Costo: $$$	Impacto: ALTO	Complejidad: BAJA

2.U: ¿Protege el WWS los registros de seguridad del acceso no autorizado y la alteración?

Recomendación: Almacene los registros de seguridad en un sistema central o base de datos al que solo puedan acceder usuarios autorizados y autenticados.

¿Por qué es importante este control?

Proteger los registros de seguridad es importante porque, si un atacante compromete un sistema, puede modificar o eliminar los registros para destruir las pruebas y ocultar sus huellas. Esta medida ayuda a garantizar que su WWS proteja sus registros de seguridad contra el acceso no autorizado y la alteración.

Detectar y responder a un ataque informático se vuelve mucho más difícil sin datos de registro confiables para rastrear lo que hace un atacante en un sistema informático.

Consejos de implementación

Almacene los registros durante un período que tenga en cuenta la política del WWS, las regulaciones estatales (si corresponde) y el riesgo informático. Un período de retención de registros habitual es de seis meses.

Asegúrese de que los registros de seguridad formen parte de los procedimientos de copia de seguridad estándar de su WWS para poder revisarlos incluso si la fuente ya no está disponible.

ORIENTACIÓN ADICIONAL

- El almacenamiento de registros en un sistema o base de datos central se puede lograr mediante sistemas de gestión de eventos e información de seguridad (SIEM), que se explican con más detalle en la hoja informativa 2.T. Además de facilitar la recopilación y el análisis de registros, las herramientas SIEM también permiten al administrador del sistema establecer permisos de acceso por usuario, lo que se conoce como control de acceso basado en roles (RBAC). Al almacenar registros en una ubicación central con o sin una herramienta SIEM, asegúrese de que cada usuario tenga una cuenta individual para acceder al almacenamiento de registros (es decir, herramienta SIEM, base de datos de registros o servidor de registros).
- Independientemente de cómo el WWS almacene los registros, debe realizar copias de seguridad en una ubicación de almacenamiento secundaria de forma periódica. Un cronograma de copia de seguridad habitual es diario. Los requisitos y las limitaciones regulatorias, operacionales y tecnológicas suelen determinar los períodos de retención de registros; sin embargo, un período de retención de registros habitual es de seis meses. Un período de retención de registros más largo suele ser mejor que uno más corto, ya que las personas encargadas de la respuesta tendrán más pruebas para revisar al investigar un posible ataque informático.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte la familia de controles AU y AU-9 (página 74) para obtener más información sobre auditoría y rendición de cuentas (sección "Audit and Accountability") y la protección de la información de auditoría (sección "Protegerion of Audit Information"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Guía de plantillas de políticas del NIST: Consulte el punto 4.5.b, "Log Access and Use" (Acceso y uso de registros) de la Política de registro (revisión 5) para ver controles de seguridad y privacidad para sistemas de información y organizaciones. SOP estándar documentado para proteger los registros de seguridad.
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