La lucha actual para proteger los PLC y las redes TO

Han pasado muchos años desde que el infame ataque Stuxnet puso de relieve las vulnerabilidades de los sistemas de tecnología operativa (TO) que desempeñan un papel crucial en nuestra infraestructura crítica. Sin embargo, a pesar de los avances, estos sistemas siguen expuestos, lo que genera preocupación sobre nuestra preparación para futuras amenazas cibernéticas.

Publicación original de Segu Info
https://blog.segu-info.com.ar/2024/03/la-lucha-actual-para-proteger-los-plc-y.html

Lectura recomendada por Diego Romero
Miembro del Consejo Editorial
romero.diego.m@gmail.com

Nota del editor: Este artículo fue originalmente escrito por Nitzan Daube para Dark Reading, disponible en *https://www.darkreading.com/ics-ot-security/ongoing-struggle-to-protect-plcs*

Vulnerabilidad de TO

Un desafío central de la vulnerabilidad TO radica en el comportamiento humano. Los actores de amenazas explotan el comportamiento humano. Esto conduce a contraseñas débiles, actualizaciones desatendidas y un cumplimiento poco estricto de los protocolos. Al explotar estas tendencias, los delincuentes informáticos convierten contraseñas fáciles de adivinar en claves maestras y aprovechan vulnerabilidades sin parches para obtener acceso.

La convergencia de TI y TO crea un arma de doble filo. Si bien fomenta la eficiencia y la innovación, también amplía la superficie de ataque. La creación de una red para gestionar dispositivos críticos (como los PLC) que controlan maquinaria y la interconexión de TI y TO tiene el potencial de convertirse en una pesadilla de seguridad.

La convergencia de TI y TO crea un arma de doble filo. Si bien fomenta la eficiencia y la innovación, también amplía la superficie de ataque.

Lo mejor es un enfoque en capas para la seguridad de OT

En principio, se recomienda el uso de tecnología que aplique medidas de seguridad, como la utilización de protocolos de cifrado modernos. Aunque esto ofrece protecciones valiosas, está lejos de ser infalible. Los actores de amenazas decididos aún pueden explotar vulnerabilidades sin parches o aprovechar vectores de ataque alternativos, como la convergencia de TI y TO. Por ejemplo, a la hora de atacar PLC, quizá un atacante puede enviar instrucciones API directamente al dispositivo, y que estas sean dañinas para los procesos críticos.

Sería recomendable implementar el enfoque de defensa en profundidad para las operaciones de la planta y configurar el entorno de acuerdo con lineamientos operativos para seguridad industrial.

No confíes en nadie

Aquí es donde la protección a nivel de dispositivo se vuelve crucial. Proteger y asegurar dispositivos, como los PLC, proporciona una solución tanto para las crecientes superficies de ataque como para el elemento humano. La seguridad implica un enfoque simple: no confíes en nadie. Por lo tanto, aplicar y hacer cumplir la confianza cero ayuda a proteger la infraestructura crítica.

Promover estas políticas de seguridad sólidas y establecer pautas claras para un entorno TO seguro implica una verificación meticulosa de cada intento de acceso a los PLC. Además, a usuarios específicos se les deben conceder solamente los permisos mínimos necesarios. Tanto los equipos de seguridad como los gerentes de TO deben defender los controles de acceso, garantizando que solo los usuarios autorizados puedan interactuar con los PLC que controlan los sistemas críticos en la fábrica. La aplicación de estas políticas de seguridad evita que determinados atacantes envíen instrucciones API directamente al PLC.

Promover estas políticas de seguridad sólidas y establecer pautas claras para un entorno TO seguro implica una verificación meticulosa de cada intento de acceso a los PLC.

Construir resiliencia

Las vulnerabilidades de los PLC sirven como un crudo recordatorio de la lucha actual para proteger nuestra infraestructura crítica.

La ciberseguridad debe ser parte de las responsabilidades de los gerentes de TO y equipos de TI. Deben comprender que es necesario un enfoque por niveles, y que el primer nivel es la protección de los PLC. Hacer cumplir y gestionar el acceso y las credenciales a los PLC transforma la infraestructura vulnerable en infraestructura resiliente. ❖