Cyber Security Month
October 2021

Retos y Mejores Prácticas de
Ciberseguridad y Transformación de Datos

INDUSTRIA MANUFACTURERA

ENCUENTRE SU PUNTO CIEGO

BDO

INDUSTRIA 4.01

La Industria Manufacturera está experimentando una transformación tecnológica que está cambiando el futuro de la industria. La Industria todavía está en sus primeros pasos en la adopción de datos digitales, conectividad digital y procesamiento digital. La transformación digital ha traído cambios significativos en todas las áreas clave de los procesos de fabricación, incluido el análisis de rendimiento, la agilidad de la investigación y el desarrollo y, en muchos casos, también ha traído cambios en la estructura organizativa y las corrientes de generación de ingresos.

En 2015, Klaus Schwab, presidente ejecutivo del Foro Económico Mundial, introdujo la frase "Cuarta Revolución Industrial" y lo que se ha denominado Industria 4.0, que describe la automatización en curso de las prácticas industriales y de fabricación tradicionales, utilizando tecnologías inteligentes. Desde entonces, las iniciativas de transformación digital han fomentado otra frase "Fábrica Inteligente" que describe fábricas estructuradas modulares con sistemas ciber físicos, monitoreo descentralizado, toma de decisiones y comunicación sobre y con dispositivos iOT. [1]

La Agencia de Seguridad de la Información en Red de la Unión Europea (ENISA) define la Industria 4.0 como un "cambio de paradigma hacia cadenas de valor digitalizadas, integradas e inteligentes que permitan una toma de decisiones distribuida en la producción mediante la incorporación de nuevas tecnologías ciber físicas como IoT". [2]

Los principales desafíos de fabricación se están abordando con éxito mediante la adopción de una mentalidad, tecnologías y procesos digitales y cambiando la forma en que las personas interactúan y trabajan dentro de ese sistema de eco. La adopción de nuevas tecnologías ha mejorado los niveles de productividad al resolver ineficiencias de procesos, reducir costos e innovar en nuevas fuentes de ingresos y desarrollo.

1 https://en.wikipedia.org/wiki/Foreign_Affairs
2 https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

FÁBRICAS INTELIGENTES

Según un estudio reciente de fabricación inteligente de Gartner, el 84% de los encuestados está de acuerdo en que el liderazgo comprende y acepta la necesidad de invertir en la fabricación inteligente.[3] Los primeros en adoptar en el sector de fabricación aprovechan cada vez más el enfoque de Fábrica Inteligente, ya que los avances en TI presentan mejoras inequívocas a los sistemas ICS / OT que aumentan la eficiencia, la escala y la calidad, al tiempo que mitigan los riesgos de tiempo de inactividad, cumplimiento, mantenimiento y seguridad.

Si bien la inversión, el diseño y el perfeccionamiento adecuado en sistemas de control administrativo y de ingeniería basados en inteligencia artificial deberían mejorar las condiciones laborales y la experiencia, las empresas también pueden analizar importantes tipos de datos previamente incomputables recopilados de múltiples fuentes, especialmente porque los objetivos estratégicos y operativos requieren tomas de decisiones más rápidas y más eficaces.

Sin embargo, a pesar de las inversiones en autosuficiencia, según la Encuesta de Tendencias de Implementación y Estrategia de Fabricación Inteligente 2020 de Gartner, el 57% de los líderes de fabricación dicen que su organización aún carece de trabajadores capacitados para respaldar los planes de digitalización.

Dicho esto, los líderes y las partes interesadas deben evitar las brechas de ejecución estratégica en el proceso de digitalización del sector manufacturero, principalmente mediante la implementación gradual de mejores sistemas, utilizando ecosistemas de cadenas de valor, redes de socios y consorcios de la industria, al tiempo que brindan a los usuarios tardíos que perciben la inmadurez tecnológica moderada como una plantilla para administrar pilotos, demostrar el ROI y escalar los éxitos.

Las Fábricas Inteligentes ya no siguen siendo un lujo, sino una necesidad para la fabricación, ya que las tecnologías de fabricación inteligente están comenzando a considerarse convencionales después de ganar suficiente madurez después de las primeras fases de adopción.

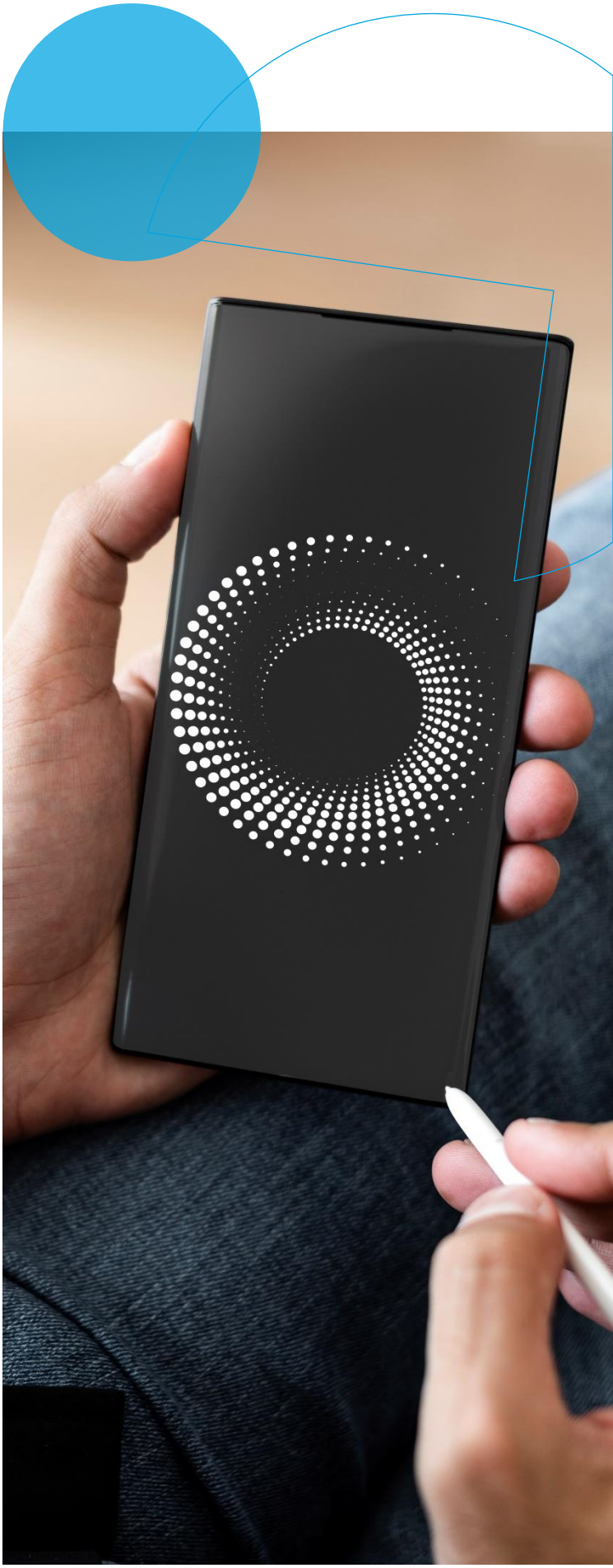
Como tal, la red específica de la industria que probablemente saldrá de la Internet Industrial de las Cosas (IIoT) debería conducir a mejoras en la producción total y la capacidad operativa, al tiempo que facilita la previsión necesaria para liderar la cooperación de desarrollos estratégicos más amplios de la industria.

3 https://blogs.gartner.com/power-of-the-profession-blog/strategy-and-execution-in-smart-manufacturing-must-meet-in-middle/

PANDEMIA DE COVID-19

En una encuesta realizada por Gartner, entre febrero y marzo de 2020, las empresas manufactureras informaron que pueden enfrentar un impacto financiero debido a la pandemia y las medidas de cuarentena. Casi la mitad de los encuestados en la encuesta de Gartner dijeron que anticipaban cambios en las operaciones y alrededor del 35% esperaban interrupciones en la cadena de suministro.[4] Casi el 80% de los fabricantes informaron que esperan algún tipo de impacto financiero, el 50% informó que anticipan que el impacto cambiará sus operaciones y casi el 40% informó que están enfrentando interrupciones en la cadena de suministro.

El impacto inicial de la pandemia comenzó a desaparecer durante la segunda mitad de 2020; sorprendentemente, alrededor del 70% de los fabricantes han informado que planean invertir, al menos lo mismo en mejoras digitales de sus procesos que antes de la pandemia.



TRANSFORMACIÓN DIGITAL

Se espera que la transformación digital en la industria manufacturera registre una CAGR (tasa de crecimiento anual compuesta) de más del 15% durante los próximos cuatro años.[5] La Fabricación Digital ha ayudado a reducir los ciclos de desarrollo, acelerar la innovación de productos y reducir los costes de fabricación.

La Fabricación Digital también representa una mayor generación de ingresos al integrar la robótica de trabajo 24x7 e iOT, lo que permite la fabricación bajo demanda, la optimización de operaciones, la gestión de la cadena de suministro y logística y la innovación de productos y servicios. El énfasis en la innovación en productos y servicios ha crecido, donde la innovación también deberá manejar e integrar información relacionada con productos y activos en las diferentes etapas del ciclo de vida del producto, desde el diseño hasta la producción y desde las ventas hasta el servicio y la jubilación.

