Costo: $	Impacto: ALTO	Complejidad: BAJA

2.E: ¿Diferencia el WWS las cuentas de usuario y con privilegios (p. ej., administrador del sistema)?

Recomendación: Restrinja los privilegios del administrador del sistema a cuentas de usuario diferentes para acciones administrativas solamente y evalúe los privilegios administrativos de manera periódica para garantizar que las personas que tienen estos privilegios tengan la información precisa.

¿Por qué es importante este control?

El uso indebido de privilegios administrativos es uno de los métodos principales que utilizan los atacantes para entrar en una red. Si un usuario ha iniciado sesión como administrador o usuario con privilegios y abre un archivo adjunto de correo electrónico malicioso, descarga un archivo de un sitio web malicioso o navega por un sitio web que aloja contenido de un atacante, el atacante puede utilizar este acceso para lanzar un ataque. El ataque podría incluir la implementación de *ransomware* o la instalación de registradores de pulsaciones de teclas, analizadores de protocolos y *software* de control remoto para encontrar contraseñas y otros datos sensibles. Una segunda técnica común utilizada por los atacantes es un ataque de elevación de privilegios, adivinando una contraseña para un administrador del sistema. Si su empresa de servicios públicos distribuye de forma amplia y libre contraseñas administrativas o las establece idénticas a las contraseñas utilizadas en sistemas menos críticos, al atacante le resultará mucho más fácil obtener el control total de un sistema.

Consejos de implementación

Mantenga una lista/inventario actualizado de todas las cuentas de administrador.

Revise todas las cuentas de usuario de TO y TI para determinar cuáles están configuradas actualmente como “usuario estándar” o “administrador”. Para aquellas cuentas que están configuradas actualmente como administrador, revise si ese usuario requiere tener privilegios de administrador para sus tareas. Si no es así, cambie la cuenta del usuario a una cuenta de usuario estándar. Si requiere privilegios de administrador, pero actualmente no tiene una cuenta de usuario estándar para las funciones diarias, cree una cuenta de usuario estándar diferente para esa persona para el uso diario. Restrinja el uso de la cuenta de nivel de administrador

ORIENTACIÓN ADICIONAL

- Asegúrese de que todos los usuarios con acceso a cuentas administrativas utilicen una cuenta exclusiva o secundaria para sus actividades administrativas. Esta cuenta solo debe utilizarse para dichas actividades administrativas y no para navegar por Internet, enviar correos electrónicos o actividades cotidianas similares.
- Limite el acceso a herramientas de programación (como Microsoft PowerShell y Python) solo a los usuarios administrativos o de desarrollo que necesiten acceder a estas herramientas.
- Configure los sistemas para crear una entrada de registro y emitir una alerta cuando el WWS agregue o elimine una cuenta de cualquier grupo que tenga privilegios administrativos. Haga lo mismo para cualquier inicio de sesión fallido en una cuenta administrativa

a aquellas personas que necesiten acceso privilegiado y que solo se usen para funciones privilegiadas.

Si su WWS usa Windows, hay cinco formas de averiguar qué tipo de cuenta tiene un usuario (consulte el recurso vinculado a continuación). Conocer el tipo de cuenta de cada usuario le permite a su WWS determinar si es necesario cambiar el tipo de cuenta de un usuario para permitir o restringir privilegios adicionales para realizar tareas administrativas.

También puede cambiar el nivel de una cuenta en un sistema operativo común yendo a "Settings > Accounts > Family & Other Users" (Ajustes > Cuentas > Familia y otros usuarios), seleccionando la cuenta en cuestión, haciendo clic en "Change Account Type" (Cambiar tipo de cuenta) y seleccionando "Administrator" (Administrador) o "Standard User" (Usuario estándar).

Recursos

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 6 (Aplicar controles de acceso) proporciona información sobre la separación de cuentas. *https://www.waterisac.org/fundamentals*

Estándar 800-53 (revisión 5) del NIST, Política y procedimientos de control de acceso, AC-1: La página 18 proporciona información sobre el control de acceso y la gestión de acceso. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Estándar 800-82r3 del NIST, Guía para la seguridad de la tecnología operacional (TO): La sección 6.2.1 (págs. 97-108) proporciona información adicional sobre el control de acceso basado en roles para sistemas SCADA. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf*

Guía de plantillas de políticas del NIST: Consulte el punto 1.d de la sección "Account Management Authenticator Management" (Gestión de cuentas, gestión del autenticador) de la Política de control de acceso. Un documento de política que establece una política o procedimiento impuesto por el sistema que requiere que los usuarios no utilicen la misma contraseña para sus cuentas de usuario general y administrador. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

Windows Central: Indica cinco formas de identificar el tipo de cuenta de los usuarios dentro de una red en Windows. *https://www.windowscentral.com/how-determine-user-account-type-windows-10#determine_windows10_account_type_settings*