Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.H: ¿Requiere el WWS el uso de la MFA siempre que sea posible, pero, como mínimo, para el acceso remoto a las redes de TO y TI del WWS?

Recomendación: Implemente la MFA de la manera más generalizada posible para las redes de TO y TI. Como mínimo, se debe usar la MFA para el acceso remoto a la red de TO.

¿Por qué es importante este control?

La MFA puede impedir que un atacante que obtenga una contraseña de usuario acceda a redes críticas del WWS. La MFA, también llamada autenticación de dos factores requiere que el personal del WWS y otros usuarios presenten al menos dos tipos de credenciales diferentes para iniciar sesión en un sistema del WWS. Las credenciales pueden estar basadas en conocimientos (como una contraseña o un PIN), basadas en activos (como una tarjeta inteligente o un teléfono móvil) o biométricas (como las huellas dactilares). Las credenciales deben proceder de dos categorías diferentes, por lo que introducir dos contraseñas diferentes no se consideraría MFA.

Se debe requerir el uso de la MFA a todos los usuarios o distribuidores remotos para reducir el riesgo. Muchas aplicaciones de acceso remoto y sistemas de redes privadas virtuales (VPN) ofrecen esta capacidad o se pueden configurar para ofrecerla mediante una herramienta de terceros.

Consejos de implementación

En las redes de TO, habilite la MFA en todas las cuentas y sistemas a los que el WWS puede acceder de forma remota, incluyendo las cuentas de distribuidores/ mantenimiento, las estaciones de trabajo de usuarios e ingeniería y las aplicaciones de HMI.

ORIENTACIÓN ADICIONAL

- Revise cualquier uso de acceso remoto, en particular a sistemas de TO, e identifique si el WWS puede habilitar la MFA en el software utilizado para este acceso. Existen varias aplicaciones que pueden ayudar a habilitar la autenticación multifactor en un WWS. Algunas de las más populares incluyen TeamViewer y Microsoft 365 para Windows. La sección de recursos a continuación proporciona enlaces para la configuración.
- Si el WWS no puede usar la MFA (p. ej., en algunas cuentas de administrador del sistema, de raíz o de servicio), esas cuentas deben usar contraseñas que sean exclusivas de ese sistema y no deben ser accesibles de forma remota siempre que sea posible.

Utilice la MFA para verificar la identidad de un usuario siempre que sea posible. Los métodos de MFA comunes incluyen datos biométricos, tarjetas inteligentes, activos de *hardware* habilitados con FIDO/CTAP (protocolo de cliente a autenticador) o códigos de acceso de un solo uso enviados o generados por activos previamente registrados, como un teléfono móvil.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte "Identification and Authentication" (Identificación y autenticación) en la página 132 para obtener más información sobre la MFA. *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 sección "Identification and Authentication" (Identificación y autenticación) de la Política de identificación y autenticación. Una política o procedimiento para toda la organización que requiere el uso de la MFA en una empresa de servicios públicos para acceder de forma remota a la red de TO. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

Referencia de autenticación multifactor de Microsoft 365: Esta página describe cómo configurar los ajustes de autenticación multifactor en las cuentas de Microsoft 365. *https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide*

Referencia de autenticación de TeamViewer: Esta página describe cómo configurar los ajustes de autenticación multifactor en la plataforma TeamViewer. *https://www.teamviewer.com/en-us/global/support/knowledge-base/teamviewer-classic/security/multi-factor-authentication/activate-two-factor-authentication/*