Costoo: $$	Impactoo: ALTO	Compleijidad: MEDIA

1.A: ¿Mantiene el WWS un inventario actualizado de todos los activos de la red de tecnología operacional (TO) y tecnología de la información (TI)?

Recomendación: Revise periódicamente (como mínimo, trimestralmente) y mantenga una lista de todos los activos de TO y TI con una dirección IP. Esto incluye equipos de terceros y heredados (es decir, antiguos).

¿Por qué es importante este control?

El WWS no puede proteger ni asegurar lo que usted no conoce. Un inventario preciso de los activos tecnológicos de TO (p. ej., SCADA, PLC, HMI) y de TI (p. ej., computadoras de oficina, conmutadores de red, servidores) es una parte fundamental de la ciberseguridad del WWS. Una vez que su WWS conozca qué activos tiene, puede realizar las mejoras de ciberseguridad necesarias en las redes de TO y TI.

ORIENTACIÓN ADICIONAL

- Según la revisión, actualice los registros desactualizados de los activos conocidos, agregue activos previamente desconocidos al inventario y elimine de la lista los activos que el WWS ya no utiliza.
- Asegúrese de que la lista identifique los activos físicos e incluya detalles sobre los activos, incluyendo la forma en que están conectados, los datos que comparten y quién en el WWS (o qué distribuidor) trabaja con el activo.

Consejos de implementación

Existen varios métodos para realizar el inventario de activos, y el mejor

enfoque es una combinación de inspección física, análisis pasivo, análisis activo y análisis de configuración (instalación).

El WWS debe conocer qué activos tiene, cómo están configurados esos activos (consulte la hoja informativa 2.O) y cómo están conectados esos activos (consulte la hoja informativa 2.P).

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control CM-8 (página 107) para obtener más información sobre el inventario de componentes del sistema (sección “System Component Inventory”). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Guía de plantillas de políticas del NIST: Consulte la sección 4.6, “IT Asset Management” (Gestión de activos de TI) de la Política de seguridad de la información. *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

Publicación del blog del SANS Institute sobre seguridad de los sistemas de control industriales (ICS) “Conózcase a usted mismo mejor que el rival: identificación y seguimiento de activos de los ICS”: Proporciona información sobre la identificación y el seguimiento de activos. *https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/*

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 5 (Contabilizar los activos críticos) proporciona información sobre cómo identificar, inventariar, clasificar y documentar los activos críticos de ICS/OT. *https://www.waterisac.org/fundamentals*

Principales medidas informáticas para proteger los sistemas de agua de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA): Consulte el punto 4 de la página 2 de este recurso para obtener información adicional. *https://www.cisa.gov/Recursos-tools/Recursos/top-cyber-actions-securing-water-systems*