4 https://www.gartner.com/en/webinars/3983070/opportunities-post-covid-for-the-manufacturing-industries
5 https://www.reportlinker.com/p05865775/Digital-Transformation-Market-in-Manufacturing-Growth-Trends-and-Forecast.html

AUTOMATIZACIÓN

La fabricación se encuentra entre las industrias con mayor potencial de automatización, especialmente en la recopilación y el procesamiento de datos, y también muestra un importante potencial de automatización dentro de los sitios de fabricación, la cadena de suministro y las adquisiciones.

IoT

Internet de las Cosas (IoT, siglas en inglés) ha generado nuevas funciones, servicios y beneficios para los fabricantes. Los casos de uso más importantes de IoT se encuentran en las operaciones, la gestión de activos y la gestión de personal. Por ejemplo, los fabricantes pueden establecer programas de mantenimiento preventivo con monitoreo en tiempo real, mejorar la eficiencia energética y las condiciones de trabajo mediante la gestión inteligente del aire, la gestión de riesgos, la productividad de los trabajadores, etc. [6]

GEMELOS DIGITALES

Los gemelos digitales aportan valor a las empresas en tres áreas principales. El primero es impulsar mejoras en el proceso de fabricación, el segundo es proporcionar un mantenimiento predictivo eficiente y el tercero es desarrollar nuevos productos basados en el uso real de los productos existentes. Los gemelos digitales pueden optimizar una implementación de IoT para obtener la máxima eficiencia, así como ayudar a los diseñadores a determinar dónde deben ir las cosas o cómo funcionan antes de que se implementen físicamente.

APRENDIZAJE AUTOMÁTICO

Con la cantidad de datos que están recopilando las máquinas, es más fácil que nunca utilizar algoritmos para decidir y realizar rápidamente el mejor curso de acción. Las máquinas actuales han demostrado que la eficiencia no sacrifica la calidad, ya que las máquinas pueden identificar y anticipar más cuidadosamente qué factores afectarán la velocidad o la calidad de la línea de ensamblaje.

Algunos ejemplos de aprendizaje automático incluyen la predicción de tiempos de espera, tiempos de envío o modelos de comportamiento para la prevención de riesgos. Además, los datos generados por las máquinas ofrecen información sobre todas las áreas del proceso de producción, que están integradas a lo largo de la cadena de suministro.

6 https://oroinc.com/b2b-ecommerce/blog/digital-transformation-in-manufacturing

COMERCIO-B2B

Además de entregar los datos de productos correctos a los clientes, las plataformas de comercio electrónico B2B pueden sincronizar automáticamente los datos con ERP (Planificación de Recursos Empresariales) y WMS (Sistema de Gestión de Almacenes) para reducir los esfuerzos de gestión de inventario y la probabilidad de errores humanos. Más importante aún, los sistemas de comercio electrónico B2B permiten a los fabricantes más flexibilidad en la venta directa al cliente o B2B2C sin interrumpir sus canales existentes.

