Costo: $$$	Impacto: MEDIO	Complejidad: MEDIO

2.X: ¿Elimina el WWS las conexiones entre los activos de TO e Internet?

Recomendación: Elimine las conexiones de los activos de TO al Internet público, a menos que sea explícitamente necesario para las operaciones.

¿Por qué es importante este control?

Los desarrolladores no diseñaron los sistemas de SCADA y TO teniendo en cuenta la ciberseguridad, y la mayoría de los WWS no los parchean ni los actualizan periódicamente. Conectar directamente la TO a Internet puede presentar un importante riesgo de ciberseguridad para las operaciones del WWS. Su empresa de servicios públicos debe saber qué activos SCADA o de TO tiene el WWS conectados a Internet y eliminar la conexión a Internet si es posible.

Si las necesidades operacionales requieren una conexión a Internet (p. ej., gestión de sitios remotos), puede reducir el riesgo informático introducido por estas conexiones mediante controles de compensación como MFA, cortafuegos y registro centralizado.

Consejos de implementación

Identifique y desconecte todos los activos de TO de Internet. Verifique la conectividad estándar (p. ej., la red SCADA conectada a la red de TI o al módem de Internet) y otros métodos (p. ej., inalámbricos o celulares) para conectar los activos de TO a Internet.

Su WWS debe justificar formalmente las conexiones a Internet a todos los activos de TO e incluir controles de compensación.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control AC-17 (página 48) y SC-7 (página 297) para obtener más información sobre el acceso remoto (sección "Remote Access") y la protección de límites (sección "Boundary Protegerion"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

ORIENTACIÓN ADICIONAL

- Como se menciona en la hoja informativa 2.W, un WWS puede buscar activos de TO expuestos a Internet mediante Shodan o los servicios gratuitos de análisis de vulnerabilidades de la CISA del DHS. Un ejemplo de una conexión que se pasa por alto fácilmente entre los sistemas de TO e Internet es el uso de módems celulares para conectar activos remotos (p. ej., tanques, estaciones elevadoras, pozos) al sistema SCADA principal. Cuando se utilizan, los módems celulares deben estar en las redes privadas del proveedor de telecomunicaciones siempre que sea posible.
- El WWS debe crear un proceso para justificar y documentar la necesidad operacional de una conexión de TO a Internet con el líder de ciberseguridad de TO. Cuando las necesidades operacionales requieren una conexión aprobada de TO a Internet, el WWS debe utilizar los controles de compensación detallados en la hoja informativa 2.W para mitigar el riesgo informático que crea esta conexión.

Servicios de higiene informática de la CISA del DHS: Consulte este recurso para obtener más información sobre el servicio gratuito de análisis de vulnerabilidades del DHS. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: Consulte este recurso para buscar activos conectados a Internet en la red del WWS. *https://www.shodan.io/*

Principales medidas informáticas para proteger los sistemas de agua de la CISA: *Consulte el punto 1 en la página 1 de este recurso para obtener información adicional.* *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*