Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.T: ¿Recopila el WWS registros de seguridad (p. ej., acceso al sistema y las redes, detección de programas maliciosos) para usar en la detección e investigación de incidentes?

Recomendación: Recopile y almacene registros o datos de tráfico de red para ayudar a detectar ataques informáticos e investigar actividad sospechosa.

¿Por qué es importante este control?

Hacer un registro es registrar datos sobre eventos que ocurren en sus sistemas de TO o TI. Cuando se debe responder a un ataque informático, tener registros detallados ayudará a su empresa de servicios públicos y a los investigadores a determinar cómo y cuándo un atacante pudo ingresar a los sistemas, a qué áreas accedió y si filtró datos sensibles. Las revisiones periódicas de estos registros también pueden permitir que su WWS detecte a un atacante antes de que pueda afectar los sistemas.

Consejos de implementación

Revise los registros periódicamente para comprobar que estén completos y garantizar que se pueda encontrar toda la información necesaria en caso de un ataque informático.

Si una fuente de registro (p. ej., el registro de eventos de Windows) no está activa, notifique al administrador del sistema o a la persona responsable de la seguridad del sistema.

Si los registros no están disponibles para ciertos activos de TO, recopile información sobre el tráfico de red y las comunicaciones hacia y desde estos activos.

Consulte la página siguiente para obtener orientación adicional sobre este control.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control AU-2 (página 66) para obtener más información sobre el registro de eventos (sección “Event Logging”). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Guía de plantillas de políticas del NIST: Consulte los puntos 4.1a/b de la sección “Initial Log Generation” (Generación de registro inicial) de la Política de registro de seguridad. SOP para recopilar y mantener registros.
https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Logging-Standard.docx

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 4 (Implementar un sistema de supervisión para la detección de amenazas y alertas) proporciona información sobre el Registro y la Auditoría. *https://www.waterisac.org/fundamentals*

Recopilador de eventos de Windows (Microsoft Learn): Consulte este recurso para obtener más información sobre cómo configurar el recopilador de eventos de Windows. *https://learn.microsoft.com/en-us/windows/win32/wec/windows-event-collector*

ORIENTACIÓN ADICIONAL

- Las fuentes de registro incluyen, entre otras, inicios de sesión de red y registros de servidores, activos de usuario final (p. ej., computadoras de escritorio y portátiles), equipos de red (p. ej., enrutadores y conmutadores), aplicaciones/programas, sistemas de detección de intrusiones/sistemas de protección contra intrusiones (IDS/IPS), cortafuegos, software antivirus, herramientas de prevención de pérdida de datos (DLP) y redes privadas virtuales (VPN).
- Si es posible, los WWS deben captar, revisar y almacenar de forma segura los registros de todas estas fuentes para futuras referencias en caso de un ataque informático. Como mínimo, los WWS deben habilitar el registro para servidores críticos, cortafuegos y herramientas de acceso remoto como las VPN. Una revisión de los manuales de configuración de cualquier cortafuegos o herramienta de acceso remoto debe proporcionar instrucciones sobre cómo configurar y habilitar el registro para estos activos específicos.
- Para los sistemas basados en Windows, la aplicación Event Viewer (Visor de eventos) de Windows le brinda al WWS la capacidad de revisar manualmente los registros de seguridad de un activo individual. Para ver un ejemplo de registro de seguridad en Windows, abra la aplicación Event Viewer. En el árbol de la consola, expanda “Windows Logs” (Registros de Windows) y luego haga clic en “Security” (Seguridad). El panel de resultados muestra una lista de eventos de seguridad individuales. Para ver más detalles sobre un evento específico, haga clic en el evento en el plano de resultados. El WWS puede recopilar eventos de Windows tanto de servidores como de puntos finales (p. ej., computadoras de escritorio y portátiles) en un servidor central para realizar un análisis manual más eficiente mediante el recopilador de eventos de Windows. Si bien este método es una mejora con respecto a la revisión de registros completamente manual, no incluirá registros de activos y aplicaciones que no sean de Windows, lo que proporciona una imagen incompleta de las operaciones del WWS.
- Para superar este problema, el WWS puede usar software de agregación de registros y sistemas de gestión de información y eventos de seguridad (SIEM) para recopilar registros de forma centralizada prácticamente de todas las fuentes, simplificar la revisión de registros e identificar eventos de interés. Además de tener todos los registros en un solo lugar, estas herramientas también pueden automatizar muchos pasos del análisis de registros, lo que hace que el equipo de seguridad del WWS sea más eficaz y ahorre tiempo en el proceso.