PROTECCIÓN DE LA CADENA DE SUMINISTRO DE PEQUEÑAS Y MEDIANAS EMPRESAS

Un manual de recursos para reducir los riesgos relacionados con las tecnologías de la información y las comunicaciones

DESCRIPCIÓN GENERAL

DESCARGO DE RESPONSABILIDAD

Este informe se proporciona "tal cual" solo con fines informativos. El Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) no ofrece garantías de ningún tipo con respecto a la información aquí contenida. El DHS no respalda ningún producto ni servicio comercial al que se haga referencia en este informe o de otro modo. Este informe es TLP:CLEAR, no se limita su divulgación. De acuerdo con las normas de derechos de autor, la información TLP:CLEAR puede distribuirse sin restricciones. Para obtener más información sobre el protocolo de semáforo, consulte www.cisa.gov/tlp.

Los riesgos de la cadena de suministro de las tecnologías de la información y las comunicaciones (ICT, por sus siglas en inglés) están aumentando en todo el país. Son potencialmente más perjudiciales para las pequeñas y medianas empresas (SMB, por sus siglas en inglés), especialmente en comparación con entidades más grandes. Los datos de la Administración de Pequeñas Empresas de los EE. UU. (U.S. Small Business Administration) indican que las SMB que son proveedores de tecnologías de la información (IT, por sus siglas en inglés) y la comunicación representan a más de 160,000 empresas en los Estados Unidos; conectan millones de hogares y empresas a Internet todos los días; y adquieren, desarrollan e integran soluciones tecnológicas para ellos mismos y sus clientes[1]. Por lo tanto, la implementación de prácticas de seguridad en la cadena de suministro es fundamental para estas entidades de ICT.

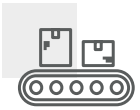
Para muchas personas, saber por dónde empezar y cómo una SMB puede conseguir los recursos financieros, de personal o de otro tipo, que son necesarios para implementar determinadas prácticas en la cadena de suministro de ICT puede parecer abrumador. Como resultado, el Grupo de Trabajo (WG, por sus siglas en inglés) del Equipo Operativo de Gestión de Riesgos de la Cadena de Suministro (SCRM, por sus siglas en inglés) de ICT se encargó de identificar los riesgos de la cadena de suministro de ICT que una SMB de IT y comunicaciones podría enfrentar, con especial atención a los riesgos cibernéticos y a la manera en que esos riesgos (en adelante, denominados "riesgos de la cadena de suministro de ICT") podrían ser diferentes a los de las empresas más grandes.

El Grupo de Trabajo utilizó una variedad de enfoques y técnicas para comprender mejor las categorías de riesgos más altas en la cadena de suministro de ICT que suelen enfrentar las SMB de IT y comunicaciones. Parte de ese proceso incluyó un grupo de discusión formado por SMB de comunicaciones, conversaciones con varios grupos de la industria, agencias gubernamentales y expertos en la materia.

[1] Fuente: Oficina de Defensa de Derechos (Office of Advocacy), Administración de Pequeñas Empresas de los EE. UU., a partir de datos proporcionados por la Oficina del Censo de los EE. UU. (U.S. Census Bureau), Estadísticas sobre empresas de los EE. UU. (Statistics of U.S. Businesses).

El WG también recibió comentarios de aproximadamente 100 SMB de IT, el 64 por ciento de las cuales tenían 100 empleados o menos.

Inicialmente, se identificaron más de una docena de categorías de riesgos en la cadena de suministro de ICT. Luego de un mayor análisis y refinamiento, las siguientes seis categorías surgieron como las categorías de riesgos de la cadena de suministro de ICT de mayor prioridad para las SMB de IT y comunicaciones.

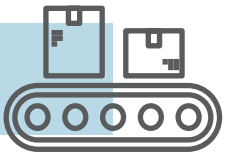


CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

1//EXPERIENCIA CIBERNÉTICA
2//COMPROMISO EJECUTIVO
3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT
4//PROVEEDOR ÚNICO
5//INTERRUPCIÓN DEL PROVEEDOR
6//VISIBILIDAD DEL PROVEEDOR

Al reconocer que muchas SMB de IT y comunicaciones no cuentan con expertos ni funciones de gestión de riesgos especializados a nivel interno, el Grupo de Trabajo preparó este manual de recursos. Este manual incluye seis casos de uso para ayudar a estas SMB a reconocer los desafíos de riesgos comunes relacionados con las ICT en la cadena de suministro, así como proporciona medidas prácticas y viables que pueden adoptar para mitigar estos riesgos. Los casos de uso se basan en empresas de ICT ficticias y presentan escenarios que estas SMB pueden enfrentar. También destacan una o más de las seis categorías de riesgos; proponen opciones potenciales que la empresa ficticia puede considerar; proporcionan un breve resumen de los costos y beneficios asociados con la implementación de las opciones propuestas y ofrecen una sección de recursos de mitigación del gobierno y la industria a los que se puede acceder para obtener más detalles.

Si bien el público objetivo del manual de recursos son las SMB de IT y comunicaciones, las categorías, los casos de uso y los recursos sugeridos son relevantes para las SMB de todas las industrias.



