Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.L: ¿Usa el WWS cifrado para mantener la confidencialidad de los datos sensibles almacenados?

Recomendación: No almacene datos sensibles, incluyendo credenciales (es decir, nombres de usuario y contraseñas) en texto sin formato.

¿Por qué es importante este control?

Consulte la hoja informativa 2.K para obtener una descripción de la importancia del cifrado general.

Este control es importante, ya que los atacantes a menudo intentarán entrar en los sistemas informáticos y las bases de datos para robar información sensible y "preparar" la red para un futuro ataque. Además, muchos ataques informáticos de *ransomware* también incluyen intentos de extorsión mediante los cuales el atacante roba datos sensibles de un WWS y amenaza con exponerlos en Internet si no se paga un rescate. Si el WWS cifra los datos, el atacante no podrá usarlos si los roba, ya que serán ilegibles.

Consejos de implementación

Permita el acceso únicamente a usuarios autorizados.

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

ORIENTACIÓN ADICIONAL

- Un WWS puede implementar el cifrado de los datos almacenados mediante BitLocker para el cifrado de unidades de servidores y clientes (computadoras de escritorio y portátiles), así como con el cifrado de datos transparente (TDE) para los archivos de bases de datos. Un WWS puede cifrar y proteger con contraseña archivos sensibles individuales en Windows haciendo clic derecho en un archivo y seleccionando "Properties -> Advanced -> Encrypt contents to secure data" (Propiedades -> Avanzado -> Cifrar contenido para proteger los datos). Los servicios en la nube para el almacenamiento remoto y el alojamiento de aplicaciones probablemente ofrecerán esta capacidad de forma predeterminada.
- Para almacenar y utilizar credenciales de forma segura, un WWS puede utilizar un software de gestión de contraseñas (p. ej., LastPass, 1Password) u otro método de gestión de cuentas. El software de gestión de contraseñas almacena las credenciales de forma segura, reduce la dificultad de recordar contraseñas y simplifica el uso de contraseñas complejas.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SC-13 (página 308) y SC-28 (página 317) para obtener más información sobre la protección criptográfica (sección "Cryptographic Protegerion") y la protección de información en reposo (sección "Protegerion of Information at Rest").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de políticas del NIST: Consulte el SOP 4.2, "Data at Rest" (Datos inactivos) del Estándar de cifrado para obtener información sobre el cifrado que se puede incluir en la política de ciberseguridad de la empresa de servicios públicos. *https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2089.pdf*

Guía de la infraestructura principal de Microsoft: Consulte los enlaces a continuación para obtener instrucciones sobre cómo cifrar datos almacenados a través del cifrado de unidad BitLocker, el cifrado de datos transparente (TDE) para bases de datos y el cifrado de archivos individuales.
https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/transparent-data-encryption;

https://learn.microsoft.com/en-us/windows/security/information-Protegerion/bitlocker/bitlocker-overview;

https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7