Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.Q: ¿Requiere el WWS la aprobación antes de instalar o implementar nuevo *software*?

Recomendación: Solo permita que los administradores instalen *software* nuevo en un activo del WWS.

¿Por qué es importante este control?

Permitir solo *software* aprobado en sus activos del WWS, preferiblemente instalado por un administrador, permite que su empresa de servicios públicos se asegure de que el *software* esté libre de código malicioso antes de la instalación. Los usuarios pueden utilizar *software* para realizar actividades comerciales normales o con fines maliciosos destinados a dañar el sistema informático o la empresa. Un atacante puede disfrazar *software* malicioso como *software* normal para engañar a un usuario para que lo instale, p. ej., publicitando funciones legítimas sin revelar las funciones maliciosas o imitando el estilo o la dirección web del portal de descarga de un distribuidor de confianza.

ORIENTACIÓN ADICIONAL

- Un WWS puede gestionar el software que se pone a disposición del personal a través de un portal de descarga en cada activo (p. ej., el centro de software de Windows) o, de manera más sencilla, mediante una lista de software aprobado. Para instalar un software nuevo, un empleado del WWS debe enviar una solicitud al personal de TO/TI o al administrador del sistema justificando la necesidad operacional del nuevo software.

Si un empleado del WWS instala intencional o involuntariamente *software* malicioso, el WWS podría ser vulnerable a filtraciones, interrupciones o daños en el sistema.

Consejos de implementación

Establezca controles para las computadoras y otros activos proporcionados por el WWS para restringir el *software* que los usuarios pueden instalar.

Algunos ejemplos incluyen restringir los privilegios administrativos (es decir, solo ciertas personas designadas pueden instalar *software* en las computadoras de un WWS, como un administrador del sistema) o permitir solo descargas de *software* aprobado.

Implemente un proceso que requiera aprobación antes de que los usuarios puedan instalar *software* nuevo o versiones de *software* nuevas.

Mantenga una lista en función de los riesgos del *software* permitido del WWS, incluyendo la especificación de las versiones aprobadas cuando sea técnicamente factible.

Recursos

Publicación 22-104746 de la GAO, Respuesta federal a los incidentes de SolarWinds y Microsoft Exchange: Consulte la sección "What GAO Found" (Lo que encontró la GAO) para obtener más información sobre el ataque a la cadena de suministro de SolarWinds en 2020. *https://www.gao.gov/products/gao-22-104746*

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control CM-11 (página 112) para obtener más información sobre el *software* instalado por el usuario (sección "User-Installed Software"). *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Guía de usuario del centro de *software* (Microsoft Learn): Consulte este recurso para obtener más información sobre cómo planificar y configurar el centro de *software* de Microsoft.
https://learn.microsoft.com/en-us/mem/configmgr/apps/plan-design/plan-for-software-center?source=recommendations