

Costo: \$

Impacto: ALTO

Complejidad: BAJA

1.I: ¿Incluye el WWS la ciberseguridad como criterio de evaluación para la adquisición de activos y servicios de TO y TI?

Recomendación: Incluya la ciberseguridad como criterio de evaluación cuando adquiera activos y servicios. Cuando sea factible, busque sistemas que sean seguros por diseño y de forma predeterminada.

¿Por qué es importante este control?

La implementación de este control ayudará al WWS a comprar productos y servicios más seguros, lo que reducirá el riesgo informático. Otorgarle a un distribuidor acceso a su red para realizar un servicio (p. ej., mantenimiento, cambios de configuración) o instalar nuevo *hardware* o *software* puede agregar una nueva vía para que los atacantes se infiltren en la red. Si un distribuidor accede de forma remota a la red de su empresa de servicios públicos sin proteger de manera efectiva sus propios sistemas informáticos, cualquier programa malicioso o infección en los sistemas del distribuidor puede migrar a los sistemas del WWS.

ORIENTACIÓN ADICIONAL

- Entre dos ofertas con un costo y una función similares, el WWS debería dar preferencia a la oferta o al abastecedor más seguro.
- El WWS también puede implementar cortafuegos para filtrar el tráfico inusual, así como para monitorear y registrar la actividad de la red.

El *hardware* o *software* instalado puede tener debilidades no intencionales (es decir, vulnerabilidades) que un atacante puede usar para ingresar a un sistema. Además, un atacante (con o sin el conocimiento del distribuidor) puede insertar intencionalmente vulnerabilidades en el *hardware* o *software* para introducir una debilidad en la red del WWS. El ataque a SolarWinds de 2020 es un ejemplo de un ataque de este tipo que afectó a varias agencias del Gobierno Federal.

La preocupación de que gobiernos extranjeros podrían colocar intencionalmente debilidades en productos de *hardware* exportados desde su país ha llevado a la Comisión Federal de Comunicaciones (FCC) a vetar a ciertos distribuidores de las redes del Gobierno Federal de Estados Unidos, así como de la importación y venta en Estados Unidos.

Consejos de implementación

Incluya los requisitos de ciberseguridad en el proceso de adquisición en la etapa más temprana para que los distribuidores que respondan a la solicitud de licitación sepan que deben incluir estos requisitos desde el principio. Su WWS debe requerir a los distribuidores que utilicen técnicas seguras, como una red privada virtual (VPN) y autenticación multifactor (MFA), cuando accedan a su red de forma remota. El recurso del Departamento de Energía a continuación proporciona un ejemplo de texto para documentos de adquisición sobre los requisitos de ciberseguridad de los distribuidores que los WWS pueden insertar en los contratos de los distribuidores.

Para evaluar a los distribuidores de *hardware* y *software* y reducir el riesgo informático que presentan para sus activos, pregúnteles sobre sus prácticas de ciberseguridad e invéstíguelos en línea para tener una idea de su ciberseguridad en general. Utilice los avisos del gobierno para investigar posibles distribuidores y buscar en bases de datos de vulnerabilidades (es decir, vulnerabilidades conocidas aprovechadas (KEV) y base de datos nacional de vulnerabilidades (NVD)) (consulte la hoja informativa 1.E).

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SR-6 (página 369) y SR-5 (página 368) para obtener más información sobre las evaluaciones y revisiones de abastecedores (sección “Supplier Assessments and Reviews”) y estrategias, herramientas y métodos de adquisición (sección “Acquisition Strategies, Tools, and Methods”).

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

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>

Vulnerabilidades conocidas aprovechadas (KEV) de la CISA del DHS: Consulte este recurso para conocer las vulnerabilidades que los atacantes ya han usado.

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Base de datos nacional de vulnerabilidades (NVD) del NIST: Consulte este recurso para obtener una lista de vulnerabilidades conocidas públicamente.

<https://nvd.nist.gov/vuln/search>

Vetos a distribuidores de *hardware* promulgados (FCC): Consulte estos recursos para obtener detalles sobre los vetos actuales a distribuidores de *hardware*.

<https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats>

<https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat>

Texto sobre ciberseguridad para documentos de adquisición del Departamento de Energía (DOE): Consulte este recurso para ver un ejemplo de texto sobre ciberseguridad que se debe incluir en los contratos con los distribuidores.

<https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014>

Alertas de la CISA del DHS: Consulte este recurso para registrarse para recibir alertas por correo electrónico del Sistema Nacional de Concientización Informática de la CISA del DHS sobre nuevas vulnerabilidades. <https://www.cisa.gov/uscrt/ncas/alerts>