LA CIBERSEGURIDAD DE LA INDUSTRIA 4.0: UN MEDIO PARA LA CONTINUIDAD DEL NEGOCIO

ANA I. AYERBE
TECNALIA

Cuando hablamos de Industria 4.0 o de la Internet Industrial estamos hablando de digitalización, de conectar máquinas, sistemas, empresas, de recoger cantidades ingentes de datos que permitan tomar decisiones de la forma más precisa y en el menor tiempo, con el objetivo final de incrementar la productividad, el volumen de negocio y en consecuencia los resultados de las empresas.

Además de múltiples beneficios, la digitalización y la conectividad aumentan la superficie de exposición de las empresas a ciberataques y las consecuencias de un ciberataque, perpetrado por cibercriminales, pueden ir desde el secuestro de datos para pedir un rescate, el robo de IPR, la parada de máquinas o el malfuncionamiento de las mismas, la modificación de setpoints que haga que el producto fabricado no salga con la calidad prevista o la manipulación de datos que puede hacer tomar decisiones equivocadas al basarse en datos manipulados. Todo ello puede impactar tanto en los resultados económicos de la empresa, como en un deterioro del medio ambiente, daños de distinta consideración a personas o en una mala imagen de la empresa.

INTRODUCCIÓN

Desde el ciberataque denominado Triton en el 2017, que fue capaz de adquirir el control remoto de una planta industrial y provocar la parada total de la planta, recordando mucho al histórico Stuxnet de 2010, pasando por ataques como el dirigido a una planta de acero en Alemania en 2014 en el que los atacantes se infiltraron en los sistemas de planta y consiguieron manipular los componentes de control provocando graves daños en un alto horno [Bundesamt für Sicherheit in der Informationstechnik, 2014], o el primer corte de suministro eléctrico de la historia en Ucrania en 2015 debido a un ciberataque que usó el troyano BlackEnergy y técnicas de Ingeniería Social, son múltiples los ciberataques industriales que se han ido produciendo en los últimos años. Otros ataques no directamente orientados al entorno industrial pero que explotaban vulnerabilidades existentes en los sistemas TI, como NotPetya y Wannacry en el 2017, que secuestraban los datos de los equipos pidiendo un rescate por los mismos, también tuvieron su impacto en el ámbito industrial.

Según datos proporcionados por [EEF, 2018], el 48% de los fabricantes en UK han sufrido algún tipo de ciber ataque y la mitad de esos negocios han sufrido bien pérdidas financieras o interrupciones de su negocio como resultados del ciberataque. Según las mismas fuentes el 91% de los fabricantes están invirtiendo o in-

tentando invertir en la digitalización pero el 35% indica que su percepción de incrementar las vulnerabilidades a las ciberamenazas les está inhibiendo de hacerlo. Aunque el 75% de los fabricantes indican que monitorizan y protegen sus sistemas y software de ciberataques, muy pocos disponen de una estrategia de negocio completa que incluya el registro de riesgos y la formación del personal. El entorno de ciberseguridad es difícil para los fabricantes y un 41% señala que no cree disponer de la información necesaria para abordar los posibles riesgos de ciberseguridad e incluso un número superior no confían en que están preparados con las herramientas, procesos y tecnologías apropiadas para abordarlos. Continuando con el mismo informe un preocupante 12% de fabricantes confiesan que no disponen de medidas técnicas o de gestión para mitigar las amenazas procedentes de ciberataques. El informe concluye indicando que un 59% de los fabricantes han recibido solicitudes por parte de sus clientes para que demuestren o garanticen la robustez de sus procesos de ciberseguridad y el 58% han realizado la misma solicitud a su cadena de suministro. Salvando las distancias la situación de los fabricantes españoles es muy similar.

Un elemento que ha empezado a impulsar la ciberseguridad en la industria son los aspectos regulatorios procedentes de Europa como los ligados a la Protección de Infraestructuras Críticas o la directiva NIS de Seguridad de las Redes y los Sistemas de Información.

Ahondando en las dificultades a las que se enfrenta la industria a la hora de abordar la ciberseguridad, el [CCI, 2018] señala que las industrias se encuentran en un estado inicial de madurez a la hora de implantar medidas que puedan gestionar los riesgos de ciberseguridad, ya que hasta no hace mucho tiempo la ciberseguridad no se encontraba entre las prioridades y los ámbitos de actuación de estas empresas. Por otro lado, se enfrentan a dificultades añadidas y conflictos internos por la necesidad de proporcionar recursos destinados a la ciberseguridad, en algunos casos difíciles de encontrar, y la dificultad para asignar responsabilidades de ciberseguridad a personal que puede no estar suficientemente preparado.

A todo lo anterior debe añadirse, como se menciona en el «Estado de la Ciberseguridad en Eukadi 2018», que hay cierta reticencia entre las empresas industriales a reconocer y notificar los impactos que haya podido tener un ciber incidente en sus empresas y esto es importante si se quiere que la dirección de la organización y las áreas de negocio conozcan las dimensiones reales del problema para poder tomar las medidas apropiadas dentro de la organización, involucrando a todos los ámbitos organizativos de la misma.

