Claves para defender la infraestructura crítica ante los ciberataques

Organizaciones estadounidenses presentaron acciones para reducir las ciberamenazas contra la tecnología operacional.

Lectura recomendada por Ing. Diego Romero
Miembro del Comité Editorial
https://www.linkedin.com/in/diegoromero/

Glosario de siglas

- CISA: *Cybersecurity and Infrastructure Security Agency*, 'Agencia de Seguridad de Infraestructura y Ciberseguridad', de Estados Unidos
- DOE: *Department of Energy*, 'Departamento de Energía', de Estados Unidos
- EPA: *Environmental Protection Agency*, 'Agencia de Protección Ambiental', ed Estados Unidos
- FBI: *Federal Bureau of Investigation*, 'Oficina Federal de Investigación', de Estados Unidos
- ICS: *Industrial Control System*, 'sistema de control industrial'
- MFA: *Multi-Factor Authentication*, 'autenticación multifactor'
- SCADA: *Supervisory Control and Data Acquisition,* 'supervisión, control y adquisición de datos'
- TI: tecnologías de la información
- TO: tecnologías operacionales
- VPN: *Virtual Private Network*, 'red privada virtual'

URL estable: https://www.editores.com.ar/node/8325

Actores no muy sofisticados están apuntando a los sistemas ICS/SCADA en los sectores de energía y transporte. Como respuesta, las agencias estadounidenses CISA y EPA, el FBI y el DOE presentaron una hoja informativa de consulta sobre ciberseguridad llamada "Mitigaciones primarias para reducir las ciberamenazas contra la tecnología operacional".

Los ciberincidentes que atacan a la tecnología operacional y a los sistemas de control industrial de infraestructura crínica están aumentando rápidamente

Los ciberincidentes que atacan a la tecnología operacional y a los sistemas de control industrial de infraestructura crítica están aumentando rápidamente a lo largo de todo Estados Unidos. Estos subrayan la urgencia de que dueños y operarios tomen acciones a favor de fortalecer sus defensas de ciberseguridad contra amenazas que apuntan directamente a su TO conectada a internet y sus ambientes ICS.

Documento original disponible en
https://www.ic3.gov/CSA/2025/250506.pdf

Acciones recomendadas

Organizaciones de Estados Unidos con autoridad sobre el tema urgen a las partes interesadas en infraestructura crítica a implementar las siguientes medidas:

- Desconectar las conexiones TO de la internet pública. Los dispositivos TO son blancos fáciles cuando están conectados a internet: carecen de métodos de autenticación y autorización que sean resistentes a las amenazas modernas y se encuentran fácilmente buscando puertos abiertos dentro de rangos de IP públicos, por medio de herramientas de búsqueda que identifican a víctimas que cuentan con componentes TO.

- Los atacantes utilizan herramientas simples, repetibles y escalables disponibles para cualquiera con un navegador de internet. Las entidades con infraestructura crítica deberían identificar cuáles de sus componentes están abiertos al público y evitar la exposición no intencional.

» Cambiar las claves recibidas por default inmediatamente por claves únicas y más fuertes. Análisis recientes sobre esta ciberactividad indica que los sistemas en la mira de los atacantes utilizan claves recibidas por default o fácilmente adivinables con herramientas de fuente abierta. Cambiar las claves recibidas por default es especialmente importante para los dispositivos conectados a internet que tienen la capacidad de controlar procesos o sistemas TO.

» Asegurar el acceso remoto a las redes TO. Muchas entidades con infraestructura crítica o terceros contratados por ellas llevan a cabo acciones riesgosas cuando implementan el acceso remoto a los dispositivos TO. Esto merece una reevaluación cuidadosa. Si el acceso remoto es esencial, se debe mejorar la conexión con una red privada a fin de quitar los dispositivos TO de la internet pública y usar una VPN con una clave fuerte y MFA resistente al *phishing*.

- Documentar y configurar soluciones de acceso remoto: aplicar principios de privilegio mínimo para dispositivos específicos; asignar roles de usuario o rangos de trabajo. Más aún, desactivar cuentas inactivas.

» Segmentar redes TI y TO. Segmentar sistemas críticos e introducir una zona desmilitarizada para pasar datos de control a la logística de la organización reduce el impacto potencial de una ciberamenaza, también reduce el riesgo risk de disrupción de operaciones esenciales de TO.

» Practicar y mantener la posibilidad de operar los sistemas TO de forma manual. La capacidad de las organizaciones de volver a los controles manuales para restaurar rápidamente las operaciones es vital inmediatamente después de un incidente. La continuidad de un negocio y los planes de recuperación tras el

Fuente: Flickr

desastre, mecanismos libros de falla, capacidad de aislación, respaldos de software, y sistemas en *standby*, todos deberían ser testeados de forma rutinaria para garantizar operaciones manuales seguras ante un incidente.

Las organizaciones a cargo de estas recomendaciones también aconsejan a todos aquellos que cuenten con infraestructura crítica que se comuniquen regularmente con sus proveedores de servicios, integradores de sistemas y fabricantes de sistemas, quienes quizá puedan proveer una orientación específica para asegurar su TO.

Las configuraciones incorrectas pueden ser introducidas durante las operaciones estándar, por el integrador del sistema, por un proveedor de servicios o como parte de la configuración predeterminada del fabricante del sistema. Colaborar con los grupos pertinentes para abordar estos problemas puede prevenir la introducción de futuras vulnerabilidades no intencionadas.

Colaborar con los grupos pertinentes para abordar estos problemas puede prevenir la introducción de futuras vulnerabilidades no intencionadas

Recursos adicionales de CISA

Para aumentar aún más los esfuerzos de mitigación de ciberamenazas, es bueno repasar las siguientes guías y herramientas de CISA:

- Descripción general de las herramientas que ayudan a identificar dispositivos públicos en internet y cómo reducir la exposición a ataques: "Stuff off Search", en la web de CISA.
- Uso de contraseñas seguras: "Use Strong Passwords", en la web de CISA.
- MFA resistente al phishing: hoja informativa de CISA "Implementación de MFA resistente al phishing".
- Segmentación de la red: hoja informativa de CISA "Escalonamiento de la seguridad de la red mediante la segmentación".
- Adquisición de componentes TO seguros por diseño: "Consideraciones prioritarias para propietarios y operadores de tecnología operativa cuando seleccionan productos digitales", de CISA.
- Principales medidas cibernéticas para proteger los sistemas de agua y los recursos correspondientes: "Principales medidas cibernéticas para proteger los sistemas de agua", de CISA.
- Segmentación de la red en sistemas de agua: guía de la EPA sobre la mejora de la ciberseguridad en los sistemas de agua potable y aguas residuales, hoja informativa 2.F.

Nota del editor: El artículo aquí presentado es una traducción realizada por Alejandra Bocchio especialmente para esta publicación. El artículo original en inglés fue publicado en el newsletter Cyber Security Hub, disponible en https://www.linkedin.com/pulse/cisa-fbi-release-mitigations-reduce-cyber-threats-a9vdc/.