

Aumento de ataques en la industria exige controladores de producción más inteligentes

Ratingen, Alemania - 20 de octubre de 2025



[Fuente: Mitsubishi Electric Europe]

Un estudio global de Telstra y Omdia encontró que el 80% de las empresas de fabricación experimentaron un aumento significativo en incidentes o brechas de seguridad el año pasado, mientras que solo el 45% está adecuadamente preparado en su posicionamiento en ciberseguridad. Esta tendencia pone de manifiesto la creciente vulnerabilidad de los entornos de producción a medida que se vuelven más conectados y digitalizados.

Según el mismo estudio, los fabricantes afectados por un ciberataque informaron de problemas que costaron entre 200.000 y 2 millones de dólares por incidente.

Vamos a analizarlo con más detalle. Los ataques de ransomware a sectores industriales crecieron un 87% interanual, con la fabricación representando el 69% de todos los incidentes, según el informe de febrero de 2025 de Dragos. Siendo la fabricación la rama industrial el objetivo más atacado durante cuatro años consecutivos según el Índice de Inteligencia de Amenazas X-Force 2025 de IBM, la seguridad industrial sin duda se ha convertido en una preocupación crítica.

La conexión entre la tecnología de la información y la tecnología operacional en la fabricación ha introducido nuevos desafíos de seguridad. Aunque los enfoques tradicionales pueden abordar muchos de estos problemas, el panorama de evolución de las amenazas ha generado la necesidad de medidas de ciberseguridad sólidas integradas directamente en los propios productos de automatización.

"Con la creciente dependencia de la conectividad IoT, incluyendo la comunicación máquina a máquina y también las interfaces hombre-máquina, los componentes centrales del 'sistema nervioso' industrial—los controladores—deben ahora servir como guardianes críticos de la seguridad de la información", dijo Daniel Sperlich, Product Manager de Controladores de Mitsubishi Electric. "Nuestros últimos controladores MX han sido desarrollados para cumplir con estos requisitos de seguridad en evolución, manteniendo la precisión y fiabilidad esenciales para las operaciones de fabricación."

DDoS y Ransomware: Amenazas gemelas para la continuidad de la producción

Las amenazas que enfrenta la fabricación van más allá del ransomware. Los ataques de Denegación de Servicio Distribuida (DDoS) han surgido como una preocupación importante, con un informe de Zayo Group que revela que el sector manufacturero ha experimentado un aumento del 257% en el tamaño de los ataques entre 2023 y 2024. Estos ataques tienen como objetivo los sistemas de producción y pueden causar una interrupción operativa considerable.

"El sector de la fabricación se enfrenta a una convergencia de amenazas", explicó Daniel Sperlich. "El ransomware apunta directamente a la propiedad intelectual y a los datos operativos, mientras que los

ataques DDoS buscan interrumpir la producción colapsando la infraestructura de red. Ambos pueden provocar costosos tiempos de inactividad que los fabricantes simplemente no pueden permitirse."

El impacto financiero de estos ataques es considerable. Según el informe del Grupo Zayo, un ataque DDoS típico dura 39 minutos y cuesta aproximadamente 5.350€ por minuto a las empresas, lo que resulta en pérdidas medias de casi 210.000€ por incidente. Para operaciones de fabricación con calendarios de producción just-in-time y cadenas de suministro complejas, incluso interrupciones breves pueden tener efectos en cascada a lo largo de todo el proceso de producción.

Seguridad sin tiempo de inactividad: El papel crítico del controlador

Un desafío clave en la ciberseguridad en fabricación es mantener la seguridad sin comprometer la disponibilidad. Como indica la investigación de Omdia, el mayor impacto financiero de los ciberincidentes se produce cuando afectan a los sistemas de control de producción.

"Las operaciones de fabricación no permiten tiempos de inactividad como la infraestructura tradicional de IT", señaló Sperlich. "El parche rutinario de ciberseguridad o la respuesta a incidentes simplemente no son opciones en muchos entornos de producción. La seguridad debe estar integrada en lo fundamental de la arquitectura de sistemas industriales."

La seguridad eficaz en entornos de fabricación requiere múltiples capas de protección que funcionen sin interrumpir los procesos de producción. Esto incluye componentes seguros por diseño, segmentación de red, controles de acceso y capacidades de monitorización continua. Los controladores MX de Mitsubishi Electric integran estos principios de seguridad manteniendo el rendimiento operativo crítico para los entornos de fabricación.

Lo que distingue a los controladores industriales modernos en términos de seguridad es su capacidad para proteger tanto los entornos de tecnología operativa (OT) como de tecnología de la información (IT) manteniendo la producción continua. Los controladores MX establecen una frontera segura entre estos

entornos, ayudando a los fabricantes a implementar medidas de ciberseguridad efectivas sin interrumpir las operaciones.

Secure-by-Design: El nuevo estándar para los sistemas de control industrial. La industria de fabricación está respondiendo a estos desafíos con una mayor inversión en medidas de ciberseguridad y una mayor atención a los estándares de seguridad en los sistemas de control industrial. Esto incluye la adopción de marcos de seguridad diseñados para entornos industriales y implementar estrategias de defensa en profundidad que protejan activos críticos de producción.

"El panorama de seguridad para la fabricación seguirá evolucionando a medida que los actores amenazantes desarrollen nuevas técnicas", añade Daniel Sperlich. "Los fabricantes deben adoptar soluciones de seguridad que puedan adaptarse a estas amenazas cambiantes manteniendo la fiabilidad operativa que requieren los entornos de producción."

Los controladores MX abordan estos retos de seguridad en evolución mediante varias características clave alineadas con las normas internacionales de seguridad y la certificación IEC 62443-4-2. Estos incluyen comunicaciones cifradas para evitar escuchas ocultas y accesos no autorizados, y una autenticación completa de usuarios que permite establecer permisos de acceso y operación para diferentes usuarios según sus roles. Este enfoque permite una gestión de activos separada para diferentes partes interesadas, como usuarios finales y fabricantes de máquinas, manteniendo al mismo tiempo un entorno operativo seguro.

Además, la próxima función: las funciones integradas de servidor OPC UA del controlador permiten una conectividad segura entre los sistemas operativos y la infraestructura de TI, abordando una de las vulnerabilidades más significativas en entornos de fabricación: la frontera entre los sistemas de producción y las redes empresariales.

Seguridad bajo control(ler)

A medida que las amenazas cibernéticas en la fabricación se intensifican, los controladores de producción se han convertido en la piedra angular defensiva crítica en las estrategias de seguridad industrial. Estos sistemas ahora actúan como guardianes activos que protegen la integridad de entornos de producción completos, no solo de componentes operativos. Al implementar controladores robustos en el centro de las operaciones, las organizaciones transforman los puntos vulnerables en activos defensivos, garantizando tanto la continuidad operativa como la protección de datos en el hostil panorama digital actual.

Fuentes:

1. https://www.telstrainternational.com/content/dam/shared-componentes-activos/telstrainternacional/global/news-research/research/secure-manufacturing-the-challenges-it-ot-convergence/WP_IT-OT-security-convergence_manufacturing_digital.pdf
2. <https://www.dragos.com/ot-Informe de Ciberseguridad del Año/Informe de #anchor>
3. https://zayoeurope.com/wpcontenido/subidas/2024_2H_Zayo_DDoS_Insights_Report_v3.pdf
4. <https://www.ibm.com/thought-liderazgo/instituto-valor-empresarial/informe/indice de inteligencia de amenazas 2025>

Acerca de Mitsubishi Electric Corporation

Con más de 100 años de experiencia en el suministro de productos confiables y de alta calidad, Mitsubishi Electric Corporation (TOKYO: 6503) es un líder mundialmente reconocido en la fabricación, comercialización y venta de equipos eléctricos y electrónicos utilizados en procesamiento de la información y las comunicaciones, el desarrollo espacial y las comunicaciones por satélite, la electrónica de consumo, la tecnología industrial, la energía, la movilidad y los equipos de construcción. Mitsubishi Electric enriquece a la sociedad con la tecnología y adoptando el espíritu de su eslogan “Changes for the Better”. La compañía registró unos ingresos de 5.257,9 mil millones de yenes (34,8 mil millones de dólares*) en el año fiscal finalizado el 31 de marzo de 2024. Para obtener más información, visite www.MitsubishiElectric.com.