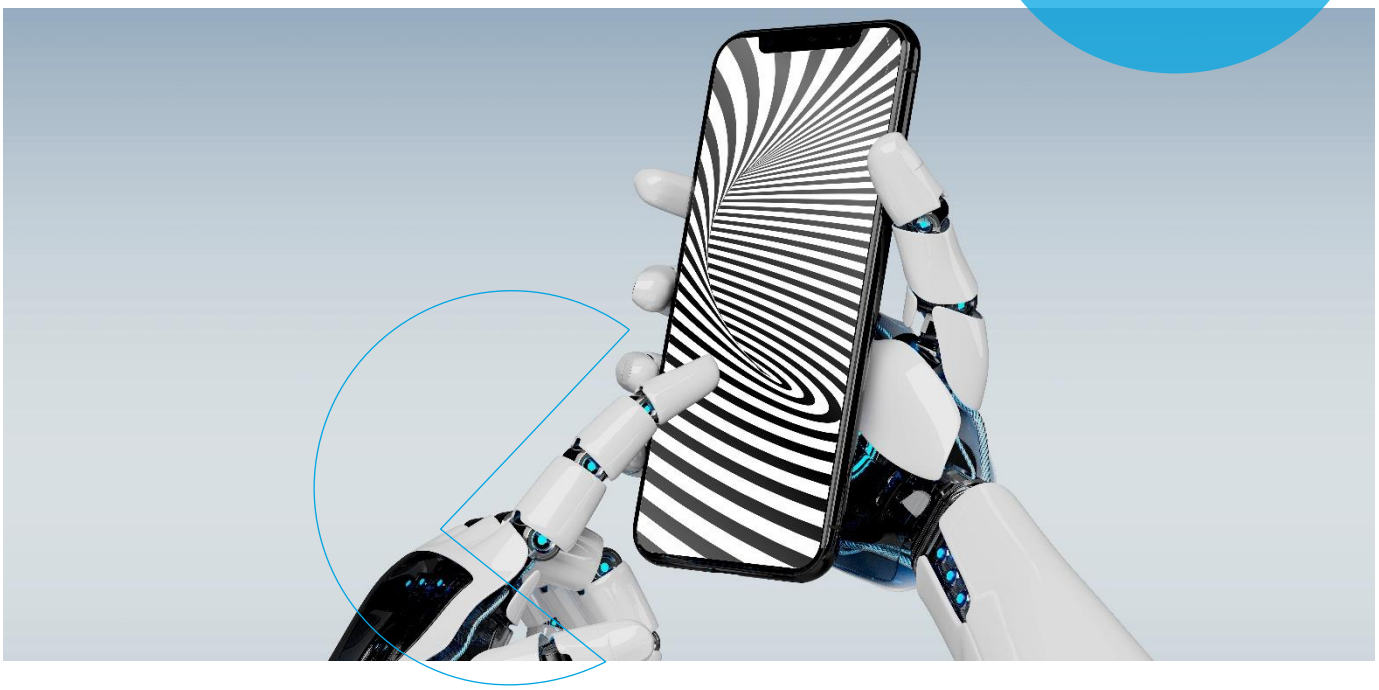
INTELIGENCIA ARTIFICIAL (IA)

A medida que aumenta la adopción de la robótica en la fabricación y se espera que aumente la cantidad de dispositivos conectados, la forma en que interactúan entre sí y el volumen de datos, la IA desempeñará un papel importante para otorgar a los robots más responsabilidad para tomar decisiones que puedan mejorar los procesos basados en datos en tiempo real recopilados de la planta de producción. Los robots también tendrán capacidades de aprendizaje del comportamiento anterior y el uso del reconocimiento de patrones para la toma de decisiones con mejores resultados.

ROBOTS

En una encuesta realizada por Gartner, entre febrero y marzo de 2020, las empresas manufactureras informaron que pueden enfrentar un impacto financiero debido a la pandemia y las medidas de cuarentena. Casi la mitad de los encuestados en la encuesta de Gartner dijeron que anticipaban cambios en las operaciones y alrededor del 35% esperaban interrupciones en la cadena de suministro.4 Casi el 80% de los fabricantes informaron que esperan algún tipo de impacto financiero, el 50% informó que anticipan que el impacto cambiará sus operaciones y casi el 40% informó que están enfrentando interrupciones en la cadena de suministro.

El impacto inicial de la pandemia comenzó a desaparecer durante la segunda mitad de 2020; sorprendentemente, alrededor del 70% de los fabricantes han informado que planean invertir, al menos lo mismo en mejoras digitales de sus procesos que antes de la pandemia.



SEGURIDAD CIBERNÉTICA

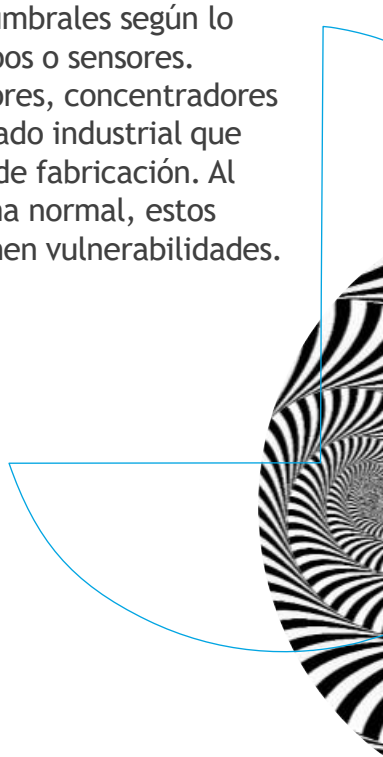
El movimiento hacia la Industria 4.0 tiene un impacto significativo en la conectividad de la red de fabricación. Anteriormente aislada y ejecutando sus propios protocolos, la red de fabricación se está integrando lentamente con la red de TI para obtener visibilidad, control e integración en tiempo real en varios sistemas que componen la línea de producción, la cadena de suministro, las ventas y los sistemas empresariales. Las computadoras y los controladores en la red de fabricación ahora están expuestos a una gama más amplia de amenazas, que requieren que tanto los administradores de TI como los ingenieros de OT trabajen juntos para llevar la seguridad y la protección de dichos sistemas a la velocidad sin comprometer los requisitos operativos.

