Ciberseguridad OT en entornos críticos:

Cómo blindar operaciones industriales ante ciberataques

En un entorno donde las amenazas digitales evolucionan constantemente, la ciberseguridad OT se ha convertido en un pilar fundamental para la protección de los sistemas de control industrial. Un claro ejemplo de esta vulnerabilidad ocurrió en junio de 2020, cuando Honda se vio obligada a cerrar dos plantas automotrices tras sufrir un ataque de ransomware. Aunque la compañía aseguró que no se filtraron datos personales, las consecuencias económicas y reputacionales fueron significativas. Este tipo de incidentes evidencia la necesidad de adoptar estrategias robustas de ciberseguridad OT que garanticen la continuidad operativa y la integridad de las infraestructuras críticas.

Hoy en día, los titulares están inundados de noticias sobre ciberataques, lo que ha generado cierta insensibilización en la opinión pública. Sin embargo, el caso de Honda marcó un cambio significativo en las estrategias de los ciberdelincuentes: en lugar de atacar primero los sistemas de TI y luego la tecnología operativa (OT) y los sistemas de control industrial (ICS), ahora los ataques se dirigen directamente a la OT.

¿Por qué los ciberdelincuentes atacan los sistemas OT?

Los atacantes han identificado que los sistemas de tecnología operativa presentan vulnerabilidades clave:

- La conectividad ha aumentado significativamente en los sistemas de control industrial (ICS).
- La seguridad en los sistemas OT es menor en comparación con los sistemas de TI.
- La mayoría de las soluciones convencionales de ciberseguridad no protegen eficazmente los dispositivos OT.

Sectores más vulnerables a los ciberataques en OT

Las industrias con una alta presencia de tecnología operativa han sido blanco frecuente de ataques, incluyendo:

- Minería
- Energía y servicios públicos
- Transporte
- Petróleo y gas
- Manufactura

La interconectividad entre dispositivos y sistemas OT optimiza procesos industriales críticos, pero también aumenta la superficie de ataque. A medida que estos sistemas se integran más en la infraestructura de fabricación e instalaciones críticas, los riesgos de ciberataques y posibles interrupciones crecen exponencialmente.

¿Por qué los dispositivos OT son más vulnerables?

La tecnología operativa (OT) abarca dispositivos diseñados para gestionar, monitorear y mantener operaciones industriales, como sensores, actuadores, robots y controladores lógicos programables (PLC). Originalmente, estos equipos se desarrollaron sin considerar la seguridad cibernética, ya que operaban en entornos aislados sin conexión a Internet.
Sin embargo, la digitalización ha transformado el panorama. Cada vez más fabricantes han conectado sus dispositivos OT para mejorar el control, optimizar análisis y recibir alertas en tiempo real. No obstante, esta integración ha expuesto vulnerabilidades significativas:

- Las redes industriales incluyen dispositivos de múltiples fabricantes, dificultando una gestión unificada.
- Muchos dispositivos tienen credenciales débiles o contraseñas codificadas de fábrica.
- La gestión y operación de los sistemas OT suelen estar a cargo del equipo de manufactura, no de TI.
- Muchos sistemas OT no pueden ser actualizados o requieren tiempos de inactividad prolongados para aplicar parches de seguridad.
- El área de TI no siempre tiene visibilidad total de los dispositivos OT en operación.

Riesgos de seguridad en la convergencia OT-TI

La falta de control y monitoreo adecuado convierte a los dispositivos OT en el eslabón más débil de la ciberseguridad empresarial. Una vez que los atacantes logran ingresar a estos sistemas, pueden optar por mantenerse en la OT o moverse lateralmente hacia TI y otros dispositivos críticos de la organización. Desde allí, pueden:

- Siniestrar propiedad intelectual y datos sensibles.
- Monitorear el tráfico interno en busca de información confidencial.
- Tomar el control de operaciones industriales y de infraestructura crítica.

¿Por qué la protección de la OT es más importante que nunca?

Según un informe de Deloitte sobre el riesgo cibernético en la fabricación, un ciberataque puede generar la pérdida de ideas valiosas y afectar la ventaja competitiva de una empresa debido al impacto financiero y reputacional, especialmente cuando se comprometen datos confidenciales de clientes.

