Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.O: ¿Mantiene el WWS documentación actualizada que explica la preparación y los ajustes (es decir, la configuración) de los activos críticos de TO y TI?

Recomendación: Mantenga documentación precisa sobre la configuración original y actual de los activos de TO y TI, incluyendo la versión de *software* y *firmware*.

¿Por qué es importante este control?

Si bien su WWS puede conocer los activos físicos que existen en sus redes informáticas mediante un inventario de activos (consulte la hoja informativa 1.A), también es importante comprender la configuración (es decir, los ajustes) de sus activos. Los atacantes suelen aprovechar vulnerabilidades (es decir, debilidades) que solo existen en ciertas versiones o configuraciones del *software* y *firmware* que se utilizan para controlar los activos. Por lo tanto, debe ser consciente de las configuraciones de los activos para saber si una vulnerabilidad recién descubierta podría utilizarse en un ataque a la red.

Además, si un atacante cambia las configuraciones de los activos, borra los ajustes o deshabilita los activos, una documentación de configuración bien mantenida permitirá que su empresa de servicios públicos detecte los cambios con mayor facilidad, restablezca los ajustes adecuados y mantenga o restaure las operaciones.

ORIENTACIÓN ADICIONAL

- Para documentar completamente las configuraciones de los activos, incluya los siguientes detalles, según corresponda: propietario (p. ej., el Departamento de Ingeniería), ubicación física y de red, distribuidor, tipo de activo, modelo, nombre del activo, versiones de firmware o software, niveles de parches, configuraciones del activo, servicios activos (es decir, procesos automatizados), protocolos de comunicación, direcciones de red (p. ej., IP y MAC), valor del activo y criticidad para las operaciones del WWS.
- Para ser eficiente, un WWS puede realizar una revisión de la configuración de sus activos al mismo tiempo que el proceso de inventario de activos que se detalla en la hoja informativa 1.A y la inspección de la red que se detalla en la hoja informativa 2.P. La información de configuración es importante para prepararse o responder a un ataque informático; sin embargo, también sería valiosa para un atacante, por lo que el WWS debe protegerla como corresponde.

Consejos de implementación

Revise y actualice la documentación de configuración de forma programada periódicamente.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte la familia de controles CM-1 (página 96) y el control CM-6 (página 103) para obtener más información sobre la gestión de configuración (sección "Configuration Management") y los ajustes de configuración (sección "Configuration Settings"). https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de políticas del NIST: Consulte el punto 4.11b), “System Security” (Seguridad del sistema) de la Política de seguridad de la información. Un documento que detalla las configuraciones de activos de TO y TI.
https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx