Costo: $	Impacto: MEDIO	Complejidad: BAJA

2.D: ¿Deshabilita el WWS de inmediato el acceso a una cuenta o red cuando el acceso ya no es necesario por motivos de jubilación, cambio de función, desvinculación u otros factores?

Recomendación: Deshabilite de inmediato el acceso a cuentas o redes después de un cambio en la situación de una persona que hace que el acceso no sea necesario (es decir, jubilación, cambio de puesto, etc.).

¿Por qué es importante este control?

Las cuentas inactivas pueden parecer inofensivas, pero plantean graves riesgos de seguridad cuando un WWS no las desactiva o cuando las cuentas no tienen límites de caducidad de contraseñas. Los atacantes pueden utilizar estas cuentas ya que es posible que el WWS no note sus actividades. Además, los empleados que dejan el WWS podrían seguir utilizando sus credenciales de inicio de sesión para acceder a los recursos de la red.

Consejos de implementación

Puede resultar útil elaborar una lista de verificación para utilizar cuando una persona deja su WWS o pasa a desempeñar una nueva función en el WWS. La lista de verificación podría incluir elementos como la devolución de cualquier equipo informático proporcionado por el WWS, como computadoras portátiles, tabletas y teléfonos inteligentes, así como la eliminación de las cuentas de usuario de la persona o el cambio de privilegios en las cuentas de usuario según sea necesario.

ORIENTACIÓN ADICIONAL

- Deshabilite el acceso a cuentas y redes siempre que un cambio en el estado de un usuario haga innecesario el acceso a la cuenta y la red.
- Revoque el acceso a empleados, distribuidores, contratistas y consultores despedidos o separados voluntariamente lo antes posible.
- Evalúe la necesidad de acceso del personal después de un ascenso u otro cambio de función dentro del WWS y elimine cualquier privilegio de acceso que ya no sea necesario para su nueva función.
- Establezca un procedimiento de desvinculación con recursos humanos, gerentes de contratos y personal de TO y TI. El procedimiento debe incluir un proceso de auditoría para identificar las cuentas que el WWS debe deshabilitar y eliminar.
- Deshabilite el acceso físico e informático de una persona a las instalaciones y sistemas del WWS tan pronto como la persona ya no requiera acceso.

Recursos

Guía de plantillas de políticas del NIST: Consulte el punto 1.h de la sección "Account Management" (Gestión de cuentas) de la Política de control de acceso. Un documento de políticas que establece un proceso administrativo definido y obligatorio para todos los empleados que dejan la empresa y que, antes de su partida, (1) revoca y devuelve de forma segura todas las credenciales físicas, tarjetas de acceso, equipos, etc. y (2) deshabilita todas las cuentas de usuario y el acceso a los recursos de la empresa de servicios públicos. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

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 revocación de credenciales. *https://www.waterisac.org/fundamentals*