Costo: $$$	Impacto: ALTO	Complejidad: ALTO

2.F: ¿Segmenta el WWS las redes de TO y TI y deniega las conexiones a la red de TO de forma predeterminada, a menos que se permita explícitamente (p. ej., por dirección IP y puerto)?

Recomendación: Requiera que las conexiones entre las redes de TO y TI se realicen a través de un intermediario, como un cortafuegos, un servidor bastión, un servidor de accesos directos o una zona desmilitarizada, que se monitorea y registra.

¿Por qué es importante este control?

Este control es importante porque un WWS puede limitar la capacidad de un atacante de acceder a los sistemas de control de TO después de comprometer la red de TI.

Los sistemas de TO no fueron diseñados originalmente con el mismo nivel de seguridad que las redes de TI. A medida que Internet se hizo popular, las organizaciones generalmente mantuvieron las redes de TO separadas de los sistemas de TI, dejando lo que se llama una "desconexión física" entre las redes de TO y TI. Sin embargo, con el tiempo, las organizaciones se dieron cuenta de que podían obtener eficiencia operacional y ahorro de costos al conectar los sistemas de TO y TI y compartir datos entre ellos.

Si bien el concepto de una desconexión física sigue siendo una respuesta popular a las preocupaciones de seguridad de conectividad TO/TI, es prácticamente imposible mantener uno incluso en las instalaciones más seguras (p. ej., Stuxnet, 2010). Por lo tanto, la mayoría de los ataques informáticos que apuntan a las redes de TO comienzan como ataques a la red de TI de un WWS.

ORIENTACIÓN ADICIONAL

- Un marco útil para comprender dónde segmentar la red es la arquitectura de referencia empresarial de Purdue (PERA), o modelo de Purdue para abreviar. Este modelo separa las redes de TO y TI en capas, lo que ayuda a diferenciar los tipos de activos en cada nivel de una red de sistema de control. Los niveles 0 a 3 consisten en activos de TO y los niveles 4 y 5 se refieren a la red empresarial de TI. La segmentación de la red se produce principalmente entre las redes de TO y TI en los niveles 3 y 4, donde un WWS puede establecer una "zona desmilitarizada" como amortiguador entre las redes de TO y TI utilizando herramientas de hardware y software para monitorear, registrar y filtrar el tráfico.
- De forma predeterminada, deniegue todas las conexiones a la red de TO desde la red de TI a menos que se permita explícitamente (por dirección IP y puerto) para una funcionalidad específica del sistema.

La segmentación es una práctica de seguridad que divide digitalmente las redes informáticas de TO y TI de un WWS con la meta de mejorar el desempeño de la red y la ciberseguridad.

Consejos de implementación

Permita únicamente conexiones a la red de TO desde la red de TI a través de activos y otros medios aprobados.

La herramienta más común que un WWS puede utilizar para la segmentación de la red es instalar un cortafuegos en el límite entre las redes de TO y TI que puede denegar todas las conexiones entre los sistemas de TO y TI de forma predeterminada. Con un cortafuegos,

un WWS puede controlar el flujo de información entre subredes o sistemas por tipo de tráfico, origen, destino y otras opciones.

Para fortalecer las medidas de ciberseguridad en los entornos operacionales, se recomienda segmentar la red de TO en función de áreas operacionales específicas, como estaciones de bombeo individuales, para localizar y mitigar de manera eficaz la propagación de posibles incidentes informáticos. Además, el acceso desde la red de TI a la red de TO debe configurarse en modo de solo lectura para evitar acciones no autorizadas, excepto cuando se accede a un servicio de escritorio remoto (RDS), donde los usuarios deben volver a autenticarse para garantizar un acceso seguro y controlado. Este enfoque no solo fortalece la situación de seguridad, sino que también garantiza el cumplimiento de las buenas prácticas establecidas, lo que mejora la protección en todas las redes.

Recursos

Estándar 800-82 (revisión 3) del NIST, Guía para la seguridad de la tecnología operacional (TO): Consulte las secciones 5 y 6 y el Apéndice E para obtener más información sobre la segmentación y segregación de la red (sección "Network Segmentation and Segregation"). *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control AC-4 (página 28) y SC-7 (página 297) para obtener más información sobre la aplicación del flujo de información (sección "Information Flow Enforcement") y la protección de límites (sección "Boundary Protegerion"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Aviso de la Agencia de Seguridad Nacional (NSA) "Detener la actividad informática maliciosa contra la TO conectada": Este aviso enumera los pasos que un WWS puede tomar para evaluar los riesgos contra su sistema de TO a través de la conexión del sistema de TI e implementar cambios con los recursos actuales para monitorear y detectar de manera realista la actividad maliciosa. *https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF*

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/*

El modelo de Purdue y buenas prácticas para arquitecturas ICS seguras (SANS Institute): Consulte este recurso para obtener más información sobre el modelo de Purdue y dónde se produce la segmentación de red en una red de TO. *https://www.sans.org/blog/introduction-to-ics-security-part-2/*

Comprender los cortafuegos para uso doméstico y en pequeñas oficinas (CISA del DHS): Consulte este recurso para obtener más información sobre cómo seleccionar y configurar un cortafuegos. *https://www.cisa.gov/tips/st04-004*