PRINCIPALES CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT DE SMB

1//EXPERIENCIA CIBERNÉTICA

Descripción: la disponibilidad de conocimientos, habilidades y experiencia necesarios para establecer, implementar y gestionar prácticas de SCRM de ICT. La colaboración es un factor clave para que una empresa invierta en experiencia cibernética de forma más eficaz.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: CISA Cyber Essentials

CISA: Evaluaciones de revisión de resiliencia cibernética

CISA: Herramienta de evaluación de seguridad cibernética (CSET®)

NIST: Ransomware Resources

NIST: NIST Cybersecurity Framework (CSF) Quick Start Guide

NIST: Rincón de ciberseguridad para pequeñas empresas (incluye una serie de estudios de casos de ciberseguridad)

2//COMPROMISO EJECUTIVO

Descripción: liderazgo empresarial, conocimiento y comprensión de la ciberseguridad como un riesgo empresarial y voluntad de fomentar una cultura de concientización sobre el riesgo cibernético en toda la organización, priorizar la gestión del riesgo cibernético y permitir prácticas seguras en la cadena de suministro necesarias para proteger a la empresa, sus activos, empleados y clientes.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: CISA, Elementos cibernéticos esenciales

CISA: Guía cibernética para pequeñas empresas

DNI: Mejores prácticas en la cadena de suministro

GCA: Capacitación sobre conceptos básicos de ciberseguridad para pequeñas empresas

NIST: Baldrige, creador de excelencia en ciberseguridad

NIST: NIST Small Business Cybersecurity Corner

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

Descripción: procesos y prácticas que garantizan la integridad de su cadena de suministro destinados a mejorar las prácticas de ciberseguridad de una empresa mediante la identificación, evaluación y mitigación de los riesgos asociados con los productos y servicios de tecnología de la información. Esto puede incluir involucrar a las partes interesadas relevantes, invertir en los recursos adecuados para proteger los datos de la empresa e integrar prácticas de ciberseguridad en la toma de decisiones, el presupuesto y los procesos operativos de la empresa.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: ICT Supply Chain Risk Management Fact Sheet

CISA: Guía de adquisición de Internet de las cosas (IoT)

CISA: Puesta en práctica de la plantilla de gestión de riesgos de la cadena de suministro de proveedores para pequeñas y medianas empresas

CISA: Best Practices in Cyber Supply Chain Risk Management

CISA: CISA, Elementos cibernéticos esenciales

CISA: Evaluaciones de revisión de resiliencia cibernética

CISA: Herramienta de evaluación de seguridad cibernética (CSET®)

FEDVTE: Gestión de riesgos cibernéticos en la cadena de suministro para el público

NCSC: Marco para la evaluación de riesgos

NCSC: Mejores prácticas en la cadena de suministro

NIST: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

NIST: NISTIR 83ware Risk Management: Un perfil del marco de ciberseguridad | Comisión de Responsabilidad Civil de Canadá (CSRC)

NIST: Curso introductorio sobre el marco de gestión de riesgos para sistemas y organizaciones

NIST: Small Business Cybersecurity Corner

NIST: Ransomware Resources

NIST: Guía de inicio rápido del NIST CSF

4//PROVEEDOR ÚNICO

Descripción: proveedores preferidos para un producto o servicio en particular o que son proveedores únicos de un producto o servicio determinado.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses

5//INTERRUPCIÓN DEL PROVEEDOR

Descripción: cualquier intento de degradar la cadena de suministro de un proveedor de ICT con la intención de interrumpir las operaciones en curso, dañar o vulnerar los datos contenidos en el sistema o la red.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: Fortalecimiento de las configuraciones de seguridad para defenderse de los atacantes que atacan los servicios en la nube

CISA: Cybersecurity Incident and Vulnerability Response Playbooks

ENISA: Panorama de amenazas a la cadena de suministro — ENISA (europa.eu)

6//VISIBILIDAD DEL PROVEEDOR

Descripción: la necesidad de visibilidad en las prácticas de ciberseguridad de terceros.

Recursos de mitigación recomendados para esta categoría de riesgo:

CISA: Puesta en práctica de la plantilla de gestión de riesgos de la cadena de suministro de proveedores para pequeñas y medianas empresas

CISA: Guía de adquisición de Internet de las cosas (IoT)

NASA: Proveedores certificados de NASA SEWP

NIST: Executive Order (EO) Guidance for Cybersecurity Supply Chain Risk Management

NIST: NIST Secure Engineering

NIST: Seguridad del software en las cadenas de suministro: evaluaciones de riesgo mejoradas de los proveedores

NTIA: Funciones y beneficios de SBOM en toda la cadena de suministro

NTIA: Recursos de la lista de materiales de software

CASOS DE USO

	número de página	5	6	7	8	10	12
	CASOS DE USO / CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT	**Rural Utility Services (RUS):** proveedor de servicios de banda ancha	**Micro Coding Wizards (MCW):** empresa de software	**Cloud Information Systems (CIS):** empresa de IT	**GreyCo:** integrador de defensa de los EE. UU.	**SubZeroQ:** computación cuántica	**AIO Company:** proveedor de ICT
1	EXPERIENCIA CIBERNÉTICA						●
2	COMPROMISO EJECUTIVO			●	●		●
3	GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT	●	●	●	●		●
4	PROVEEDOR ÚNICO					●	●
5	INTERRUPCIÓN DEL PROVEEDOR			●			●
6	VISIBILIDAD DEL PROVEEDOR	●	●		●		●

ESCENARIO DE CASO DE USO: **RURAL UTILITY SERVICES (RUS)**

RUS es un pequeño proveedor de servicios de banda ancha con una red de banda ancha que da servicio a 5,000 clientes. La administración de RUS identificó la necesidad de implementar un sistema de gestión de interrupciones (OMS, por sus siglas en inglés) que se utiliza para rastrear las interrupciones de los clientes, así como otros tipos de interrupciones (es decir, líneas y equipos de fibra de banda ancha). RUS emitió una solicitud de propuesta (RFP, por sus siglas en inglés) para este nuevo OMS, y se otorgó un premio a una pequeña empresa de desarrollo de software de IT, Micro Software Wizards (MSW), para desarrollar, respaldar y mantener el software OMS durante un período de 5 años.

Se firmó un contrato entre RUS y MSW, que incluía las disposiciones contractuales de SCRM de ICT siguientes:

- MSW debe proporcionar a RUS certificaciones de la cadena de suministro de software que muestren el ciclo de vida del desarrollo de software (SDLC, por sus siglas en inglés) y las prácticas de ciberseguridad, junto con certificaciones que reconozcan el cumplimiento de MSW de las políticas y prácticas de ciberseguridad y SDLC, de acuerdo con las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés).
- MSW debe notificar a RUS sobre cualquier vulnerabilidad recién descubierta que afecte al software OMS dentro de las 24 horas posteriores al primer descubrimiento.
- RUS debe proporcionar a MSW acceso a una red privada virtual segura, remota y con autenticación multifactor para realizar actividades de asistencia al cliente.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

RUS no cuenta con un programa interno de SCRM de ICT ni personal dedicado a la gestión de riesgos y carece de una estructura o marco para identificar, evaluar y mitigar eficazmente los riesgos que pueda presentar el software OMS de MSW.

6//VISIBILIDAD DEL PROVEEDOR

RUS carece de acceso a los procesos o prácticas de MSW para comprender completamente la postura en materia de ciberseguridad de MSW.

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

Las tarifas por hora de un consultor independiente pueden variar entre $75/h y $250/h

BENEFICIOS POTENCIALES

Acceso a experiencia en SCRM de ICT según sea necesario, en comparación con los costos de una contratación interna a tiempo completo.

La visibilidad y una mejor comprensión de las prácticas de SDLC y ciberseguridad de MSW brindan mayor confianza.

OPCIONES POTENCIALES PARA RUS

Considerar la contratación de un consultor externo de SCRM de ICT para utilizar un marco de gestión de riesgos comprobado con el fin de ayudar a RUS a identificar, evaluar y mitigar los riesgos reales o potenciales del software OMS de MSW.

Modificar el contrato de MSW para exigir que completen la Plantilla SCRM de proveedores para SMB.

RECURSOS

CISA: Puesta en práctica de la plantilla de gestión de riesgos de la cadena de suministro de proveedores para pequeñas y medianas empresas
CISA: Best Practices in Cyber Supply Chain Risk Management
CISA: Guía de adquisición de Internet de las cosas (IoT)
FEDVTE: Gestión de riesgos cibernéticos en la cadena de suministro para el público
NIST: Curso introductorio sobre el marco de gestión de riesgos para sistemas y organizaciones

ESCENARIO DE CASO DE USO: **MICRO CODING WIZARDS (MCW)**

MCW es una pequeña empresa de desarrollo de software que ofrece soluciones de software a fin de ayudar a gestionar una flota de vehículos eléctricos para corporaciones. La solución de software de MCW, MCWManager, es una plataforma de gestión de activos diseñada específicamente para gestionar flotas de vehículos eléctricos. MCWManager rastrea el uso, el nivel de carga, la autonomía y otras características importantes de cada vehículo eléctrico de la flota. El Departamento del Interior de EE. UU. (DOI, por sus siglas en inglés) expresó su interés en adquirir licencias del software MCWManager para gestionar una flota de 20 vehículos eléctricos, distribuidos en la región occidental, que incluye estados al oeste de Rocky Mountains. El DOI le ha informado a MCW que su software deberá proporcionar una lista de materiales de software (SBOM, por sus siglas en inglés), así como un informe de divulgación de vulnerabilidades, al DOI antes de la adquisición. El proceso actual del ciclo de vida de desarrollo del software de MCW carece de una capacidad de SCRM de ICT, lo que dificulta la producción de una SBOM y un informe de divulgación de vulnerabilidades por parte de MCW.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

MCW carece de un proceso de SCRM de ICT y actualmente no está produciendo una SBOM ni documentos de informe de divulgación de vulnerabilidades en su proceso de desarrollo. Es necesario cambiar el proceso de desarrollo de MCW para producir estos documentos.

6//VISIBILIDAD DEL PROVEEDOR

El DOI está siguiendo las recomendaciones de la cadena de suministro del software del NIST para que los proveedores de software proporcionen certificaciones de procesos y procedimientos en el ciclo de vida de desarrollo del software de MCW. Esta información le dará al DOI una mayor visibilidad sobre los componentes de software de MCW y cualquier vulnerabilidad que pueda presentarse en la aplicación MCWManager, antes de comprar el producto.

OPCIONES POTENCIALES PARA MCW

Seguir las recomendaciones del NIST para generar una SBOM y un informe de divulgación de vulnerabilidades de MCWManager.

Integrar una SBOM y un informe de divulgación de vulnerabilidades en el proceso de creación de Operaciones de Desarrollo (DevOps), utilizando herramientas de SBOM y de informes de divulgación de vulnerabilidades de código abierto.

Proporcionar a los clientes acceso seguro a la SBOM de MCWManager y a los informes de divulgación de vulnerabilidades.

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

Tiempo y esfuerzo de los ingenieros de desarrollo para implementar herramientas gratuitas de código abierto para producir una SBOM y un informe de divulgación de vulnerabilidades durante el proceso de desarrollo.

BENEFICIOS POTENCIALES

Cumplimiento de los requisitos del DOI que posiciona a MCW para garantizar un posible contrato gubernamental para la aplicación MCWManager.

MCW obtiene visibilidad de su propia cadena de suministro de software de proveedores de componentes y software de código abierto.

Visibilidad y una mejor comprensión de las prácticas de SDLC y ciberseguridad de MSW que brindan mayor confianza.

RECURSOS

CISA: ICT Supply Chain Risk Management Fact Sheet
CISA: Gestión de riesgos en la cadena de suministro - YouTube
NIST: EO Guidance for Cyber security Supply Chain Risk Management
NIST: Guía de inicio rápido del NIST CSF
NTIA: Recursos de la lista de materiales de software

ESCENARIO DE CASO DE USO: **CLOUD INFORMATION SYSTEMS (CIS)**

CIS es una empresa de IT que opera un software como servicio de facturación a clientes, llamado CISCustomerManager (CCM), para operadores de banda ancha rurales. CIS proporciona servicios de facturación a clientes de 230 operadores de banda ancha en los Estados Unidos; cuenta con 420,000 clientes de banda ancha con una factura promedio de $60/mes por un ingreso total de facturación mensual de $25,200,000. CIS tiene ocho empleados con ingresos mensuales de $2,300,000. CCM opera en la nube utilizando una interfaz web para interactuar con los clientes de CCM en la comunidad de banda ancha. En marzo de 2019, el director de IT de CIS se acercó al director ejecutivo (CEO, por sus siglas en inglés) con una propuesta para implementar un plan de respuesta a incidentes que requería inversión en un plan de continuidad comercial (BCP, por sus siglas en inglés) para permitir que CIS se recuperara rápidamente de un incidente de ciberseguridad que lo había debilitado: un ataque de ransomware que podía cifrar los datos y las aplicaciones de CIS y perjudicaba esencialmente la capacidad de CIS para operar su aplicación CCM. La propuesta del BCP tenía un costo único estimado de $100,000 y $25,000 por año, y permitiría a CIS recuperar la totalidad de las operaciones de producción de la plataforma CCM en cuatro horas. Después de una consideración inicial, el CEO rechazó la propuesta, y CIS continuó operando sin un BCP establecido. En enero de 2022, CIS fue atacado mediante la vulnerabilidad Log4j, lo que provocó un ataque de ransomware que impidió a CIS facturar a los clientes durante cuatro meses y le costó a CIS $500,000 en gastos de recuperación. Esto afectó significativamente el flujo de caja y las operaciones de facturación de los 230 clientes de CIS.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

2//COMPROMISO EJECUTIVO
E
5//INTERRUPCIÓN DEL PROVEEDOR

El CEO de CIS rechazó una propuesta de $100,000 para implementar un BCP utilizando un sitio de respaldo activo que podría haber permitido a CIS recuperarse de un ataque de ransomware en cuatro horas. CIS no pudo facturar a los clientes durante cuatro meses, lo que dio lugar a un importante déficit de flujo de caja y obligó a solicitar préstamos costosos para mantener las operaciones en marcha. Los clientes de CIS tampoco pudieron facturar a sus propios clientes durante cuatro meses, por un total de más de $100,000,000 en las facturas de los clientes de banda ancha.

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

La plataforma en la nube CCM estuvo fuera de funcionamiento durante cuatro meses debido a una higiene cibernética deficiente que no logró reparar la vulnerabilidad de Log4j de manera oportuna.

OPCIONES POTENCIALES PARA CIS

Gastar el monto de $100,000 para implementar el BCP con el fin de reducir el tiempo de recuperación en el futuro.

Reparar inmediatamente la vulnerabilidad de Log4j para evitar un ataque exitoso que aproveche esta vulnerabilidad.

Realizar una "copia de seguridad activa" de la aplicación CCM en otra plataforma en la nube que permanezca en "modo de espera" hasta que se la ponga en servicio.

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

$100,000 para implementar un BCP utilizando un gemelo digital y $25,000 por año para mantener el servicio. Un ingeniero a tiempo completo para gestionar el entorno de gemelo digital.

BENEFICIOS POTENCIALES

Tiempo de recuperación de cuatro horas frente a estar fuera de servicio durante cuatro meses y no poder enviar facturas a los clientes.

CIS y sus 230 clientes de banda ancha no registran pérdidas de flujo de caja durante cuatro meses.

RECURSOS

CISA: CISA, Elementos cibernéticos esenciales
CISA: Guía cibernética para pequeñas empresas
CISA: Manuales de respuesta a vulnerabilidades e incidentes de ciberseguridad
ENISA: Panorama de amenazas a la cadena de suministro — ENISA (europa.eu)
NIST: Guía de inicio rápido del NIST CSF

ESCENARIO DE CASO DE USO: **GREYCO**

GreyCo es un integrador de defensa de los EE. UU. de tamaño mediano, que ofrece sistemas y soluciones personalizados. GreyCo ofrece una solución única y reforzada en campo para la interceptación, recopilación y decodificación de señales de radio. GreyCo tiene una amplia experiencia y propiedad intelectual en interceptación y decodificación de señales de radio. La mayor parte de su producto proviene de múltiples proveedores, entre ellos, un importante fabricante de sistemas, circuitos integrados (IC, por sus siglas en inglés) estándar en los que se graba y aloja su software, así como varios cientos de componentes electrónicos básicos. GreyCo ha sido subcontratado por un contratista principal para proporcionar un elemento importante de un nuevo contrato de plataforma móvil adjudicado por el Ejército de los EE. UU. El contratista principal exigió a GreyCo que aporte pruebas de que se abastece de fuentes confiables y de que sus prácticas de integración mitigan el riesgo de componentes falsificados y contaminados. Esta evidencia deberá proporcionarse como requisito previo para la adjudicación del subcontrato.

Además, GreyCo debe proporcionar evidencia de que utiliza prácticas de ingeniería seguras y modernas en el proceso de fabricación de sus soluciones.

GreyCo tiene antecedentes de cumplimiento de los estándares federales de ciberseguridad; sin embargo, GreyCo no tiene una experiencia significativa en seguridad de la cadena de suministro y en cómo esas mitigaciones de riesgos se diferencian de los controles cibernéticos puros. El director de tecnología (CTO, por sus siglas en inglés) de GreyCo realiza investigaciones sobre estándares apropiados y observa que muchas empresas de tamaño similar han obtenido con éxito la certificación para proporcionar mitigaciones de SCRM que brindan evidencia de cumplimiento de los requisitos de SCRM de muchas agencias federales. El CTO asiste a varios eventos de SCRM de la industria, donde habla con varios de los proveedores y descubre que la mayoría de las empresas han contratado consultores que les ayudan a ofrecer una evaluación previa de sus procesos de abastecimiento y fabricación. El equipo ejecutivo de GreyCo asiste a una revisión de la evaluación

realizada por un consultor y obtiene información sobre el ciclo de vida necesario, la ingeniería segura y las prácticas de adquisición necesarias para mitigar los riesgos de la cadena de suministro. Algunos ejecutivos de GreyCo se muestran reacios a invertir en el ciclo de vida, la ingeniería segura y las prácticas de adquisiciones, porque quieren evidencia empírica de que su inversión se traduciría en mayores oportunidades y capacidades del producto. GreyCo otorga a un grupo de trabajo la responsabilidad de definir el caso de negocios, actualizar las prácticas de GreyCo, documentar el ciclo de vida del producto, la gobernanza y los procesos de supervisión de la implementación para garantizar la mejora continua. El CTO de GreyCo también trabaja con el gerente principal de productos de GreyCo a fin de adoptar herramientas y prácticas necesarias para abordar las brechas identificadas en las prácticas de ingeniería segura y cadena de suministro de GreyCo. Para lograr estas actualizaciones, el equipo de GreyCo aprovecha las pautas federales sobre prácticas de ingeniería segura y estándares de análisis de riesgos cuantitativos. Varias semanas después, el equipo de GreyCo presenta el alcance de la evaluación de sus prácticas de SCRM para que un laboratorio acreditado las analice y certifique. Después de que el laboratorio realiza la evaluación y valida la evidencia proporcionada, se notifica a GreyCo que cumple con los criterios de conformidad. GreyCo proporciona la evaluación y los resultados al contratista principal, y se confirma la adjudicación de su subcontrato. GreyCo utiliza su ciclo de vida de desarrollo de productos documentado, ingeniería segura y adquisiciones de la cadena de suministro, y prácticas de gobernanza para mejorar continuamente su postura con respecto a los riesgos a medida que se comunican nuevas amenazas a la seguridad de la cadena de suministro.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

2//COMPROMISO EJECUTIVO

Los ejecutivos de GreyCo se mostraron escépticos de financiar mitigaciones de riesgos adicionales sin comprender mejor el retorno de su inversión. El CEO de GreyCo quería evidencia empírica de que una inversión no solo protegería su reputación sino que también generaría ingresos adicionales para cubrir costos añadidos.

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

MCW carece de un proceso de SCRM de ICT y actualmente no está produciendo una SBOM ni documentos de informe de divulgación de vulnerabilidades en su proceso de desarrollo. Es necesario cambiar el proceso de desarrollo de MCW para producir estos documentos.

6//VISIBILIDAD DEL PROVEEDOR

GreyCo quiere expandir su negocio y vender en sectores adicionales del espacio y la defensa. GreyCo reconoce que las políticas actuales requieren que los proveedores sigan los mejores estándares y normas de la industria dentro de sus prácticas de fabricación y cadena de suministro. El equipo de GreyCo financia una evaluación independiente y una certificación industrial que puede utilizarse para cumplir con sus obligaciones contractuales y su visibilidad como proveedor confiable.

OPCIONES POTENCIALES PARA GREYCO

Utilizar un estándar formal de gestión de riesgos cuantitativos para determinar mejor dónde aplicar los recursos en toda la cadena de suministro de fabricación y abastecimiento de GreyCo a fin de maximizar las oportunidades de ingresos futuras y minimizar los riesgos para su reputación y sus clientes.

Obtener una evaluación y certificación independiente de terceros para determinar las brechas de SCRM mientras se utiliza la guía de ingeniería segura federal y aprovechan los marcos de prácticas recomendadas de la industria.

Implementar prácticas mejoradas de abastecimiento de proveedores mientras se optimizan los procesos de gobernanza y supervisión de desarrollo y fabricación.

Comunicar la certificación de GreyCo a las entidades de contratación gubernamental. Utilizar los activos creados por la evaluación constante como evidencia de cumplimiento y futuras licitaciones.

RECURSOS

CISA: CISA Cyber Essentials
NASA: NASA SEWP Certified Vendors
NIST: NIST Secure Engineering
NIST: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

GreyCo decidió contratar a un consultor para que realice una evaluación y ayude a documentar las prácticas actuales e identificar dónde podrían requerirse cambios para mitigar el riesgo de SCRM. GreyCo descubrió que algunas brechas en el desarrollo justificaban el uso de nuevas herramientas de operaciones de desarrollo seguras (SecDevOps) y requerían un mejor proceso de gobernanza para gestionar y calificar a los proveedores. GreyCo evaluó el retorno de la inversión proporcionado por las mitigaciones sugeridas e implementó nuevas herramientas para gestionar el ciclo de vida de su producto. Esto incluyó un análisis automatizado adicional de vulnerabilidades del código que produjeron, incluido el software de código abierto utilizado en su producto.

BENEFICIOS POTENCIALES

Cumplir con los requisitos del gobierno federal para los proveedores, lo que generará mayores oportunidades al ser incluido como proveedor confiable.

La adopción de un marco de riesgo cuantitativo formal ayudó a GreyCo a explicar mejor cómo estaban aplicando los recursos de la empresa para mitigar el riesgo de SCRM frente a las prácticas recomendadas de la industria.

ESCENARIO DE CASO DE USO: **SUBZEROQ**

Varios laboratorios de investigación de los EE. UU. buscan ampliar la investigación sobre la aplicación de la computación cuántica. Un componente necesario para construir o mantener computadoras cuánticas es el cableado superconductor criogénico. Estos cables, a diferencia de sus contrapartes de cobre, están hechos de una mezcla exótica y patentada de elementos de tierras raras utilizando prácticas de fabricación patentadas. Los equipos de adquisiciones del Laboratorio de Investigación Naval (NRL, por sus siglas en inglés) están liderando el proceso de adquisiciones. NRL determina que, evidentemente, solo hay un proveedor que cumple con sus requisitos, SubZeroQ.

Un proveedor único presenta a NRL un desafío único en materia de seguridad de la cadena de suministro. Si bien SubZeroQ tiene una reputación excelente en la comunidad de computación cuántica, el equipo de adquisiciones de NRL es responsable de calificar las prácticas de SCRM de SubZeroQ antes de su colocación en la lista de proveedores preferidos. Gran parte del trabajo que realiza NRL se considera confidencial y requiere una visibilidad limitada de las adquisiciones. NRL está particularmente interesado en garantizar que SubZeroQ pueda proporcionar un suministro continuo de minerales de tierras raras, proteger la información de adquisiciones proporcionada por NRL y garantizar la entrega de un producto auténtico a sus clientes.

El Departamento de Adquisiciones de NRL se comunica con SubZeroQ para obtener una reunión informativa en persona sobre sus prácticas de SCRM. Con el fin de facilitar la conversación, los funcionarios de adquisiciones de NRL se reúnen para revisar la plantilla de SCRM de proveedores de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) y determinar qué preguntas pueden ayudar a iniciar y guiar el debate con SubZeroQ. NRL presenta una lista de preguntas que incluye las siguientes:

- ¿El suministro continuo de minerales de tierras raras depende de una única fuente?
- ¿Los materiales de distribución se suministrarán desde un país de especial interés?
- ¿Los clientes y las actividades de adquisición de NRL están protegidos y respaldados por la integridad de los sistemas de adquisición de SubZeroQ?
- ¿Existe un proceso utilizado por SubZeroQ para informar incidentes de seguridad de productos y de la cadena de suministro?
- ¿Cuál es el proceso para garantizar la integridad y autenticación del transporte y la entrega de los productos SubZeroQ al cliente previsto?

SubZeroQ se reúne con NRL para analizar la lista de preguntas y revisar sus prácticas con el fin de proteger a sus clientes en toda la cadena de suministro. SubZeroQ explica que dividieron su suministro de materias primas y materiales raros entre dos fuentes conocidas y están pagando precios más altos, en algunos casos, para evitar proveedores de alto riesgo. Proporcionan a NRL una visión de su marco de puntuación de proveedores y de cómo gestionan requisitos similares de sus subproveedores. SubZeroQ explica qué estándares siguen para guiar sus prácticas de SCRM. SubZeroQ también proporcionó una revisión integral de la manera en que protegen el transporte de productos desde su planta en Japón hasta su clientela global. Esto incluía embalajes a prueba de manipulaciones, así como una codificación de autenticación de los paquetes, que permite su seguimiento a través de códigos a medida que viajan a través de la cadena de distribución.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

Y

4//PROVEEDOR ÚNICO

SubZeroQ es el único proveedor de piezas para el cableado superconductor utilizado en las computadoras cuánticas. NRL busca proporcionar a sus laboratorios de investigación la capacidad de adquirir sus productos. NRL busca la confirmación de que SubZeroQ puede proteger adecuadamente sus datos de adquisiciones, garantizar el suministro a largo plazo y mitigar eficazmente los riesgos de SCRM al evitar que se inserten piezas falsificadas o de repuesto durante el transporte.

OPCIONES POTENCIALES PARA SUBZEROQ

SubZeroQ se encuentra en la posición única de ser proveedor exclusivo de un componente muy solicitado. Esto garantiza que SubZeroQ adopte un enfoque más práctico para interactuar con los clientes que buscan comprender cómo abordar la SCRM, proteger los datos de adquisiciones de sus clientes y garantizar la entrega del producto sin alteraciones a sus clientes.

Los sistemas de adquisiciones de SubZeroQ están alojados en un entorno basado en la nube y utilizan pautas de estándares internacionales para la implementación de controles cibernéticos. SubZeroQ reconoce la necesidad de proporcionar una comparación entre los estándares internacionales implementados y los estándares nacionales aplicables a los clientes fuera de su país de origen.

SubZeroQ desarrolló un paquete informativo integral y autorizó a los miembros del equipo del director de seguridad de la información (CISO, por sus siglas en inglés) a viajar hasta donde se encuentran los clientes para brindarles información directa y responder preguntas sobre sus prácticas.

Se redactó una versión depurada del plan de gestión de riesgos de la cadena de suministro de SubZeroQ para que los clientes puedan disponer de ella. Esto protege eficazmente la información confidencial de SubZeroQ y, al mismo tiempo, proporciona información adicional a los equipos de adquisiciones.

SubZeroQ implementó un Equipo de Respuesta a Incidentes de Seguridad de Productos (PSIRT, por sus siglas en inglés) bien documentado que responderá a cualquier posible incidente de transporte o cumplimiento de productos. A cada cliente se le proporciona contacto directo con el equipo PSIRT para responder a posibles incidentes.

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

SubZeroQ autorizó a su equipo de CISO a viajar hasta NRL para brindar una sesión informativa sobre SCRM a los proveedores. También invirtieron en la comparación entre los estándares internacionales que emplean y los estándares nacionales de los EE. UU. SubZeroQ también invirtió en un PSIRT responsable de gestionar y mitigar los riesgos durante la adquisición y el cumplimiento, así como de comunicar incidentes de seguridad importantes a los clientes.

BENEFICIOS POTENCIALES

Satisfacer los requisitos del gobierno federal para los contratos, brindar visibilidad en las prácticas de SCRM de fuente única para obtener una designación de proveedor preferido por parte de agencias y empresas de los EE. UU.

RECURSOS

CISA: Internet of Things (IoT) Acquisition Guidance
NCSC: Framework for Assessing Risks

Marcos de gestión de riesgos:
NIST: NIST Risk Management Framework

ESCENARIO DE CASO DE USO: **AIO COMPANY (AIO)**

AIO es una organización de tamaño mediano con 100 empleados ubicados en varios lugares alrededor del país. AIO está buscando formas de comunicarse eficazmente con sus clientes, ya que las líneas telefónicas tradicionales ya no son la principal vía de contacto. Después de investigar varios productos, AIO identifica un producto que ofrece voz, texto y chat en vivo con capacidades para compartir pantalla, lo que cubre todas las necesidades de servicio al cliente de la organización. Se solicita al CISO de la empresa que realice una evaluación de riesgos. La evaluación de riesgos revela que el proveedor del producto elegido es en realidad un integrador externo y no proporciona directamente ninguno de los servicios requeridos, sino que utiliza un tercero para cada una de las ofertas de servicios.

