Costo: $	Impacto: ALTO	Complejidad: MEDIO

2.A: ¿Cambia el WWS las contraseñas predeterminadas?

Recomendación: Cuando sea factible, cambie todas las contraseñas predeterminadas del fabricante o distribuidor antes de que el equipo o el software se ponga en marcha.

¿Por qué es importante este control?

Los atacantes pueden obtener fácilmente las contraseñas predeterminadas del manual de usuario de un producto y usarlas para obtener acceso a los sistemas, ya sea de forma local o a través de Internet si el sistema de destino está conectado. El *hardware* y el *software* comercial están diseñados para una instalación y uso fácil. Los ajustes predeterminados de fábrica incluyen contraseñas simples y documentadas públicamente, como "1111". Muchas veces, estas contraseñas predeterminadas son idénticas (compartidas) entre todos los sistemas de un distribuidor o dentro de las líneas de productos.

Consejos de implementación

Desarrolle una política o un proceso obligatorio para toda la organización que requiera cambiar las contraseñas predeterminadas de los distribuidores o fabricantes de cualquier *hardware* o *software* que se utilice en su WWS.

Para mejorar la seguridad y la integridad del sistema, es posible que los WWS deseen requerir que todos los distribuidores involucrados en la instalación y configuración de *hardware* y *software* eliminen todas las contraseñas predeterminadas y las reemplacen con credenciales seguras y únicas antes de que se entregue el sistema. Esta medida es esencial para garantizar que los sistemas estén protegidos contra el acceso no autorizado y para aliviar la necesidad de que el personal gestione ajustes técnicos que requieren conocimientos especializados.

ORIENTACIÓN ADICIONAL

- Los WWS deben revisar su inventario de activos existentes e identificar los activos que tienen contraseñas predeterminadas. 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 en las que el fabricante o distribuidor que instala la aplicación en el WWS establece contraseñas predeterminadas. Revise la documentación de estos activos, incluyendo los manuales de instrucciones y las guías de configuración (generalmente disponibles en el sitio web del distribuidor), para identificar los nombres de usuario o contraseñas predeterminados. El administrador del sistema debe intentar iniciar sesión con las credenciales predeterminadas y, si tiene éxito, determinar si el administrador puede cambiarlas sin afectar las operaciones del sistema. En los casos en que no sea factible cambiar las contraseñas predeterminadas, implemente y documente los controles de seguridad compensatorios adecuados y monitoree los registros del tráfico de red y los intentos de inicio de sesión en esos activos. Si bien cambiar las contraseñas predeterminadas en la TO existente de un WWS puede requerir el soporte de un distribuidor o integrador calificado y puede que no siempre sea factible, el WWS debe cambiar las credenciales predeterminadas para todo el hardware o software recientemente implementado.

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 IA-5 (página 138) para obtener más información sobre la gestión de autenticadores (sección "Authenticator Management").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de políticas del NIST: Consulte los puntos 1.b a 1.d y 1.f de la Política de identificación y autenticación. Esta política detalla cuántos intentos de inicio de sesión fallidos son necesarios para bloquear una cuenta.
https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx

Alerta de la CISA del DHS (TA13-175A): Esta alerta, emitida en 2016, describe por qué es importante cambiar la contraseña predeterminada y proporciona medidas de mitigación.
https://www.cisa.gov/uscert/ncas/alerts/TA13-175A#:~:text=Attackers%20can%20easily%20identify%20and,to%20critical%20and%20important%20systems.

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 3 de la página 2 de este recurso para obtener información adicional.
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems