Costo: $	Impacto: ALTO	Complejidad: BAJA

2.W: ¿Se asegura el WWS de que los activos conectados al Internet público no exponen de manera innecesaria servicios que se pueden aprovechar (p. ej., protocolo de escritorio remoto)?

Recomendación: Elimine los puertos y servicios expuestos de manera innecesaria en activos públicos y realice revisiones periódicas.

¿Por qué es importante este control?

Este control es importante porque cerrar los puertos y servicios al Internet público ayuda a evitar que los atacantes accedan a la red. Si su WWS conecta un puerto o servicio (es decir, un programa) a Internet, existe una vía para un ataque informático y debe implementar medidas de seguridad para abordarlo. Un perímetro de red es el límite seguro entre el lado de la red que da al WWS (la intranet) y el lado de la red que da al Internet público. El perímetro contiene los puertos o "entradas" que los atacantes intentan usar para obtener acceso a la intranet de un WWS.

ORIENTACIÓN ADICIONAL

- Puede buscar puertos y servicios expuestos a Internet utilizando Shodan (un "motor de búsqueda" para activos expuestos a Internet) para los activos de su red. Además, la CISA del DHS ofrece servicios gratuitos de análisis de vulnerabilidades que buscan servicios expuestos a Internet y alertan al WWS sobre los resultados.
- A veces, su WWS debe conectarse y, por lo tanto, exponer un servicio o puerto al Internet público debido a requisitos operacionales. En estos casos, el WWS debe utilizar un servicio de MFA (p. ej., Duo, Okta, RSA) para restringir el acceso a los usuarios autorizados y un cortafuegos para filtrar el tráfico inusual, y el WWS debe monitorear el acceso a la red y los registros de actividad para detectar acciones inusuales que puedan indicar un ataque informático.

Consejos de implementación

Implementar controles compensatorios adecuados (p. ej., cortafuegos, autenticación multifactor o registro y monitoreo de actividad) para todos los servicios (p. ej., acceso remoto, alojamiento web) conectados al Internet público para prevenir formas comunes de ataque.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control AC-17 (página 48) y SC-7 (página 297) para obtener más información sobre el acceso remoto (sección "Remote Access") y la protección de límites (sección "Boundary Protegerion").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de gestión de políticas del NIST: Consulte el Estándar de análisis de vulnerabilidades: Plantilla de SOP para análisis de vulnerabilidades.
https://www.cisecurity.org/wp-content/uploads/2020/06/Vulnerability-Scanning-Standard.docx

Alertas AA21-042A y AA21-287A de la CISA del DHS: Consulte estos recursos para obtener información sobre diversas filtraciones en sistemas de agua entre 2019 y 2021.
https://www.cisa.gov/uscert/ncas/alerts/aa21-042a
https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

Servicios de higiene informática de la CISA del DHS: Consulte este recurso para obtener más información sobre el servicio gratuito de análisis de vulnerabilidades del DHS.
https://www.cisa.gov/cyber-hygiene-services

Shodan: Consulte este recurso para buscar activos conectados a Internet en la red del WWS.
https://www.shodan.io/

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 1 de la página 1 de este recurso para obtener información adicional.
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems