

Costo: \$\$

Impacto: MEDIO

Complejidad: MEDIO

2.P: ¿Mantiene el WWS documentación actualizada que describe la topología de la red (es decir, las conexiones entre todos los componentes de red) en las redes de TO y TI del WWS?

Recomendación: Mantenga documentación completa y precisa sobre todas las topologías de red de TO y TI del WWS para facilitar la respuesta y recuperación de incidentes.

¿Por qué es importante este control?

Una topología de red bien definida ayuda a los administradores del sistema a localizar fallas, solucionar problemas y asignar recursos de red. Los diagramas/topologías de la red son un punto de referencia importante para diagnosticar problemas de red e identificar posibles vulnerabilidades de seguridad, ya que representan diseños físicos y lógicos. Un diagrama de red lógico completo y actualizado es esencial para la recuperación ante desastres informáticos.

Consejos de implementación

Para crear una topología de red precisa, su WWS debe realizar una inspección de la red para validar las vías de conexión conocidas y desconocidas anteriormente. Cuando realice esta inspección, incluya conexiones de red basadas en Ethernet tradicionales y vías menos tradicionales, como comunicaciones seriales, inalámbricas, de acceso telefónico y de línea de visión. Cuando haya activos remotos (p. ej., tanques, estaciones elevadoras), evalúe cómo se comunican estos activos con la red del WWS.

Después de completar la inspección de la red, documente los resultados y manténgalos actualizados. La

documentación de la inspección debe incluir detalles sobre los activos específicos de la red, las conexiones y el método utilizado para la conexión (p. ej., cableado, inalámbrico). Su empresa de servicios públicos debe centrarse especialmente en los sistemas que se conectan directamente al Internet público y en las vías de comunicación entre los sistemas de TO (p. ej., SCADA) y TI (es decir, de la empresa comercial). Su WWS puede realizar una inspección de la red al mismo tiempo que la revisión de la configuración de los activos que se detalla en la hoja informativa 2.O y el proceso de inventario de activos que se detalla en la hoja informativa 1.A. Un sitio web gratuito y fácil de usar que puede ayudarlo a crear diagramas de red es Lucidchart. Microsoft proporciona un breve desglose de lo que se debe incluir en un diagrama

ORIENTACIÓN ADICIONAL

- Para ser eficiente, un WWS puede realizar una inspección de la red al mismo tiempo que la revisión de la configuración de los activos que se detalla en la hoja informativa 2.O y el proceso de inventario de activos que se detalla en la hoja informativa 1.A. Un sitio web gratuito y fácil de usar que puede ayudarlo a crear diagramas de red es Lucidchart. Microsoft proporciona un breve desglose de lo que se debe incluir en un diagrama de red. La herramienta CSET de la CISA es una versión gratuita de gráficos básicos relacionados con Visio y TO para crear topologías de red.
- Considere incluir el diagrama de la red en el plan de respuesta a incidentes (IR) o el plan de respuesta a emergencias de ciberseguridad del WWS, ya que esta información puede ser valiosa para la respuesta a incidentes..

de red. La herramienta CSET de la CISA tiene una versión gratuita de gráficos básicos relacionados con Visio y TO para crear topologías de red.

Para una respuesta y recuperación a incidentes efectiva, es esencial mantener una documentación completa y precisa de todas las topologías de red de TO y TI del WWS. Esta documentación detallada ayuda a identificar y abordar las vulnerabilidades. Además, es recomendable incorporar un texto en los acuerdos con proveedores de servicios externos, como distribuidores, integradores y proveedores de servicios gestionados (MSP), que los obligue a respaldar estos esfuerzos de documentación. Dichas cláusulas deben garantizar que los terceros aporten la información y la asistencia necesarias para mantener una documentación de topología de red actualizada y completa.

Considere incluir el diagrama de la red en el plan de respuesta a incidentes (IR) de ciberseguridad, ya que esta información puede ser valiosa para la respuesta a incidentes.

Recursos

Lucidchart: Lucidchart es una aplicación de diagramas basada en la web que permite a los usuarios colaborar visualmente en el dibujo, la revisión y el intercambio de gráficos y diagramas y mejorar procesos, sistemas y estructuras organizacionales.

<https://www.lucidchart.com/pages/examples/diagram-maker>

Crear un diagrama básico de red (Microsoft): Si el WWS utiliza el *software* Microsoft Visio, esta página describe cómo la plantilla de diagrama de red básica incluye formas estándar para servidores, computadoras y otras partes de la red de un WWS.

<https://support.microsoft.com/en-us/office/create-a-basic-network-diagram-f2020ce6-c20f-4342-84f7-bf4e7488843a>

Herramienta CSET de la CISA del DHS: Esta aplicación de escritorio independiente guía a un WWS a través de un proceso sistemático de evaluación de sus activos de TO y TI, incluyendo los diagramas de red.

<https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr>