Costo: $	Impacto: ALTO	Complejidad: BAJA

2.B: ¿Requiere el WWS una longitud mínima para las contraseñas?

Recomendación: Implemente un requisito de longitud mínima para las contraseñas. La implementación puede realizarse a través de una política o controles administrativos establecidos en el sistema.

¿Por qué es importante este control?

El uso de contraseñas cortas en un WWS es un riesgo de seguridad importante, ya que las contraseñas desempeñan un papel fundamental para evitar que los atacantes obtengan acceso a las cuentas de los usuarios. Los atacantes utilizan programas para adivinar las contraseñas de los usuarios, y una contraseña más larga y compleja es más difícil de descifrar para un atacante. Imponga la longitud y la complejidad de las contraseñas (p. ej., utilizar letras mayúsculas y minúsculas) y asegúrese de que los usuarios sigan las buenas prácticas de seguridad de las contraseñas (p. ej., que no coloquen notas adhesivas con recordatorios pegadas en los monitores).

Consejos de implementación

Cree una política o establezca controles administrativos que exijan una longitud mínima para las contraseñas (se recomiendan 15 caracteres o más) para todos los activos de TO y TI protegidos con contraseña, siempre que sea factible.

ORIENTACIÓN ADICIONAL

- En los casos en que no sea factible requerir una longitud mínima para las contraseñas, utilice controles de seguridad compensatorios (p. ej., utilizando un inicio de sesión único) y registre todos los intentos de inicio de sesión. Además, si los activos informáticos no admiten contraseñas más largas, priorice estos activos para actualizarlos o reemplazarlos.
- Utilice contraseñas o frases más largas como contraseña (p. ej., "Megustacomermanzanasyplátanos").

Para los activos de TO y TI basados en Windows, según la versión de Windows, el administrador del sistema puede usar la política de seguridad local para establecer una longitud mínima para las contraseñas. Para acceder a esta función, escriba "Local Security Policy" (Política de seguridad local) en el cuadro de búsqueda del menú Inicio y haga clic en la aplicación "Local Security Policy". Una vez que se abra el panel del menú, haga clic en "Account Policies" (Políticas de cuenta) y luego en "Password Policy" (Política de contraseñas) para ajustar la longitud de la contraseña.

Si un WWS utiliza un dominio de Microsoft con muchos sistemas y cuentas de usuario conectadas a un solo dominio, puede gestionar estos ajustes mediante objetos de directiva de grupo (GPO). El administrador del sistema puede configurar los ajustes de la política de contraseñas en la siguiente ubicación en la consola de gestión de directivas de grupo: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy (Configuración del equipo\Ajustes de Windows\Ajustes de seguridad\Políticas de cuenta\Política de contraseñas). La referencia de ajustes de la política de contraseñas de Microsoft Windows que se encuentra a continuación proporciona detalles adicionales.

En el caso de todas las demás contraseñas de activos que no sean de Windows, el administrador debe revisar las contraseñas existentes para garantizar que cumplan con la política de contraseñas siempre que sea posible. Estos activos pueden incluir *hardware* de red (p. ej., conmutadores de red, puntos de acceso inalámbricos, enrutadores de red); activos de comunicaciones (p. ej., radios); activos de TO (p. ej., PLC y HMI) y aplicaciones de *software* que utilizan contraseñas para autenticar a los usuarios.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Proporciona un enfoque proactivo y sistémico para desarrollar y poner a disposición un conjunto integral de medidas de protección para todo tipo de plataformas informáticas. Consulte el control AC-1 (página 39) para obtener más información sobre política y procedimientos de control de acceso (sección "Access Control Policy and Procedures").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de políticas del NIST: Consulte el punto 4.m de la sección "Authenticator Management" (Gestión de autenticadores) de la Política de identificación y autenticación. Un documento de política que aborda los requisitos de longitud mínima de las contraseñas.
https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx

Guía de contraseñas del NIST: El NIST creó un video breve que explica la protección de contraseñas y brinda orientación sobre la implementación de buenas prácticas.
https://www.nist.gov/video/password-guidance-nist-0

Guía de políticas de contraseñas de control del CIS: El Centro para la Seguridad de Internet (CIS) proporciona un desglose detallado de cómo crear e implementar una política de contraseñas, los detalles sobre la longitud de las contraseñas comienzan en la página 7.
https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide

CISA exige contraseñas efectivas: CISA ofrece consejos para crear contraseñas efectivas.
https://www.cisa.gov/secure-our-world/require-strong-passwords