Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.K: ¿Usa el WWS cifrado eficaz para mantener la confidencialidad de los datos en tránsito?

Recomendación: Cuando envíe información y datos, use los estándares de cifrado de seguridad de la capa de transporte (TLS) o capa de puertos seguros (SSL).

¿Por qué es importante este control?

El cifrado es el proceso mediante el cual las computadoras convierten la información (p. ej., archivos, tráfico de red) de texto sin formato que las personas pueden leer a un mensaje codificado ilegible. Esta medida es importante, ya que los atacantes a menudo intentarán interceptar mensajes para alterar los comandos a los activos de TO y TI y robar contraseñas u otra información sensible.

Cuando utiliza cifrado para enviar información y los atacantes interceptan un mensaje, no podrán usar la información porque será ilegible. Esta medida ayuda a mantener la confidencialidad (es decir, el secreto) de la información sensible y la integridad (es decir, la exactitud) de la información de TO y TI.

Consejos de implementación

Para los sistemas informáticos de TO y TI, utilice cifrado para las comunicaciones con activos remotos o externos.

Actualice cualquier *software* de cifrado de datos débil u obsoleto.

ORIENTACIÓN ADICIONAL

- TLS y SSL son los protocolos de cifrado más comunes que utilizan los sistemas para enviar información y datos, y los WWS pueden configurar activos, como computadoras de escritorio y servidores, para enviar y recibir mensajes cifrados utilizando uno de estos protocolos. TLS es una alternativa más nueva y segura que SSL y, en general, es el estándar de cifrado preferido, si es factible. Un WWS debe realizar una revisión del protocolo de cifrado actual que utiliza, comparar este protocolo con los estándares actuales y desarrollar un plan de mejora si es necesario y factible a nivel operacional.
- Los ajustes de configuración para el cifrado pueden estar disponibles para una variedad de comunicaciones, incluyendo el software de acceso remoto, el software de HMI basado en la web, las comunicaciones inalámbricas (p. ej., wifi) y las comunicaciones por radio. Un WWS debe cifrar y proteger con contraseña las comunicaciones inalámbricas y evitar las redes de wifi abiertas (es decir, sin contraseña). Las redes privadas virtuales (VPN) para el acceso remoto a los sistemas del WWS y los servicios en la nube para el almacenamiento remoto y el alojamiento de aplicaciones probablemente ofrecerán esta capacidad de forma predeterminada.
- Dentro de Windows, el WWS puede habilitar la TLS a través del administrador de configuración. Si implementa TLS a través del administrador de configuración de Windows, asegúrese de comenzar con los clientes/puntos finales (computadoras de escritorio y portátiles). Si comienza la implementación a nivel de servidor, puede cortar la comunicación con los activos del cliente.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SC-8 (página 304) para obtener más información sobre la confidencialidad e integridad de la transmisión (sección "Transmission Confidentiality and Integrity").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de políticas del NIST: Consulte la sección 4.1," Data in Transit" (Datos en tránsito) del Estándar de cifrado. Procedimiento operativo estándar (SOP) documentado para el cifrado que se puede incluir en la política de ciberseguridad de la empresa de servicios públicos.
https://www.cisecurity.org/wp-content/uploads/2020/06/Encryption-Standard.docx

Guía de la infraestructura principal de Microsoft: Consulte los enlaces a continuación para obtener instrucciones sobre cómo habilitar TLS 1.2 en clientes (p. ej., computadoras de escritorio y portátiles) y servidores a través del administrador de configuración de Windows.
https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client
https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2