SECTOR DE FABRICACIÓN CRÍTICA:
Seguridad de la Cadena de Suministro y el Mercado Gris

Esta hoja informativa informa a los lectores sobre el continuo aumento de los mercados grises y cómo sus componentes pueden afectar las cadenas de suministro nacionales. Este documento también presenta varios tipos de mercado (gris y negro) y por qué son problemáticos.

¿POR QUÉ ES IMPORTANTE LA SEGURIDAD DE LA CADENA DE SUMINISTRO PARA LA FABRICACIÓN CRÍTICA?

El sector de fabricación crítica depende en gran medida de cadenas de suministro complejas (tanto nacionales como internacionales) para entregar materias primas, piezas fabricadas y componentes finales. Las cadenas de suministro de los fabricantes son cada vez más extensas, complejas e interdependientes; a veces involucran a cientos de instalaciones, vendedores y proveedores en todas las regiones. El enfoque de una organización hacia la seguridad de la cadena de suministro es clave y debe adaptarse para satisfacer las características y necesidades únicas de su cadena de suministro.

MERCADOS BLANCO, GRIS Y NEGRO

Las organizaciones deben diferenciar entre los mercados blanco, gris y negro **para garantizar que sus productos importados provengan de distribuidores autorizados, aquellos conectados con la marca o el fabricante de componentes originales (OCM, por sus siglas en inglés).**

- **El mercado blanco** es el mercado legal, oficial o autorizado de bienes y servicios, utilizando canales, fabricantes y distribuidores autorizados.
- **El mercado gris** es un mercado controvertido que proporciona acceso a vendedores y compradores a través de canales no autorizados, que no están afiliados a la marca ni al OCM.
- **El mercado negro** evita las sanciones gubernamentales mediante el intercambio de bienes y transacciones a través de canales ilícitos.

¿QUÉ SUCEDE SI MATERIAL DEL MERCADO GRIS LLEGA A LA CADENA DE SUMINISTRO?

Los materiales del mercado gris y negro pueden entrar en la cadena de suministro a través de numerosos puntos, lo que dificulta el rastreo de su origen y proveedor original. Los productos y componentes del mercado gris a largo plazo afectan negativamente la reputación de la marca, los costos, la responsabilidad y los ingresos a lo largo de la cadena de suministro. A pesar de los esfuerzos de mitigación, los materiales del mercado gris pueden integrarse en la cadena de suministro de una organización. Las consideraciones de riesgo y las implementaciones de mejores prácticas pueden mitigar las intrusiones del mercado gris.

Consideraciones sobre los riesgos de la cadena de suministro

- Número y ubicación de proveedores.
- Origen de los envíos.
- Términos contractuales que definen los requisitos de seguridad para los envíos de proveedores o vendedores.
- Proveedores de logística de terceros o socios involucrados en la cadena de suministro (por ejemplo, empresas de embalaje, almacenamiento, empresas de transporte, transportistas y transportistas aéreos o marítimos) que manejan envíos.

Mejores prácticas para la revisión de la cadena de suministro

- **Establecer una política de la empresa para la gestión de riesgos de proveedores.** Una política de gestión de riesgos de proveedores debe comenzar con criterios de selección específicos, procedimientos de investigación y el número de opciones de proveedores para obtener cada tipo de producto o componente. Tener múltiples proveedores aprobados puede mitigar las interrupciones en la cadena de suministro.
- **Utilizar una matriz de control y gestión de riesgos de proveedores para evaluarlos.** Con una matriz de control y gestión de riesgos de proveedores se pueden calcular los riesgos estimados y la probabilidad de ocurrencia de incidentes para ayudar a determinar los pasos necesarios para mitigar el riesgo inaceptable de proveedores o vendedores.

- **Desarrollar e implementar un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) con proveedores o vendedores seleccionados.** Un SLA define el nivel de servicio esperado de un proveedor, vendedor o distribuidor estableciendo métricas de servicio, así como soluciones o sanciones en caso de que no se cumplan las métricas y los requisitos de servicio.
- **Realizar la debida diligencia continua del proveedor.** Revisar continuamente a los proveedores para detectar riesgos comerciales a lo largo de su ciclo de vida.

GESTIÓN DE RIESGOS DE PROVEEDORES

La gestión de riesgos de proveedores (también conocida como gestión de riesgos de vendedores), que suele aplicarse antes y después de comprar o subcontratar a terceros distribuidores y proveedores, ayuda a las organizaciones a evitar riesgos y proteger su reputación.

¿Por qué es importante la gestión de riesgos de proveedores?

La dependencia de proveedores de dudosa reputación afecta significativamente a las operaciones empresariales de una organización, a la seguridad de los datos y la información, los resultados financieros y la reputación de la organización. Es imprescindible asegurarse de que los vendedores y proveedores cumplan con los requisitos normativos.[1] Este tipo de gestión disminuye el riesgo de que se produzcan fallas en la seguridad de los datos y la ciberseguridad, infracciones normativas e interrupciones de la actividad empresarial por fallas de los proveedores o retrasos importantes en la entrega de la cadena de suministro.

Ejemplos de gestión de riesgos de proveedores

- Falta de contratos adecuados u órdenes de compra aprobadas antes de obtener productos de un proveedor o vendedor.
- Una violación de los datos de ciberseguridad se rastrea hasta el proveedor o vendedor externo.
- Vendedores o proveedores fraudulentos.
- Cierres o retrasos imprevistos de proveedores debido a una mala gestión fiscal que pueden afectar la continuidad del negocio.

El proceso de toma de decisiones en materia de adquisiciones

Adoptar un enfoque diligente en las prácticas de compra, inspección y prueba es fundamental para minimizar el impacto del mercado gris. La adquisición de artículos del fabricante de componentes originales (OCM, por sus siglas en inglés), que son organizaciones que diseñan o fabrican una pieza y tienen derechos de propiedad intelectual sobre el artículo, garantiza el menor riesgo de falsificación y, en consecuencia, la mayor confianza en la autenticidad. Es probable que los distribuidores autorizados/con franquicia y los fabricantes contratados también sean confiables y tengan un acuerdo contractual con el OCM para comprar, almacenar, reenvasar, vender y distribuir sus líneas de productos. Al abrir las fuentes de suministro, los distribuidores independientes e intermediarios no siempre están obligados contractualmente con el OCM, sino que compran piezas para venderlas y redistribuirlas en un mercado abierto. Las fuentes desconocidas ofrecen la menor confianza de autenticidad y existe un alto riesgo de falsificación.

CÓMO DENUNCIAR UNA VIOLACIÓN DE SEGURIDAD EN LA CADENA DE SUMINISTRO

Debido a su tamaño y la complejidad de sus relaciones, las violaciones de seguridad de la cadena de suministro pueden ser difíciles de rastrear. El Grupo Operativo para la Gestión de Riesgos en la Cadena de Suministro de Tecnologías de la Información y las Comunicaciones (ICT SCRM, por sus siglas en inglés) ha elaborado una serie de consejos para gestionar estos riesgos. Para obtener más información sobre cómo denunciar infracciones, consulte los Aspectos esenciales de ICT SCRM en la página de CISA de ICT SCRM.

EJEMPLO DE ESTUDIO DE CASO PERTINENTE

El Comité de las Fuerzas Armadas del Senado (SASC, por sus siglas en inglés) inició una investigación sobre piezas electrónicas falsificadas en la cadena de suministro del Departamento de Defensa entre 2009 y 2011, muchas de las cuales provenían de varios puntos de reventa en Estados Unidos, el Reino Unido y Canadá. Los investigadores señalaron a China como fuente de los productos electrónicos falsificados y descubrieron presuntas piezas falsificadas en computadoras de misión para misiles de la Agencia Antimisiles de Defensa (MDA, por sus siglas en inglés) y visores térmicos de armas. En esta investigación se identificaron 1,800 casos de falsificación. Posteriormente, se prohibió la entrada en China al personal del SASC. Todos los materiales, componentes y piezas electrónicas deben examinarse para garantizar que sean productos de distribuidores y proveedores autorizados o franquiciados dentro de la cadena de suministro. Este proceso de verificación y autenticación ofrece la máxima confianza en la autenticidad y el menor riesgo de adquirir materiales del mercado gris y falsificaciones.[2]

PARA OBTENER MÁS INFORMACIÓN SOBRE EL SECTOR DE FABRICACIÓN CRÍTICA

Póngase en contacto con el Equipo de Gestión del Sector de Fabricación Crítica en CriticalManufacturingSector@cisa.dhs.gov o visite el sitio cisa.gov/critical-manufacturing-sector para saber más.

[1] Los requisitos regulatorios de la cadena de suministro incluyen, de manera enunciativa mas no limitativa, la normativa sobre comercio internacional; las normas medioambientales, sociales y de gobierno (ESG, por sus siglas en inglés); la normativa sobre seguridad y calidad de los productos; la normativa sobre privacidad y seguridad de los datos; y la normativa contra la corrupción y el soborno.
[2] Abesamis, C. and Leblanc, M. (2015) NASA Counterfeit Parts Awareness and Inspection [diapositivas 23 y 24 de PowerPoint]. Obtenido de la copia en versión PDF de NASA Counterfeits Parts Awareness and Inspection.