Trabajar para lograr una industria 4.0 resiliente implica entender y potenciar la ciberseguridad en las empresas industriales, considerando la ciberseguridad en el diseño, despliegue y operación de cualquier proyecto de Industria 4.0, sin olvidar que si se vende un producto es importante asegurar la ciberseguridad del mismo en las instalaciones en las que se utilice, caso por ejemplo de una máquina herramienta o en el usuario final si se trata por ejemplo de un coche.

EL PARADIGMA DE LA INDUSTRIA 4.0

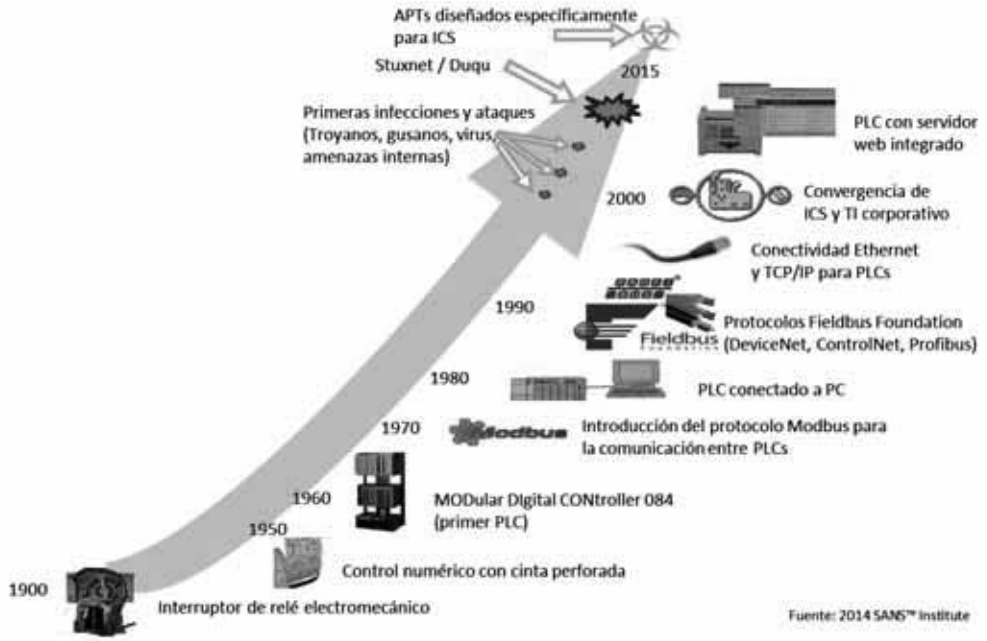
Los avances en las Tecnologías de Información y Comunicación (TICs), la electrónica cada vez más pequeña, los datos y servicios disponibles en Internet, el Internet of Things, el Internet de los Servicios, Big Data, Inteligencia Artificial y la Computación en la Nube son algunos de los motores para la innovación. Estos avances permiten embeber potencia de procesamiento, software y por lo tanto inteligencia en cualquier proceso y producto, así como conectar productos a Internet y crear productos que ofrezcan servicios.

Estos avances están en la base del cambio de paradigma promovido por iniciativas como Industria 4.0 [ACATECH 2014] o la Internet Industrial [ANNUNZIATA 2012] que se basan en la utilización de las Tecnologías de la Información y las Comunicaciones de una manera más profunda e integral durante el proceso de fabricación y ciclo de vida del producto, cubriendo las fases de diseño de producto, aprovisionamiento, fabricación, distribución y tratando de estrechar lo más posible las relaciones con los clientes. Este paradigma propone una integración completamente digital y abierta entre agentes y sistemas dentro de una industria.

El paradigma de Industria 4.0 establece tres niveles de integración:

- ***Integración Vertical:*** Se refiere a la integración de sistemas relacionados a diferentes niveles jerárquicos dentro de la organización, desde los niveles más básicos como los actuadores o sensores, pasando por niveles intermedios de control y fabricación, hasta llegar a los niveles más altos de gestión de la producción, ejecución y/o planificación. Este nivel de integración favorece, facilita y flexibiliza los mecanismos propios de fabricación.
- ***Integración Horizontal:*** Se refiere a la integración de sistemas entre los agentes y sistemas involucrados en las distintas etapas de los procesos de fabricación y planificación de negocio, que implican un intercambio de materiales, energía, información y productos, tanto dentro de una empresa como entre diferentes empresas o entidades a lo largo de la cadena de valor.
- ***Integración Circular:*** Trata de unificar los dos anteriores tipos de integración, vertical y horizontal, con el usuario final y con el ciclo de vida del producto. Esta integración cierra el ciclo de producción para conseguir obtener una digitalización completa extremo a extremo, desde las etapas iniciales de diseño, pasando por las

FIGURA 1
EVOLUCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL



Fuente: 2014 SANS Institute

etapas de planificación de producción, la fabricación, los mecanismos de gestión de recursos y logística, llegando hasta el cliente final y los servicios asociados a los productos. Ésta última integración consigue una digitalización completa de toda la cadena de valor y una importante realimentación del usuario en todo el ciclo de vida del producto.

En este contexto nos encontramos con una demanda que se vuelve cada vez más sofisticada y a la que se debe satisfacer con productos cada vez más inteligentes y personalizados, con fábricas inteligentes capaces de producir miles de configuraciones diferentes de un producto, fabricando grandes lotes en lugar de series cortas, apareciendo nuevos modelos de negocio basados en el servicio y el pago por uso, y en donde el dato y su soberanía adquieren un gran valor.

La industria 4.0 supone smartización y conectividad a Internet, creando sistemas de sistemas, y según dice el experto en seguridad y privacidad Mlkko Hypponen, en la denominada Ley de Hypponen «cualquier objeto calificado como smart es vulnerable», por lo que la superficie de exposición de estos sistemas y en consecuencia de las empresas a ciberataques aumenta sustancialmente.

EVOLUCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL

En las empresas industriales se suele diferenciar entre Tecnologías de la Información (TI) que son las redes ofimáticas o corporativas y Tecnologías de Operación (TO) formadas por las redes de control y producción industrial. Aunque estas redes tradicionalmente han estado separadas, los sistemas de control industrial han ido evolucionado de arquitecturas aisladas de las redes TI de la empresa a formar parte de arquitecturas integradas.

Por otro lado, los sistemas de control industrial utilizaban protocolos específicos y propietarios, como Modbus o ProfiBus que eran propietarios y conocidos con detalle únicamente por los expertos en la materia y en los que la seguridad era por oscuridad u ocultación. Estos protocolos han evolucionado para utilizar protocolos Ethernet como TCP/IP que están ampliamente extendidos y documentados.

Los sistemas de control industrial también han pasado de funcionar con sistemas en bucle abierto/cerrado controlados de forma estática a sistemas retroalimentados con parámetros provenientes de sensores en tiempo real exteriores como por ejemplo sensores de la Internet of Things (IoT).

Si analizamos la evolución de los sistemas de control industrial, podemos observar como a partir del año 2000 que es cuando se produce la conectividad de los sistemas de control industrial a través de TCP/IP y la integración con los TI corporativos, se empiezan a producir los primeros ciberataques dirigidos a este tipo de sistemas (Figura 1).

Una búsqueda realizada en Mayo del 2017, en el motor de búsqueda para dispositivos conectados a Internet SHODAN del puerto 502, que es el puerto

FIGURA 2
RESULTADOS DE DISPOSITIVOS PARA EL PUERTO 502 EN MAYO 2017

Fuente: SHODAN

FIGURA 3
RESULTADOS DE DISPOSITIVOS PARA EL PUERTO 502 EN JUNIO 2018

Fuente: SHODAN

utilizado por uno de los protocolos industriales más utilizados como es Modbus, proporcionó 13.841 resultados (Figura 2). Ese resultado quiere decir que todos esos dispositivos eran directamente accesibles desde Internet sin ofrecer ningún tipo de protección.

La misma búsqueda realizada en Junio del 2018 proporcionó 18.806 resultados (Figura 3). Como puede observarse, a pesar de todos los esfuerzos de sensibilización hacía la ciberseguridad en entornos industriales, no sólo no ha disminuido el número de resultados sino que se ha incrementado. Este es un hecho preocupante porque quiere decir que las nuevas instalaciones que se están realizando utilizando el protocolo Modbus, no están siguiendo pautas de ciberseguridad que minimicen las puertas de entrada de ciberatacantes a los sistemas industriales.

VULNERABILIDADES MAS COMUNES EN LOS SISTEMAS DE CONTROL INDUSTRIAL

Dado que los sistemas de control industrial han venido funcionando de forma aislada de otras infraestructuras TI, muchas de sus vulnerabilidades eran difícilmente explotables al no existir acceso físico a los sistemas. La sucesiva conexión de los sistemas de control industrial, tanto con los sistemas corpo-

rativos como con Internet, hacen que aumente la superficie de exposición de los sistemas a posibles ciberatacantes por lo que las posibles vulnerabilidades existentes representan un enorme riesgo, ya que ofrecen puertas de entrada para quienes desean explotarlas.

Podemos decir que los sistemas de control industrial son vulnerables fundamentalmente a dos tipos de amenazas informáticas. Una de ellas es la amenaza a las TI que se utilizan para fines comerciales y administrativos. Estos son los ataques de los que se oye a menudo y en los que se comprometen equipos de oficina con el resultado de robo o destrucción de datos. Mientras este tipo de amenazas está relativamente bien entendido y existen soluciones avanzadas de protección en forma de aplicaciones antivirus o para la detección y prevención de intrusiones (IDS/IPS), el segundo tipo de amenazas que tiene como objetivo a la Tecnología Operativa carece todavía de soluciones integrales de seguridad.

La regla por defecto para mitigar y prevenir vulnerabilidades de aplicaciones en el mundo de los sistemas TI corporativos es la de actualizar las aplicaciones y servicios con su última versión disponible. No obstante, la actualización a tiempo de los componentes software afectados no supone una garantía para la ausencia de vulnerabilidades, sino que sólo asegura que las vulnerabilidades conocidas están siendo tratadas. Esta es la razón por la que en los entornos TI corporativos se emplean diferentes tipos de protección, como cortafuegos, sistemas de gestión de información y eventos de seguridad (SIEM), o sistemas de detección de intrusiones (IDS) para poder prevenir, o por lo menos detectar de forma temprana, cualquier ataque.

Sin embargo, en los sistemas de control industrial la actualización de los componentes software conlleva unas dificultades añadidas. Debido al prolongado ciclo de vida de muchos de sus componentes, que pueden estar en operación durante decenas de años, y sus requisitos de rendimiento en tiempo real, en muchos casos no es posible actualizarlos con las últimas tecnologías protectoras. Esta situación es la que limita particularmente el empleo de técnicas de criptografía para asegurar la integridad y confidencialidad de datos en sistemas de control industrial, ya que el tiempo añadido necesario para encriptar y desencriptar la información supera los límites de ejecución de muchas de sus operaciones.

Otro aspecto que dificulta la aplicación de políticas de actualización de componentes parecidas a las empleadas en entornos TI, es la alta interdependencia de los componentes y elementos en un sistema de control industrial, por lo que se hace necesario efectuar extensas pruebas para garantizar el correcto funcionamiento del sistema antes de desplegar actualizaciones en un sistema en producción.

Si tenemos en cuenta que la gran mayoría de los sistemas de control industrial en uso han sido desarrollados hace más de una década y con la práctica ausencia de consideraciones de ciberseguridad, se observa que muchas de las vulnerabilidades se deben a faltas de previsión, deficientes prácticas de programación y/o a la antigüedad de sus componentes. Por ello entre las vulnerabilidades más utilizadas para perpetrar ataques se encuentran las de «buffer overflow/segmentation faults», un control de acceso insuficiente, y una arquitectura de red deficiente bien por falta de protección del perímetro o por una falta de segmentación interna o por ambas.

Otro punto de posible ataque en un sistema de control industrial lo constituyen los sistemas operativos (SO) instalados en los diferentes servidores, tanto en el conjunto puramente TO, como en la infraestructura TI corporativa. Si las dos infraestructuras están conectadas entre sí, una vulnerabilidad en el SO de un servidor corporativo puede crear una posible puerta de entrada a través de la cual un atacante puede infiltrarse en el sistema de control industrial.

Finalmente, también se utilizan determinadas vulnerabilidades en SO, aplicaciones y servicios para acometer ataques dirigidos, en los que un adversario aprovecha estas debilidades para establecer puertas de entrada ocultas o puntos que sirven de cabeza de puente para infiltrarse en un sistema.

TIPOS DE CIBERATAQUES

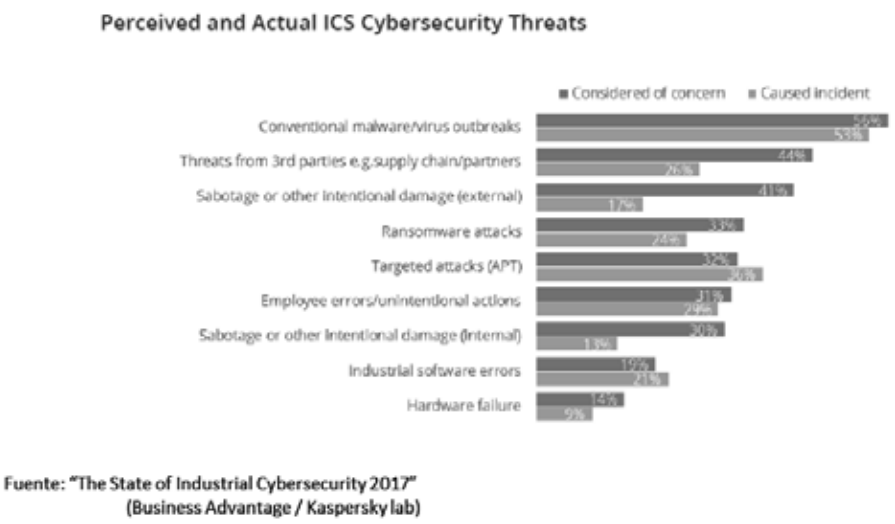
Un ciberataque perpetrado en una industria puede revestir diferentes niveles de gravedad en función de su impacto en el negocio. El Spam o Adware únicamente producen molestias a la organización, sin embargo el Spyware que puede monitorizar hábitos de uso y de navegación y el Phishing resultan más peligrosos ya que se puede utilizar posteriormente la información adquirida para realizar ciberataques más especializados y de mayor gravedad. En el caso de los Troyanos, Virus, Gusanos y Ransomware pueden posibilitar el establecimiento de puertas traseras y el secuestro, la manipulación o la destrucción de datos.

Entre los ciberataques de mayor gravedad nos podemos encontrar con los RootKit y Advance Persistent Threats (APT) que pueden suponer una pérdida total e inconsciente del control del sistema y que pueden ser prácticamente indetectables permaneciendo en un sistema durante mucho tiempo antes de que sus efectos sean visibles.