AIO no cuenta con un proceso formal de gestión de riesgos interno y carece de suficiente experiencia cibernética para identificar los riesgos asociados con el uso de la nueva plataforma. El integrador externo del producto identificado por AIO actúa como un proveedor único y ofrece visibilidad y acceso limitados que permitirían a AIO comprender mejor la postura del proveedor en materia de ciberseguridad. Esto aumenta el riesgo de una posible interrupción de las operaciones de AIO si AIO experimenta un incidente cibernético como resultado de

una vulnerabilidad en el producto del integrador externo. Aunque existen riesgos relacionados con las ICT que no se han identificado ni mitigado por completo, la dirección ejecutiva de AIO, en oposición a lo aconsejado por el CISO, decide seguir adelante con la solución propuesta por el integrador para acelerar la implementación del nuevo producto para sus clientes.

CATEGORÍAS DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

1//EXPERIENCIA CIBERNÉTICA

Si bien los miembros del equipo de IT y CISO de AIO tienen antecedentes técnicos en ingeniería de redes, administración y desarrollo de software, carecen de experiencia específica en ciberseguridad que les permita reconocer riesgos de terceros que podrían ser perjudiciales para AIO.

2//COMPROMISO EJECUTIVO

El compromiso de la dirección ejecutiva de AIO con la toma de decisiones basada en riesgos se reemplazó por la presión de tener un producto listo rápidamente, aun cuando no se conocen ni se comprenden completamente los riesgos potenciales de ICT que el producto puede presentar.

3//GESTIÓN DE RIESGOS DE LA CADENA DE SUMINISTRO DE ICT

Si bien AIO tiene un CISO, ninguno de los miembros del equipo de IT tiene antecedentes ni experiencia en gestión general de riesgos empresariales ni en gestión de riesgos de la cadena de suministro.

4//PROVEEDOR ÚNICO

El integrador externo que actúa como proveedor único presenta un mayor riesgo para AIO, ya que pasa a depender exclusivamente de un integrador que tiene la capacidad de limitar dónde y cuándo AIO tiene acceso a los productos y servicios del integrador.

5//INTERRUPCIÓN DEL PROVEEDOR

Todo proveedor inevitablemente experimenta una interrupción del servicio. Probablemente esto será cierto para los integradores externos. Una interrupción de este tipo no solo afectaría a AIO, sino también a sus clientes finales.

6//VISIBILIDAD DEL PROVEEDOR

La renuencia del integrador externo a brindar a AIO la visibilidad y el acceso adecuados para comprender los riesgos potenciales de la cadena de suministro de ICT es una señal de alerta y puede indicar su incapacidad para demostrar su postura en materia de ciberseguridad.

OPCIONES POTENCIALES PARA AIO

Contratar a un consultor externo con experiencia en gestión de riesgos y ciberseguridad en la gestión de riesgos de la cadena de suministro de ICT para realizar una evaluación de riesgos del integrador externo e identificar, priorizar y desarrollar estrategias de mitigación de riesgos de alta prioridad.

Continuar la búsqueda de un proveedor que ofrezca todos los servicios solicitados de forma nativa por una tarifa aceptable.

Realizar el trabajo de integración a nivel interno y contratar personal calificado para realizar una evaluación de riesgos.

Establecer un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) con el integrador que registre los requisitos de tiempo de actividad y estipule consecuencias financieras específicas cuando no se cumplan esos requisitos.

COSTOS Y BENEFICIOS

COSTOS POTENCIALES

Las tarifas por hora de un consultor independiente externo pueden variar entre $75/h y $250/h.

- Los costos de reclutamiento y contratación de personal interno con experiencia en ciberseguridad y gestión de riesgos probablemente serán de varios miles de dólares además de la compensación.
- La elaboración de un SLA puede llevar días o semanas y puede requerir la asistencia de un consultor independiente o un asesor legal con experiencia en la redacción de SLA.

BENEFICIOS POTENCIALES

La contratación de un consultor independiente proporciona a AIO acceso a experiencia en SCRM de ICT según sea necesario, en comparación con los costos de una contratación interna a tiempo completo.

- La identificación de un nuevo proveedor que aborde todos los requisitos relacionados con las ICT permite a AIO reducir el riesgo de exposición.
- Establecer un SLA con el integrador ayuda a que se responsabilice de su desempeño a través de consecuencias monetarias si su producto falla o causa daños o interrupciones a AIO.

RECURSOS

CISA: Cyber Security Evaluation Tool (CSET®)
CISA: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses
CISA: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
DNI: Supply Chain Best Practices
NIST: NIST Small Business Cybersecurity Corner
NIST: Software Security in Supply Chains: Enhanced Vendor Risk Assessments

El Centro Nacional de Gestión de Riesgos (NRMC, por sus siglas en inglés) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) es el centro de planificación, análisis y colaboración que trabaja en estrecha coordinación con la comunidad de infraestructura crítica para identificar, analizar, priorizar y gestionar los riesgos más estratégicos para las funciones críticas nacionales. Estas son funciones del gobierno y el sector privado tan vitales para los Estados Unidos que su interrupción, corrupción o mal funcionamiento tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de estos aspectos. Los productos NRMC están disponibles en https://www.cisa.gov/national-risk-management.

CONTACTO DEL DHS

Centro Nacional de Gestión de Riesgos
Agencia de Ciberseguridad y Seguridad de la Infraestructura
Departamento de Seguridad Nacional de los EE. UU.

NRMC@hq.dhs.gov

Para obtener más información sobre NRMC, visite www.cisa.gov/national-risk-management