Al reconocer la vulnerabilidad de la tecnología operativa (OT), los ciberdelincuentes han cambiado su estrategia. Antes, atacaban los sistemas de TI y luego se desplazaban lateralmente hacia OT. Ahora, la situación ha cambiado: muchos atacantes apuntan directamente a la OT, debido a sus debilidades inherentes y menor protección en comparación con los sistemas de TI.

La evolución de las amenazas a la OT

Los ciberdelincuentes están desarrollando nuevas variantes de malware específicas para OT, como EKANS, diseñadas para explotar vulnerabilidades en sistemas de control industrial (ICS). Aunque el malware dirigido a ICS sigue siendo relativamente poco común, es casi seguro que aumentará en el futuro, como lo demuestran ataques recientes de alto perfil como Triton/Trisis e Industroyer.
Pero, ¿cuál es la principal razón por la que las empresas deben actuar ahora para proteger sus dispositivos OT? La falta de visibilidad del problema. Muchas organizaciones afectadas por ciberataques a la OT no hacen públicos los incidentes, lo que impide a otras empresas prepararse adecuadamente.
Un caso excepcional fue el del fabricante noruego de aluminio que, tras sufrir un ataque masivo de ransomware en 2019 que paralizó sus plantas por semanas y generó pérdidas de hasta 110 millones de dólares, decidió compartir los detalles del ataque para ayudar a otras organizaciones. Sin embargo, muchas empresas en EE.UU. y la UE siguen optando por el silencio debido al estigma asociado a las brechas de seguridad.

La importancia de una estrategia robusta de ciberseguridad OT

El hecho de que no se informe sobre los ataques no significa que no estén ocurriendo. Ante esta realidad, es crucial adoptar una estrategia efectiva de protección para los sistemas OT.
Una solución avanzada de seguridad para ICS debe permitir:

- **Bloquear ataques antes de que alcancen sistemas críticos de OT** mediante una prevención eficaz de amenazas.
- **Minimizar la exposición al riesgo** con políticas de seguridad automáticas fáciles de implementar.
- **Segmentar la red OT/TI** para aislar dispositivos vulnerables de funciones críticas.
- **Controlar la red con un análisis de riesgos integral** que permita visibilidad total sobre los sistemas industriales.

Solo se puede proteger lo que se puede ver. Con el aumento de los ataques dirigidos a OT, el departamento de TI ya no puede ignorar esta amenaza. La **ciberseguridad OT** debe ser una prioridad para evitar interrupciones operativas, pérdidas económicas y daños a la reputación corporativa. Implementar soluciones de protección adecuadas permitirá que los sistemas de TI y OT trabajen.

La **creciente amenaza de ciberataques** dirigidos a la **tecnología operativa (OT) y los sistemas de control industrial (ICS)** exige una respuesta inmediata. **Los ataques recientes han demostrado que la OT es un objetivo primario** debido a sus vulnerabilidades, y muchas empresas aún desconocen la magnitud del problema. La falta de divulgación de estos incidentes no significa que no ocurran, sino que agrava el riesgo de futuras brechas de seguridad. Proteger los dispositivos OT con soluciones avanzadas de ciberseguridad es clave para preservar la reputación de la empresa, además de prevenir interrupciones operativas y reducir pérdidas económicas significativas.

Procetradi es una empresa con amplia experiencia en la implementación de soluciones de ciberseguridad OT para el sector industrial y minero. Con un enfoque integral, ayuda a las organizaciones a proteger sus infraestructuras críticas contra amenazas digitales, garantizando la continuidad operativa y el resguardo de activos estratégicos. Gracias a su profundo conocimiento en ciberseguridad y tecnología industrial, Procetradi se posiciona como un socio clave para aquellas empresas que buscan fortalecer su resiliencia frente a los ciberataques en entornos OT e ICS.

Soluciones tecnológicas únicas de clase mundial

CONTÁCTANOS

soluciones@procetradi.com

www.procetradi.com

T: +(51) 445-1862 | +(51) 445-2115 | +(51) 445-7660

Av. Benavides 1850 Of. 301 Miraflores
Lima – Perú