Acerca de Mitsubishi Electric Factory Automation Business Group

Al ofrecer una amplia gama de tecnologías de automatización y procesamiento, incluidos controladores, productos de accionamiento, productos de control y distribución de energía, máquinas de descarga eléctrica, máquinas de haz de electrones, máquinas de procesamiento láser, controladores numéricos computarizados y robots industriales, Mitsubishi Electric ayuda a aumentar la productividad y la calidad en la planta de producción. Además, sus extensas redes de servicio en todo el mundo brindan comunicación directa y soporte integral a los clientes. El eslogan global “Automating the World” muestra un enfoque de la empresa para aprovechar la automatización para mejorar la sociedad, a través de la aplicación de tecnología avanzada, el intercambio de conocimientos y el apoyo a los clientes como un socio de confianza.

Para obtener más información sobre la historia detrás de “Automating the World”, visite:

www.MitsubishiElectric.com/fa/about-us/automating-the-world

Factory Automation EMEA

Mitsubishi Electric Europe B.V., Factory Automation EMEA tiene su sede europea en Ratingen, cerca de Düsseldorf, Alemania. Es una parte de Mitsubishi Electric Europe B.V. que ha estado representada en Alemania desde 1978, una subsidiaria de propiedad total de Mitsubishi Electric Corporation, Japón. La función de Factory Automation EMEA es gestionar las ventas, el servicio y el soporte a través de su red de sucursales y distribuidores locales en toda la región EMEA.

Para obtener más información, visite emea.mitsubishielectric.com/fa

Acerca de e-F@ctory

e-F@ctory es el concepto integrado de Mitsubishi Electric para crear sistemas de fabricación fiable y flexibles que permitan a los usuarios alcanzar muchas de sus aspiraciones de fabricación de alta velocidad y basada en la información. A través de su actividad de soluciones asociadas, la e-F@ctory Alliance, y su trabajo con asociaciones de redes aciertas como la CC-Link Partners Association (CLPA), los usuarios pueden construir soluciones integrales basadas en un principio de “best in class”. En resumen, e-F@ctory y e-F@ctory Alliance permiten a los clientes lograr una fabricación integrada, pero aun así conservan la capacidad de elegir los proveedores y soluciones más óptimos.

**e-F@ctory, iQ Platform son marcas comerciales de Mitsubishi Electric Corporation en Japón y otros países.*

**Otros nombres y marcas pueden ser reclamados como propiedad de otros.*

**Todas las demás marcas comerciales son reconocidas*

Síguenos en:



[youtube.com/user/MitsubishiFAEU](https://www.youtube.com/user/MitsubishiFAEU)



<https://x.com/EsMitsubishi>



<https://www.linkedin.com/company/mitsubishielectric-automatizacion/>



https://www.instagram.com/mitsubishi_electric_fa_emea/

Contacto de prensa:

Mitsubishi Electric Europe B.V.

Factory Automation ES

Crta. De Rubí 76-80, E-08190 Sant
Cugat del Vallés (Barcelona), España

Tel: +34 935 653 131

Marketing.fad@sp.mee.com

Story/Editor:

Tigers Ltd.

Artur Kosior

Q22, Jana Pawła II 22

Warsaw, PL, 00-132

Tel.: +48 663 525 108

artur.kosior@tigers.pl

www.tigers.pl

Distribution/Circulation:

MEPAX

Jessica REITMAIER

Tel.: +34 (0) 695 202 002

j.reitmaier@mepax.com

www.mepax.com