Identificar: Informes de incidentes y divulgación de vulnerabilidades en la cadena de suministro

Costo: $	Impacto: ALTO	Complejidad: BAJA

1.G/1.H: ¿Requiere el WWS que todos los distribuidores y proveedores de servicios de TO notifiquen al WWS sobre incidentes o vulnerabilidades de seguridad en un plazo en función de los riesgos?

Recomendación: Requiera que los distribuidores y proveedores de servicios notifiquen al WWS sobre posibles incidentes y vulnerabilidades de seguridad dentro de un plazo estipulado que se describa en los documentos y contratos de adquisición.

¿Por qué es importante este control?

Receiving timely notification of vendor security incidents and vulnerabilities gives your WWS the opportunity to prevent or respond to potential attacks.

Consejos de implementación

ORIENTACIÓN ADICIONAL

- Cuando revise los requisitos de ciberseguridad dentro de los contratos, revise tanto los contratos de los proveedores de servicios como los acuerdos con los distribuidores de hardware/software (p. ej., integrador de TO, distribuidor de TI).

Su empresa de servicios públicos debe incluir un requisito de notificación contractual en los documentos de adquisición de productos de *hardware* y *software* y en los acuerdos de nivel de servicio (SLA) para los servicios. Puede elegir un plazo razonable y en función de los riesgos para que el distribuidor notifique a su WWS sobre las vulnerabilidades recién descubiertas en los productos del distribuidor y los ataques informáticos a los sistemas informáticos del distribuidor. Incluya cláusulas que requieran estos plazos de notificación en futuros contratos de adquisición y SLA con los distribuidores, así como las sanciones si el distribuidor no cumple con estos requisitos.

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.

Recursos

Estándar 800-53 (revisión 5) del NIST, Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SR-8 (página 371) para obtener más información sobre los acuerdos de notificación (sección “Notification Agreements”).
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Publicación 22-104746 de la Oficina de Responsabilidad Gubernamental (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

Texto sobre ciberseguridad para documentos de adquisición del Departamento de Energía (DOE): Consulte la sección 3.3, "Problem Reporting" (Informes de problemas) dentro de este recurso para ver un ejemplo de texto sobre ciberseguridad que se debe incluir en los contratos de los distribuidores.
https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014