Costo: $$$	Impacto: ALTO	Complejidad: ALTO

2.V: ¿Prohíbe el WWS la conexión de *hardware* no autorizado (p. ej., unidades USB, medios extraíbles, computadoras portátiles ingresadas al sitio por otras personas) a los activos de TO y TI?

Recomendación: Cuando sea factible, quite, deshabilite o proteja de algún modo los puertos físicos (p. ej., puertos USB en una computadora portátil) para evitar la conexión a activos no autorizados.

¿Por qué es importante este control?

Permitir que solo los activos autorizados se conecten a las redes del WWS ayuda a evitar que los atacantes ingresen o roben datos de esas redes.

Conectar un activo USB malicioso a la red del WWS puede provocar una filtración, interrupción o daño en el sistema. El ejemplo más conocido de un atacante que utilizó una unidad de USB para dañar una planta industrial es Stuxnet, el primer programa malicioso conocido públicamente diseñado para atacar sistemas de TO. Incluso si su WWS no conecta una red a Internet (p. ej., una desconexión física), aún podría ser vulnerable a ataques desde conexiones directas.

Consejos de implementación

Desactive las funciones de ejecución automática que otorgan acceso automático a medios extraíbles (p. ej., unidades USB) cuando se conectan a una computadora.

Permita el acceso a puertos de conexión físicos en computadoras solo a través de excepciones aprobadas.

ORIENTACIÓN ADICIONAL

- Los WWS pueden detener el uso no autorizado de activos mediante el uso de rejas físicas para cubrir los puertos de las computadoras, a través de políticas administrativas (menos efectivas) o deshabilitando los permisos técnicos mediante una política para toda la organización dentro de Microsoft Windows. Si un WWS permite a los usuarios conectar activos externos a sus sistemas, el WWS debe revisar los activos en busca de programas maliciosos antes de conectarlos. Los WWS generalmente pueden configurar un software antivirus para analizar automáticamente las unidades externas, como las unidades USB, cuando un usuario las inserta.
- Si es necesario, establezca un proceso administrativo donde un usuario pueda solicitar una excepción para usar un activo externo justificando la necesidad operacional. El personal de TO/TI o el administrador del sistema correspondiente deberán sopesar la necesidad operacional frente al riesgo potencial de seguridad para los sistemas informáticos del WWS.

Recursos

Stuxnet (MITRE ATT&CK): Consulte “Replication Through Removable Media” (Replicación a través de medios extraíbles) para obtener más información sobre la propagación de Stuxnet. *https://attack.mitre.org/software/S0603/*

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control MP-7 (página 176) y SC-41 (página 326) para obtener más información sobre el uso de medios (sección "Media Use") y el acceso a puertos y dispositivos de E/S (sección "Port and I/O Device Access"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Guía de plantillas de políticas del NIST: Consulte la sección 4.6b, "IT Asset" (Activo de TI) de la Política de seguridad de la información, una política administrativa escrita que prohíbe el uso de unidades USB y otros medios extraíbles cuando sea apropiado. *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

Habilitación y deshabilitación de la ejecución automática (Microsoft Learn): Consulte la sección "Using the Registry to Disable AutoRun" (Uso del registro para deshabilitar la ejecución automática) para obtener más información. *https://learn.microsoft.com/en-us/windows/win32/shell/autoplay-reg#using-the-registry-to-disable-autorun*