Según [Kaspersky Lab, 2017], Malware y APTs han sido las principales fuentes de amenazas de ciberseguridad en los sistemas de control industrial, junto con los errores no intencionados de empleados (Figura 4):

Aunque existen múltiples vías posibles de infección, uno de los primeros pasos que suelen utilizar los ciberatacantes es obtener información de contexto del sistema y de sus usuarios, utilizando técnicas de Ingeniería Social para poder perpetrar los ciberata-

FIGURA 4
PRINCIPALES FUENTES DE AMENAZAS DE CIBERSEGURIDAD



Fuente: Kaspersky Lab

ques de la forma más eficiente y con el menor riesgo posible. Posteriormente puede haber un acceso físico por parte de una persona a una determinada zona, accediendo a los dispositivos que allí se encuentran introduciendo un dispositivo infectado, como un USB u otro tipo de dispositivo tipo BYOD que se conecta al sistema, explotando vulnerabilidades debidas al diseño de la red y/o a los protocolos utilizados, o puede haber una incorrecta o insuficiente validación de entradas, control de accesos o una autenticación incorrecta o insuficiente que hagan que personas que no debieran hacerlo entre en nuestro sistema.

El factor humano también es importante ya que un usuario puede acceder a sitios web maliciosos, responder a emails de tipo phishing, dejar claves en sitios visibles, mostrar falta de precaución al abrir o ejecutar ficheros desconocidos o ejecutar programas infectados abriendo puertas a los ciberatacantes.

Los ciberataques también pueden clasificarse en dirigidos o accidentales. Los ciberataques dirigidos persiguen lograr un objetivo concreto. Sería el caso de Myriad, que provoco ataques de denegación de servicio en gran cantidad de empresas utilizando un ejército de bots de la Internet of Things o el Wannacry que explotó una vulnerabilidad conocida del sistema operativo Windows en todas aquellas empresas que no habían descargado un parche, que subsanaba dicha vulnerabilidad. También nos podemos encontrar con ataques multi-vector que son los que utilizan otras áreas o dispositivos como trampolín hasta llegar a su objetivo como el caso de Stuxnet en el que a través de un USB infectado se llegó al nivel TI de una empresa de enriquecimiento de uranio para desde allí llegar al nivel TO.

Entre los ataques dirigidos a empresas multi sector se encuentran las estafas «Business Email Compromise» (BEC) que es un tipo de ataque que consiste en suplantar la identidad de una persona vía email para engañar a otra con el fin de que realice una transferencia económica a una cuenta controlada por el estafador. Estos ataques están diseñados específicamente para cada víctima, por lo que los ciberdelincuentes estudian las últimas noticias de la empresa objetivo, investigando en las redes sociales de los empleados y utilizan correos electrónicos totalmente profesionales para hacer que el señuelo resulte lo más convincente posible. Este nivel de personalización ayuda a que este tipo de estafas por correo electrónico superen los filtros de spam y otras protecciones.

Decimos que nos enfrentamos a un ciberataque accidental cuando nos encontramos con una infección que se ha propagado desde un área de la empresa a otra, sin que el objetivo del ciberataque fuese llegar a esta última. Entre la categoría de ciberataques accidentales el error humano es uno de los principales, por ejemplo, un empleado que abre un adjunto infectado o que introduce en la empresa un USB infectado.

CLASIFICACIÓN DE LOS CIBERATACANTES

Es habitual pensar que los ciberdelincuentes sólo se interesan por las grandes empresas y qué por ser una pequeña empresa o un ciudadano normal no se despierta interés cuando la gran mayoría de los ciberataques se realizan de manera masiva e indiscriminada y no tienen en cuenta el tamaño de la empresa, por lo que cualquier empresa con independencia de su sector es una víctima potencial.

Si analizamos el perfil de los ciberatacantes podemos ver que ha cambiado mucho en los últimos años. Ahora los ciberatacantes se han profesionalizado y

FIGURA 5
CLASIFICACIÓN DE LOS CIBER ATACANTES

Fuente: Elaboración propia

entre sus principales motivaciones se encuentran fundamentalmente el beneficio económico, objetivo del cibercrimen y del ciberespionaje principalmente, así como la política, reivindicación y activismo que son objetivo de la ciberguerra, ciber terrorismo y ciberactivismo (Figura 5).

La estrategia de los ciberatacantes es obtener beneficios con el mínimo riesgo posible y obteniendo el mayor retorno de la inversión. Son altamente profesionales, funcionan como empresas con un modelo de negocio claro, ofreciendo la tecnología y la infraestructura necesaria para cometer ciberdelitos. También cuentan con fuentes de financiación sólidas y trabajan de manera conjunta con otras mafias del mundo real para conseguir sus objetivos. Estas empresas que operan en la Deep Web han creado el conocido como «Crime as a Service (CaaS)» y entre los servicios que ofrecen pueden citarse el desarrollo de exploits, la creación de malware, los ataques de denegación de servicio, campañas de phishing o spam entre otros [CybercrimeDependenciesMap].

