Recursos bajo CTPAT/AEO

CIBERSEGURIDAD

AIAG

¿Qué tiene que ver la Ciberseguridad con el cumplimiento de CTPAT?

CTPAT se desarrolló para proteger las cadenas de suministro estadounidenses e internacionales de posibles actividades terroristas. Y, en nuestra sociedad cada vez más digital y dependiente de la tecnología, la definición de terrorismo ahora incluye varios tipos de delitos cibernéticos. Los piratas informáticos organizados pueden representar riesgos de seguridad sustanciales para los fabricantes, las empresas de transporte y logística y otras empresas involucradas en cualquier nivel de la comunidad comercial mundial.

Para cubrir todas las bases, CTPAT requiere que las organizaciones tomen varias medidas para mitigar el riesgo de una violación de seguridad cibernética. Afortunadamente, se dedica recursos a evitar el ciberdelito, es muy probable que ya haya satisfecho al menos algunos de los criterios.

Los 13 requisitos de ciberseguridad para el cumplimiento de CTPAT (y cómo cumplirlos)

De acuerdo con los criterios mínimos de seguridad de CTPAT, existen trece requisitos de seguridad cibernética que una organización debe cumplir para obtener la certificación o conservar su estado actual de CTPAT:

Políticas y procedimientos de seguridad cibernética por escrito

Primero, deberá crear una política de ciberseguridad por escrito basada en los estándares de la industria. El Instituto Nacional de Estándares y Tecnología (NIST) tiene un marco de ciberseguridad con orientación para ayudar a las organizaciones a crear sus propias políticas.

Suficiente protección de software y hardware

Debe tener suficiente infraestructura de IT para protegerse contra las amenazas de seguridad cibernética, incluido software (como tecnología antivirus) y soluciones de hardware (como servidores proxy). También deberá desarrollar procedimientos para recuperar o reemplazar rápidamente los sistemas de TI en caso de que experimente pérdida de datos o daños en el equipo.

Pruebas periódicas de la infraestructura de IT

Deberá probar regularmente la seguridad de su infraestructura de IT y tomar medidas correctivas si descubre alguna vulnerabilidad.

Políticas claras sobre la denuncia de amenazas

Asegúrese de que sus políticas comuniquen claramente cómo compartir información o denunciar amenazas con entidades gubernamentales y socios comerciales.

Identificar y actuar en caso de acceso no autorizado por IT

Debe implementar un sistema que identifique el acceso no autorizado a sus sistemas o datos de IT, así como el abuso de sus políticas y procedimientos. Los empleados que violen sus políticas deben estar sujetos a medidas disciplinarias.

Revisión anual de ciberseguridad

Debe revisar sus políticas de ciberseguridad al menos una vez al año y actualizar los procedimientos según sea necesario.

Restricciones basadas en la descripción del puesto y funciones

Su organización debe restringir el acceso a datos y sistemas confidenciales según las funciones y responsabilidades laborales de los empleados. Si alguien deja la organización, el acceso debe ser eliminado de inmediato.

Cuentas asignadas individualmente para el acceso al sistema de IT

Asegúrese de que cada empleado que tenga acceso a los sistemas de TI tenga su propia cuenta asignada y no compartida. Cada cuenta debe estar protegida por una contraseña segura u otra forma de autenticación. Si una cuenta se ve comprometida, el usuario debe cambiar su contraseña de inmediato.

Acceso remoto seguro

Asegúrese de que los miembros remotos del equipo utilicen una conexión segura para interactuar con sistemas y datos confidenciales, como una red privada virtual.

Cumplimiento de la ciberseguridad de los dispositivos personales

Si su organización permite que los empleados usen sus propios dispositivos para fines laborales, asegúrese de que todos los dispositivos se actualicen regularmente con el último software de seguridad y cumplan con los requisitos de ciberseguridad.

Prevención de productos tecnológicos falsificados

Debe tomar todas las medidas necesarias para evitar que productos tecnológicos falsificados o ilegítimos ingresen a su entorno de IT, el software sin una licencia adecuada puede contener malware.

Respalde de datos sistematico

Realice un respalde de datos sistematico al menos una vez a la semana o con la frecuencia que corresponda. Asegúrese de cifrar todos los datos y mantenerlos almacenados fuera del sitio.

Protección de información sensible de importación/exportación

Tome en cuenta todos los medios, hardware u otra tecnología que contenga datos confidenciales relacionados con el proceso de importación/exportación en sus inventarios regulares. Además, asegúrese de utilizar procesos de desinfección o destrucción aprobados por el NIST cuando se deshaga de estos artículos.

Fortalecer sus protecciones de ciberseguridad es solo un aspecto de los requisitos de CTPAT. También deberá implementar educación, capacitación y concientización sobre seguridad, realizar evaluaciones de riesgos, cumplir con los criterios de seguridad física y mucho más.

EE. UU. se alinea más estrechamente con programas similares como el Operador Económico Autorizado ("AEO"), que son el equivalente europeo y asiático de CTPAT.

CBP tiene grandes planes para la seguridad de importación/exportación a través de CTPAT. Uno de los anuncios recientes de CBP es el inicio de un programa piloto llamado Iniciativa Global Business Identifier ("GBI") que asignará un identificador único a cada importador y exportador en el mundo. EE. UU. se está asociando con otros 10 países (incluidos Canadá, Australia, Francia, etc.) para crear un prototipo de este programa en 2022 con el objetivo de armonizar aún más el movimiento mercantil dentro y fuera del país. Este avance construiría rápidamente la base de datos de empresas comerciales para ayudar a CBP a identificar cargas de alto riesgo.

Se espera otra actualización del MSC en 2022. Esto pone un enfoque adicional en los desafíos empresariales como la ciberseguridad y los problemas de cumplimiento social como la prevención de la esclavitud humana. En cierto modo, CTPAT apenas está comenzando...

Lo más importante es reunir a las partes interesadas claves de la alta dirección, recursos humanos y operaciones, y comprometerse a implementar CTPAT.

CTPAT es una obviedad para las empresas de logística que buscan competir en un campo más amplio con nombres más importantes, clientes educados y un enfoque transfronterizo. Hay distintas ventajas que ofrece el programa. En un futuro no muy lejano, CTPAT continuará expandiéndose, y CBP tiene planes de catalogar a todas las empresas que realizan transacciones en el comercio mundial. Si actualmente es un representante en carga internacional, podría tener más sentido involucrarse en CTPAT ahora.