Un informe sobre ciberseguridad y fabricación, publicado por Make-UK, ha colocado a la industria manufacturera como el quinto sector más ciberatacado en 2019, y también describe a las empresas industriales como las menos protegidas en el Reino Unido.

El Reino Unido es una de las naciones manufactureras más grandes del mundo, con más de tres millones de personas trabajando en la industria y entregando casi la mitad de todas las exportaciones del Reino Unido, lo que hace que esas estadísticas sean una preocupación mundial.[7] El informe publicó cifras más preocupantes, ya que el 60% de los fabricantes afirmaron haber estado sujetos a un incidente de seguridad cibernética en algún momento, y casi un tercio de ellos dijeron haber sufrido una pérdida financiera directa o una interrupción del negocio como resultado. "Los fabricantes a menudo informan sobre la confianza en su postura de seguridad cibernética, lo que los deja muy expuestos debido a la falta de una estrategia integral", concluyó el informe. Esta percepción se ha infiltrado en sus negocios y ha creado una barrera; impidiendo el despliegue de estrategias integrales de mitigación.

El 27% de los fabricantes informaron que no tienen un registro de riesgos o un plan de mitigación para limitar la amenaza, el 33% informó que no brindan resúmenes de concientización o capacitación formal a sus empleados, el 41% informó que no tienen un líder designado para la seguridad cibernética a nivel de directorio, el 49% informó que no monitorea el desempeño de la seguridad cibernética a través de indicadores clave de desempeño comercial, y el 55% informó que no tiene seguro para cubrir las pérdidas debido a un ataque cibernético.

Los equipos de fabricación modernos tienen interfaces hombre-máquina (HMI) que permiten a los operadores e ingenieros monitorear y controlar el equipo. Los controladores lógicos programables (PLC) se utilizan para programar la lógica en varios equipos, lo que les permite actuar en función de ciertas condiciones o umbrales según lo informado por otros equipos o sensores. Además, existen enrutadores, concentradores y puertas de enlace de grado industrial que manejan la red en la red de fabricación. Al igual que cualquier sistema normal, estos equipos y dispositivos tienen vulnerabilidades.



7 https://www.makeuk.org/insights/publications/cyber-security-and-manufacturing

De acuerdo con los informes de vulnerabilidades presentados al Equipo de Respuesta a Emergencias Informáticas de Sistemas de Control Industrial (ICS-CERT), se mostró un salto significativo en la cantidad de vulnerabilidades que afectan a los equipos relacionados con la fabricación, lo que también muestra que la mayoría de las vulnerabilidades disponibles públicamente involucraban vulnerabilidades HMI. Donde las HMI son de hecho aplicaciones, a veces tienen interfaces web y están sujetas a valorizaciones web tradicionales.

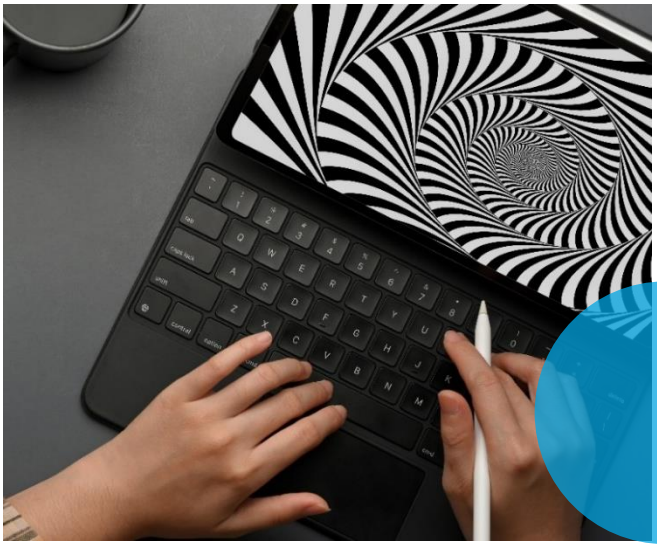
Según un estudio de Trend Micro, los problemas de seguridad comunes con las HMI implican corrupción de memoria, desbordamientos de búfer, vulnerabilidades de lectura / escritura, mala gestión de credenciales (uso de contraseñas codificadas, almacenamiento de contraseñas en formato recuperable y credenciales insuficientemente protegidas), falta de autenticación y transmisión de texto sin cifrar valores predeterminados no seguros, cifrado faltante y controles ActiveX inseguros.[8]

Trend Micro y Politecnico di Milano, la universidad técnica más grande de Italia, han publicado una investigación titulada "Código Vulnerable y Malicioso en la Programación Industrial". El informe describió cómo los piratas informáticos avanzados podrían aprovechar las vulnerabilidades en los robots industriales conectados a Internet y las máquinas automatizadas para interrumpir las líneas de producción y robar la propiedad intelectual. [9]

El informe también destaca cómo la automatización industrial puede no estar en condiciones de detectar y evitar que ocurra tal explotación. El informe señala las tecnologías heredadas, que son intrínsecamente difíciles de reemplazar y no se han discutido ni examinado desde una perspectiva de ciberseguridad. El informe también ha demostrado la explotación de los flujos de diseño y las vulnerabilidades en las plataformas lógicas de automatización y los lenguajes de programación heredados, que permitieron a los atacantes robar datos de un robot, alterar el movimiento del robot a través de la red, inyectar malware dinámico y ejecutar el código de forma remota sin ser detectados. En resumen, pudieron ejecutar un ataque exitoso mediante la creación de un malware autopropagable, escrito en plataformas lógicas de automatización basadas en lenguajes de programación heredados y propietarios.

Stuxnet, a menudo se hace referencia al mismo porque fue el primer malware que demostró la posibilidad de ocultación utilizando lenguajes de programación heredados. En 2010, Stuxnet provocó un cambio en el enfoque de la seguridad de ICS al demostrar la explotación práctica de la lógica de control en esos sistemas de control industrial.[10]

Stuxnet era un malware sofisticado contra gusanos informáticos diseñado para apuntar solo a un sistema ICS de Siemens específico. Hizo uso de múltiples vulnerabilidades de día cero, modificó las bibliotecas del sistema, ejecutó un servidor RPC e instaló controladores firmados robados en los sistemas operativos Windows. También pudo actualizarse desde la red local o conectándose a un sistema de comando y control y enviar información de su progreso.



8 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities
9 https://documents.trendmicro.com/assets/white_papers/wp-rogue-automation-vulnerable-and-malicious-code-in-industrial-programming.pdf
10 https://arxiv.org/pdf/1702.05241.pdf

Otra pieza de malware a destacar es Triton, que demostró que el malware específico del dispositivo y del proceso de control era factible y podría tener consecuencias desastrosas.[11] Triton fue el primer malware diseñado para atacar sistemas de seguridad, jamás visto en la naturaleza.

Triton, se descubrió por primera vez en 2017 en una planta petroquímica en el Medio Oriente, diseñada para manipular los controladores del Sistema Instrumentado de Seguridad (SIS) Triconex de Schneider Electric responsables de los sistemas de apagado de emergencia. Triton fue construido con una serie de características, incluida la capacidad de leer y escribir programas, leer y escribir funciones individuales y consultar el estado del controlador SIS.

El malware contenía la capacidad de comunicarse con controladores SIS (por ejemplo, enviar comandos específicos como detener o leer su contenido de memoria) y reprogramarlos de forma remota con una carga útil definida por el atacante.[12] Triton fue diseñado para cerrar los sistemas instrumentados de seguridad de la planta de fabricación, que fue el primer código malicioso que se escribió y usó deliberadamente para poner vidas en riesgo.

Los riesgos de ciberseguridad para las industrias manufactureras han ganado la atención mundial en paralelo a los avances en la transformación digital. El 11 de mayo de 2017, el presidente Trump firmó la Orden Ejecutiva (OE) 13800, Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica. OE 13800 pidió específicamente una revisión de "la suficiencia de las políticas y prácticas Federales existentes para promover la transparencia del mercado adecuada de las prácticas de gestión de riesgos de ciberseguridad por parte de entidades de infraestructura crítica".[13]

El 30 de abril de 2019, el DHS publicó una lista de 'funciones críticas nacionales' que el Departamento y la Casa Blanca consideran "Las funciones del gobierno y el sector privado son tan vitales para los Estados Unidos que su interrupción, corrupción o disfunción tener un efecto debilitante sobre la seguridad, la seguridad económica nacional, la salud o la seguridad pública nacional, o cualquier combinación de las mismas ".

El 15 de mayo de 2019, la Casa Blanca emitió la Orden Ejecutiva 13873, Asegurando la Cadena de Suministro de Tecnología y Servicios de Información y Comunicaciones, diciendo que "La comunidad de seguridad nacional y nacional estaba preocupada por el riesgo agregado que proviene del uso de ICT (siglas en inglés) y servicios comunes".