IMPACTO DE UN CIBERATAQUE

El impacto de un ciberataque puede ser diferente si se trata de una infraestructura crítica o de otro tipo de industria. En el caso de una infraestructura crítica, un ciber ataque puede producir la interrupción de un servicio ofrecido a las empresas o al ciudadano, como es el caso de las redes de distribución de agua o energía, o producir un efecto en cascada provocando problemas de funcionamiento en otras industrias caso de la energía.

Existen diferentes formas en las que un ciberataque puede impactar en la operativa de las empresas industriales, pudiendo ir desde una pérdida de la disponibilidad de un sistema a una disminución del rendimiento del mismo o a la pérdida del control de la producción. Sus consecuencias pueden ser económicas, pero pueden llegar a producirse daños medio ambientales o incluso provocar lesiones de diferente consideración a las personas.

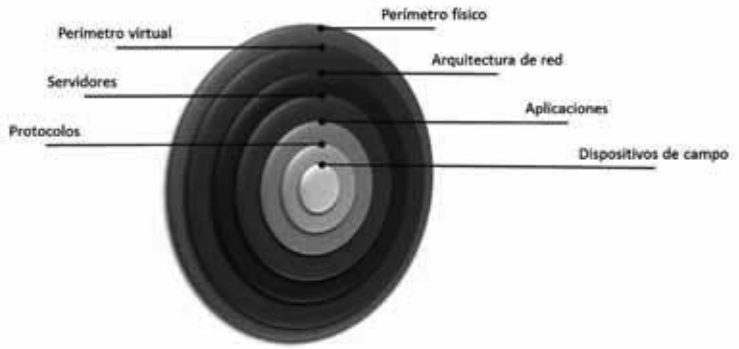
En cualquier de los casos se pueden producir pérdidas económicas y daños a la imagen de la empresa, existiendo una estrecha relación entre el riesgo financiero y el riesgo cibernético que puede llegar a provocar una caída de hasta el 5% del valor de las acciones, una pérdida de la facturación de las empresas por valor de unos 2,7 millones de euros y en el caso de filtraciones de datos o de su robo, con la aplicación del GDPR pueden llegar a producirse multas de hasta 20 millones de euros o el 4% de la facturación total anual del ejercicio anterior [Harvard Business Review, 2017]. Por estos motivos intentar evitar un ciberataque o al menos minimizar su impacto es importante si se desea gestionar la continuidad del servicio esencial que se esté prestando, la continuidad del negocio e incluso la propia supervivencia de la organización industrial.

El impacto de un ciberataque no debe verse únicamente desde el punto de vista de la organización industrial, también debe considerarse desde el punto de vista del producto fabricado y vendido. Si se piensa en un automóvil, los riesgos de ciberseguridad seguirían existiendo en el vehículo cuando esté siendo utilizado por su propietario [CCI, 2018].

LA SEGURIDAD COMO UN PROCESO

El mantra de cualquier buen ingeniero de seguridad es que «La seguridad no es un producto, sino un proceso» y como señala el criptógrafo Bruce Schneier «la seguridad es algo más que diseñar sólidos algoritmos criptográficos. Es el diseño de todo el sistema de tal manera que todas las medidas de seguridad incluyendo la criptografía trabajen en conjunto». Por este motivo la protección ante amenazas de ciberseguridad requiere adoptar un enfoque integral que implique a los recursos necesarios de la organización, ya no se trata únicamente de un problema del departamento de TI, e implica actuar sobre los procesos, capacitar a las personas y actuar sobre la tecnología.

FIGURA 6
DEFENSA EN PROFUNDIDAD



Fuente: Elaboración propia

Dado que la ciberseguridad 100% no existe, el objetivo debe ser mejorar la resiliencia de la empresa para mantener la funcionalidad de la misma ante condiciones adversas y para ello uno de los primeros pasos debe ser realizar un diagnóstico del estado de la industria en cuanto a ciberseguridad. Para ello deben analizarse las vulnerabilidades existentes, intentando resolver las que sean posibles y determinando qué nivel de riesgo va a ser necesario asumir porque habrá vulnerabilidades que no sea posible resolver porque sean muy costosas las medidas a tomar o porque pueda no ser viable por otros factores. El objetivo final es garantizar la continuidad del negocio ante un posible ciberataque en el menor tiempo posible y con el menor coste económico. Para ello debemos contar con un modelo de evaluación integral de una instalación completa y sus sistemas de seguridad evaluando los riesgos existentes, los elementos que sean críticos, analizando las posibles dependencias tanto internas como externas y las posibles medidas a tomar para minimizar esos riesgos en términos de procesos, personas y tecnologías.

También será necesario disponer de un plan de respuesta ante incidentes que contemple la redundancia de componentes críticos, evitando fallos en cadena mediante el aislamiento de componentes que en caso de fallo puedan provocar efectos secundarios en otros elementos, permitir una degradación elegante del sistema contando con una posible operación de emergencia o manual, posibilitando la restauración del sistema mediante copias de seguridad y con un tiempo de recuperación aceptable y todo ello fijando los roles y responsabilidades necesarias. No debe olvidarse que el objetivo final es garantizar la continuidad del negocio en el menor tiempo posible, con el menor coste económico y el menor impacto posible.

