* superior con formación parcial en IoT: sistemas electrotécnicos y automatizados, automatización y robótica industrial, administración de sistemas informáticos en red y desarrollo de aplicaciones multiplataforma.

Por otra parte, la Universidad de Salamanca está impartiendo el Máster en Internet de las Cosas. Los alumnos que lo finalicen estarán capacitados para ocupar diferentes cargos en equipos multidisciplinares ya que abarca desde la programación de sensores y elementos de comunicación, hasta la extracción e interpretación de datos a través de *big data* y visualización.

En la actual etapa de adopción del internet de las cosas en el entorno industrial, se prioriza la experiencia del usuario y la inmediatez del mercado, dejando la seguridad para más adelante. Es toda una temeridad: varios dispositivos IoT pueden ser pirateados en solo tres minutos, pero el remedio puede llevar días o semanas, según pruebas realizadas por Forescout. Si alguno de estos dispositivos se infectara, los ciberdelincuentes pueden plantar puertas traseras para lanzar un ataque de denegación de servicio (DDoS) de *bots*. De este modo, aprovecharían técnicas de interferencia o falsificación para acceder a sistemas inteligentes de seguridad empresariales y controlar sensores de movimiento, cerraduras y equipos de vigilancia. Sin ir más lejos, en 2015, unos ciberatacantes obtuvieron acceso a una planta de acero alemana a través de la red comercial, se abrieron camino en las redes de producción para acceder a los sistemas de control y provocaron daños en un alto horno de la fábrica.

Este tipo de amenazas crecen de forma exponencial: a mayor número de componentes instalados, mayor riesgo. El fabricante de chips ARM calcula que hacia el año 2035 existirán un billón de dispositivos IOT en red. Por eso, ha creado un marco de seguridad, el Platform Security Architecture (PSA), respaldado por los principales proveedores de servicios en la nube, *hardware* y servicios incluidos Microsoft Azure, Google Cloud Platform, Cisco, Sprint y Vodafone. Está previsto publicar el PSA y entregar un *firmware* de implementación de referencia de código abierto a principios de 2018.

Enfocado más en la seguridad y la fiabilidad de los entornos de sistemas de control industrial, el Industrial internet Consortium (grupo fundado por AT&T, Cisco, GE, IBM e Intel) lanzó su propio marco de seguridad de la IIoT. Son un conjunto de mejores prácticas para ayudar a los desarrolladores y usuarios a evaluar los riesgos y defenderse contra ellos. Explica cómo la seguridad se ajusta al negocio de las operaciones industriales, define los componentes funcionales para abordar las preocupaciones de seguridad y proporciona orientación y técnicas prácticas para establecer medidas. El objetivo es impulsar el consenso de la industria, promover las mejores prácticas de seguridad de IIoT y acelerar su adopción.

Los técnicos también se deben enfrentar a otros retos, como la multitud de tecnologías inalámbricas y otras que están surgiendo en torno al IoT, desde el Bluetooth Low Energy, al NarrowBand IoT y Sigfox.