Del 8 al 9 de junio de 2019 en la reunión ministerial del G20 centrada en el comercio y la economía digital, la Declaración Ministerial articuló claramente los beneficios y riesgos que un mundo digital trae a industrias como la manufactura, afirmando: "La seguridad en una economía digital es esencial para fortalecer la confianza pública en las tecnologías digitales y en toda la economía digital". La Declaración Ministerial también citó los beneficios y los riesgos al afirmar que "La manufactura, que es una de las industrias más cruciales en la economía global, se está volviendo más digitalizada, interconectada e inteligente", y reconoció el riesgo que también proviene del mundo de tecnologías emergentes e IoT (siglas en inglés).

11 https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware

12 https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

13 https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

DESAFÍOS

El 20 de mayo de 2019 la Agencia de Ciberseguridad de la Unión Europea (ENISA, siglas en inglés) ha publicado un trabajo en el que se identifican los principales retos para la adopción de las medidas de seguridad y seguridad de la Industria 4.0 y el IoT Industrial. El estudio ENISA se centró en abordar los desafíos de seguridad relacionados con la evolución de los sistemas y servicios industriales precipitados por la introducción de la Fabricación Inteligente. ENISA ha asociado desafíos de ciberseguridad con una de las siguientes categorías: Personas, Procesos y Tecnologías.

CATEGORÍA	DESAFÍO	DESCRIPCIÓN
Personas	Falta de experiencia en seguridad de la información	Por lo general, las personas solo tienen conocimientos de seguridad de TI u OT, mientras que la fabricación inteligente requiere experiencia en varias áreas, por ejemplo, seguridad de redes, sistemas integrados, OT y TI.
Personas	Falta de formación y sensibilización	Las empresas de fabricación a menudo se están quedando atrás en la formación de los empleados que trabajan con equipos de TO y, en cambio, emplean soluciones de seguridad sin garantizar primero la aceptación por parte de los empleados.
Personas	Falta de una estructura de gobernanza adecuada	Los programas de seguridad definidos rara vez se implementan y, en general, faltan programas integrales que consideren la seguridad cibernética. También se observa a menudo que los roles y responsabilidades de los empleados relacionados con la seguridad no están claramente definidos.
Personas	Falta de financiación y compromiso por parte de la alta dirección	Se da la debida consideración a la ciberseguridad 'después del efecto', solo cuando una brecha de seguridad conduce directamente a pérdidas financieras.
Procesos	La responsabilidad está mal definida	Un gran número de partes interesadas están involucradas en la cadena de suministro y en el ciclo de vida de la Industria 4.0, por lo tanto, distribuir la responsabilidad después de un incidente de seguridad se vuelve un desafío.
Procesos	Complejidad de la Cadena de Suministro	La propiedad compartida de las soluciones conectadas de la Industria 4.0, las asignaciones de funciones poco claras o no especificadas y la falta de disposiciones en los contratos de adquisición y los acuerdos de nivel de servicio complican aún más el tema de la responsabilidad.
Procesos	Falta de estándares técnicos de seguridad	Las iniciativas integrales para abordar la seguridad de la industria 4.0 y la Fabricación Inteligente de manera integral se están quedando atrás.
Procesos	Fragmentación de estándares técnicos	La falta de esfuerzos uniformes de estandarización a nivel global da como resultado una situación en la que los sitios que pertenecen a una organización no pueden colaborar y compartir experiencia y soluciones entre sí.

CATEGORÍA	DESAFÍO	DESCRIPCIÓN
Procesos	Complejidad de la gestión de la cadena de suministro	La Fabricación Inteligente introdujo nuevas capacidades (Visibilidad de extremo a extremo, análisis predictivo, automatización y toma de decisiones basada en datos) que tienen un impacto adicional en la cadena de suministro, una mayor interdependencia de las cadenas de suministro da como resultado un impacto más amplio.
Procesos	Escalabilidad para la gestión de riesgos de la cadena de suministro	Las empresas deben tomar numerosas decisiones (por ejemplo, seleccionar proveedores, acordar métodos de colaboración, establecer procesos organizativos), de las que dependerá la seguridad del producto final. Esto implica una gran cantidad de personas, organizaciones, procesos y riesgos que deben gestionarse.
Tecnología	Sistemas Heredados sin soporte	Para entornos industriales, asegurar la interconectividad entre diversos dispositivos a menudo es un desafío, especialmente cuando se consideran dispositivos que no tienen soporte durante mucho tiempo.
Tecnología	Protocolos Patentados	Garantizar la interoperabilidad entre dispositivos y plataformas de diferentes proveedores no siempre es posible, especialmente si los protocolos propietarios no siempre son seguros.
Tecnología	Diferentes marcos de Aplicación	No siempre es posible garantizar una línea base de ciberseguridad común unificadora de capas de seguridad en todos estos elementos: plataformas, dispositivos, protocolos y marcos.
Tecnología	Limitaciones en la implementación de la seguridad por diseño	Las capacidades de procesamiento limitadas y la necesidad de asegurar un tiempo de operación prolongado mientras se mantiene un precio competitivo, afectan la implementación de características de seguridad en la fase de diseño.
Tecnología	Limitaciones en la implementación de la protección fundamental	Los parches y las actualizaciones de software en la mayoría de los casos son muy difíciles, a veces imposibles de implementar, cuando se trata de dispositivos de gama baja.
Tecnología	Falta de medidas de seguridad avanzadas	En ocasiones, no se admite la implementación de cifrado o autenticación, ya que solo protege la red y deja los dispositivos vulnerables a los ataques.
Tecnología	Falta de herramientas de ciberseguridad dedicadas	Las herramientas de ciberseguridad dedicadas para los sistemas de la Industria 4.0 son generalmente demasiadas, están menos maduras y aún no muestran un valor distintivo en la protección de redes y sistemas de TI y OT interconectados.