DEFENSA EN PROFUNDIDAD

El concepto que implementa esta idea de enfoque integral se denomina «Defensa en Profundidad» (Figura 6) y contempla diferentes dimensiones como el perímetro físico con sus instalaciones físicas y como acceder a ellos, el perímetro virtual con sus conexiones al mundo exterior, la arquitectura de la red, los servidores y sus sistemas operativos, las aplicaciones que se utilicen en la industria, y los protocolos de comunicación hasta llegar a los dispositivos de campo. A continuación se describe cada una de estas dimensiones en más detalle:

Perímetro Físico

El objetivo es abastionar el acceso físico mediante una combinación de controles de acceso físico basado en cerraduras, lectores de tarjetas y sistemas biométricos, registrando todos los accesos autorizados y protegiendo los interfaces físicamente accesibles como puertos de serie, USBs, etc.

Perímetro Virtual

La segunda capa del concepto de defensa en profundidad es el perímetro virtual y para protegerlo es necesario restringir el acceso remoto a los sistemas mediante credenciales y mecanismos de autenticación separadas para los usuarios de las redes corporativas y de los sistemas de control industrial, identificando los usuarios y sistemas que solicitan acceso, autenticando la identidad proporcionada y manteniendo registros históricos sobre accesos.

Se deben restringir los accesos de terceros gestionando los privilegios que se dan a operadores e ingenieros de sistemas, a los vendedores, integradores y personal de soporte, a los técnicos de campo, operadores de la cadena de suministro, proveedores de servicios administrados, socios de negocio y clientes.

También se debe seguir el principio del mínimo privilegio, restringiendo el acceso sólo a aquellas personas o sistemas que realmente lo necesitan, limitando los protocolos y herramientas de acceso remoto a lo absolutamente necesario, utilizando tecnologías seguras para acceso remoto, permitiendo el acceso sólo a los sistemas para los que el usuario o el sistema autenticado tenga autorización. Aunque pueda resultar incomo-

do siempre será mejor tener que abrir accesos en caso de que el sistema esté demasiado blindado que dejar abiertas puertas por defecto.

PROTEGER LA ARQUITECTURA DE REDES

Las principales recomendaciones asociadas a la protección de la arquitectura de redes consisten en segmentar las redes mediante zonas desmilitarizadas y de sandboxing, instalando cortafuegos capaces de filtrar e inspeccionar diferentes capas del modelo OSI, estableciendo una red multi-capa en las que las comunicaciones más críticas se ejecuten en la capa más segura y fiable.

Proteger los Servidores

En el caso de los servidores es necesario que sus sistemas operativos estén configurados con la seguridad como requisito principal y no tanto la comodidad o el rendimiento en la medida de lo posible, Los sistemas operativos deben actualizarse cuando sea necesario, aunque en los entornos industriales esto plantea el problema añadido de la posible pérdida de la garantía del fabricante al actualizar el sistema. También deben definirse cuentas de usuario y privilegios, así como limitar el acceso a la red a través de cortafuegos o proteger el registro de Windows.

Proteger las Aplicaciones

Resulta necesario garantizar la configuración segura de las diferentes aplicaciones empezando con el propio SCADA o MES, actualizándolos con los parches disponible, securizando las bases de datos y servidores Web. En caso de ser posible es recomendable utilizar una combinación de SIEM, IDS/IPS y antivirus para proteger, prevenir y registrar amenazas

Proteger los Protocolos

La protección de los protocolos de comunicación es quizás la parte más difícil de lograr en un enfoque de defensa en profundidad, dado que en muchos casos son protocolos propietarios lo que limita la posibilidad de modificarlos. En estos casos la forma más asequible suele ser la de «envolver» los protocolos con parsers que eviten inyección de tráfico o suplantar comandos, y limitar y/o deshabilitar todos los protocolos no necesarios y aquellos que trabajan con mensajes en texto plano.

Proteger los Componentes Individuales de los Sistemas de Control Industrial

Las recomendaciones para proteger los diferentes componentes individuales del sistema de control industrial consisten en actualizar siempre con los últimos parches de seguridad, ponerlos a prueba en condiciones de campo y verificar que no influyen en el funcionamiento correcto del sistema antes de ponerlos en producción, deshabilitar todos los puertos y servicios no utilizados y restringir los privilegios de acceso a lo mínimo necesario.

EL FACTOR HUMANO

Uno de los principales puntos de entrada de malware en las organizaciones es a través de personas que accidentalmente abren correos o ficheros infectados, o acceden a webs maliciosas. Por este motivo, concienciar al personal de la existencia del peligro y formar al personal sobre protección proactiva y reactiva con el fin de que sean capaces de identificar solicitudes fuera de lo común, prestando especial atención, por ejemplo a los emails que soliciten cambios relacionados con el destino de facturas o cuentas bancarias, resulta fundamental. Algunas pautas básicas que convendría que se tuviesen en cuenta son las siguientes:

- No abrir archivos desconocidos de remitentes desconocidos o sospechosos.
- Cambiar contraseñas con frecuencia y no dejarlas en sitios accesibles ni compartirlas con otras personas
- Evitar las descargas y los accesos a sitios sospechosos.
- No abrir ficheros adjuntos sospechosos
- Disponer de copias de seguridad
- No conectar dispositivos externos que no hayan pasado previamente por un antivirus.
- Mantener el sistema operativo actualizado y navegador actualizados
- Tener un antivirus instalado y actualizado continuamente.
- Validar la solicitud de transferencias electrónicas a través de otros medios como por ejemplo por teléfono, con el fin de eludir un posible email falso.
- Implementar medidas técnicas como pueden ser SPF, DKIM o DMARC .
- Implementar medidas de seguridad robustas para acceder al correo.

Así como la capacitación relacionada con las redes TI está muy avanzada, la capacitación de las personas en materia de ciberseguridad industrial no es un tema trivial, ya que las empresas se enfrentan con que la oferta formativa en la materia es escasa, a veces muy orientada hacía la ciberseguridad digital con ciertas nociones de temáticas industriales o muy centrado en el ámbito industrial con pequeños toques de ciberseguridad, pero sin existir un claro itinerario formativo disponible por el momento. Al mismo tiempo y en el caso de que la empresa quiere contratar profesionales de ciberseguridad se va a encontrar con una gran escasez de profesionales expertos.

CONCLUSIONES

La aproximación a la ciberseguridad en un entorno industrial debe considerase de forma holística teniendo en cuenta la tecnología, las personas y los procesos para minimizar los impactos de un ciberataque, poder volver a la operativa normal en el menor tiempo posible y garantizar la continuidad del negocio. Para ello debe hablarse de defensa en profundidad contemplando las diferentes dimensiones: perímetro físico, virtual, arquitectura de red, los servidores y sus sistemas operativos, las aplicaciones, los protocolos de comunicación y los dispositivos de campo.

Una adecuada gestión de la ciberseguridad bajo un enfoque integral implica la definición de los procesos necesarios para garantizarla y poder responder a los posibles incidentes que puedan producirse definiendo los roles y responsabilidades necesarios e intentando minimizar los posibles problemas interdepartamentales.

Al no existir la seguridad 100% es necesario tratar de minimizar el impacto de un potencial ciberataque en nuestras empresas, pero si queremos construir confianza en la Industria 4.0, no sólo es necesario preocuparse porque las industrias sean seguras, también es necesario preocuparse por la ciberseguridad de los productos que se fabrican y de los servicios que se ofrecen porque si no están adecuadamente protegidos pueden aumentar la superficie de ataque de la instalaciones industriales o empresas en la que se instalen o hagan uso de los servicios, o poner en riesgo a los usuarios de los mismos. Para ello es importante tener en cuenta la ciberseguridad durante todo el ciclo de vida de desarrollo de un producto y a lo largo de toda la cadena de suministro, utilizando procesos de desarrollo seguros y desarrollando actualizaciones y parches para cubrir vulnerabilidades descubiertas haciéndolo de una forma rápida y ágil.

Dado que los Riesgos Cibernéticos están cada vez más ligados a los Riesgos Financieros, el papel del CFO es entender donde se encuentran los ciberriesgos que pueden afectar financieramente a la empresa y en qué medida los presupuestos e inversiones en seguridad solicitados por parte del Director de Seguridad de la Información (CISO) o del Director de Tecnologías de la Información (CIO) pueden ayudar a disminuir las vulnerabilidades y los riesgos financieros asociados.

Finalmente, una industria debe poner todos los medios que estén en sus manos para estar preparada y poder garantizar la continuidad de negocio antes situaciones adversas procedentes de incidentes de ciberseguridad de los que ninguna organización está a salvo.

BIBLIOGRAFÍA

[ITS 2017] «Los 12 ciberataques con mayor impacto del 2017». www.its-security.ces

Bundesamt für Sicherheit in der Informationstechnik, 2014. https://www.bsi.bund.de/DE/Home/home_node.html

[EEF, 2018] Cyber Security for Manufacturing

[CCI, 2018] CIberseguridad en Infraestructuras Críticas e Industria 4.0

Centro de Ciberseguridad Industrial y Basque Cybersecurity Center. Estudio sobre el Estado de la Ciberseguridad en Euskadi, 2018.

[Acatech 2014] Final report of the Industrie 4.0 Working Group. «ACATECH: Recommendations for implementing the strategic initiative INDUSTRIE 4.0.», Abril 2014.

[Annunziata 2012] Annunziata, M., Evans, P.C. «Industrial Internet: Pushing the Boundaries of Minds and Machine.» General Electric, 2012.

SHODAN. https://www.shodan.io/

[Kaspersky Lab, 2017]. The State of Industrial Cybersecurity 2017.

[CybercrimeDependenciesMap]. https://www.europol.europa.eu/publications-documents/cybercrime-dependencies-map

[Harvard Business Review, 2017]. ¿Realmente le preocupa la ciberseguridad al equipo financiero?. https://www.hbr.es/seguridad-y-privacidad/933/realmente-le-importa-la-ciberseguridad-al-equipo-financiero