La interconectividad en toda la industria manufacturera se caracteriza por una mezcla interesante de OT (la red industrial), TI (la red empresarial) e IP (propiedad intelectual). Es la única industria que combina los tres, creando así estos conjuntos únicos de desafíos.

MEJORES PRÁCTICAS

ENISA ha publicado algunas recomendaciones de alto nivel para promover la ciberseguridad en la industria manufacturera. [14]

Conocimiento interfuncional sobre seguridad de TI y OT

Sensibilización sobre la seguridad básica del control industrial, así como sobre la forma segura de transición a la Industria 4.0 y la fabricación inteligente.

Las personas a cargo de la seguridad dentro de las organizaciones de la Industria 4.0 deben pasar por capacitaciones dedicadas en ciberseguridad que cubran todos los aspectos necesarios específicos para la convergencia de TI / OT y la fabricación Inteligente.

Incentivos para la Seguridad de la Industria 4.0

La ciberseguridad puede ser una ventaja competitiva importante para las empresas, ya que conduce a tener productos y servicios seguros, confiables y dignos de confianza.

Es importante establecer estructuras administrativas para que la gerencia de alto nivel discuta e intercambie opiniones con expertos en ciberseguridad y CISO y lancen esquemas de financiamiento para respaldar su transición a un ecosistema seguro de la Industria 4.0.

Estándares básicos dedicados a la seguridad de la Industria 4.0

Explore iniciativas y pautas que mapeen los estándares de seguridad de muchas fuentes diferentes para proporcionar un punto de referencia completo y así garantizar que se consideren todos los controles de seguridad necesarios. Desarrolle y mantenga esquemas de mapeo entre las actividades de estandarización para explorar sinergias y similitudes entre estándares.

Procesos seguros de gestión de la cadena de suministro

Lleve a cabo una evaluación de riesgos a intervalos periódicos para identificar los riesgos potenciales de la cadena de suministro de la Industria 4.0, considerando también la inteligencia de amenazas cibernéticas para monitorear el panorama de amenazas emergentes y en curso. Confíe en proveedores cuyos productos cumplan con estándares de seguridad y esquemas de certificación reconocidos y sigan un ciclo de vida de desarrollo de software seguro para los productos y servicios de la Industria 4.0.

Líneas base para la interoperabilidad de la seguridad

Identificar las recomendaciones de seguridad de referencia para los componentes, servicios y procesos de la Industria 4.0 basadas en el análisis de riesgos es un primer paso para abordar una solución a las desafiantes limitaciones técnicas de este dominio.

14 https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

EN CONCLUSIÓN

La manufactura aporta el 16% del Producto Interno Bruto (PIB) mundial, el 64% del gasto mundial en I + D y es un indicador líder de la salud económica mundial. Adoptar nuevos modelos de transformación que unan tecnología, personas, políticas y procesos junto con hacer de la ciberseguridad la máxima prioridad, es un propósito multinacional global.

OPHIR ZILBIGER

Líder Cibernético Global
Socio, Jefe del Centro de Ciberseguridad
BDO Israel
OphirZ@bdo.co.il

NOAM HENDRUKER

Socio Director de Cyber Consulting Group
Centro de Ciberseguridad de BDO
NoamH@bdo.co.il

TOMMY BABEL

Director Jefe de Operaciones
de Amenazas y Seguridad Ofensiva
Centro de Ciberseguridad BDO,
TommyB@bdo.co.il

ROTEM BAR

División Gerencial
de Defensa Industrial
Centro de Ciberseguridad de BDO,
RotemB@bdo.co.il

www.bdo.global

BDO