Alerta C-TPAT por ciberamenazas en teletrabajo

En enero 2021, Customs and Border Protection (CBP) emitió a través del portal de C-TPAT el boletín "Ciberamenazas: La Nube y Conexiones Remotas", en el cual informa a los miembros de C-TPAT la importancia de la ciberseguridad, así como de las distintas amenazas a las que pueden ser susceptible al trabajar de forma remota y utilizar la nube para realizar actividades empresariales.

Debido a la contingencia sanitaria que está afectando al mundo en estos momentos, muchos de los miembros C-TPAT decidieron trabajar de forma remota o en modalidad de teletrabajo como una medida de protección. Asimismo, muchas compañías reportan que permitirán el trabajo remoto de forma permanente, incluso una vez ya terminada la pandemia.

Es por ello que C-TPAT ve la necesidad de recalcar que, al trabajar remotamente y tener operaciones en la nube, los miembros del programa siguen teniendo la responsabilidad de adherirse a los criterios de seguridad y a seguir realizando prácticas de ciberseguridad.

Muchas de las empresas que comenzaron a realizar operaciones de forma remota han sido víctimas de distintas amenazas cibernéticas que buscan aprovechar las vulnerabilidades cibernéticas con el fin de obtener información interna. Empresas globalmente han reportado accesos no autorizados a sus redes empresariales, así como la pérdida y secuestro de información.

Un análisis realizado por la Agencia de Ciberseguridad y Seguridad de la Infraestructura (por sus siglas en inglés CISA) reporta que una de las amenazas más observadas fue el *phishing*, el cual se trata de enviar un correo electrónico a los empleados con una liga web, la cual cuenta con distintas herramientas para poder obtener las credenciales necesarias para acceder a la información de la compañía una vez que el empleado hace *click* en ella.
En el boletín también se mencionan distintas acciones que pueden llevar a cabo los miembros C-TPAT para asegurar que sus empleados no sean susceptibles a estas amenazas.

- Utilizar autorizadores multifactores para acceder a las cuentas empresariales.
- Implementar una política que no permita a los empleados utilizar dispositivos personales para realizar actividades de trabajo.
- Restringir el envío de correo electrónicos a destinatarios fuera del dominio empresarial, así como prohibir a los empleados acceder a sus correos personales en los equipos de la compañía, así como enviar correos empresariales a su cuenta personal y viceversa.
- Prohibir a los empleados descargar programas no autorizados y realizar cambios a aplicaciones sin permiso previo.
- Llevar a cabo capacitaciones a los empleados para que conozcan las amenazas cibernéticas y realizar simulacros para verificar que los empleados tomen las medidas necesarias al momento de encontrarse con una amenaza.

Subcomité de Trade Compliance

- Contar con un sistema para que los empleados puedan notificar cualquier actividad sospechosa o cuando crean ser víctimas de un ciberataque. De esta forma se puede llevar a cabo las acciones necesarias para mitigar los riesgos.

La ciberseguridad es crucial en estos momentos que muchas empresas trabajan de forma remota. Para la protección de su información es importante conocer las distintas ciberamenazas que buscan acceder a ella. Te invitamos a asesorarte con TLC para que conozcas los estándares mínimos de seguridad para mantener la información y cadena de suministros segura.

Referencias: Boletín- Alerta C-TPAT "Ciberamenazas- La nube y conexión remota"

Fuente: División de Certificaciones OEA y C-TPAT, TLC Asociados S.C.

Atentamente:

Octavio de la Torre de Stéffano

Vicepresidente de cumplimiento en comercio exterior y aduanas en CANACINTRA Tijuana.

Alan Padilla Castellanos

Coordinador de Comités de trabajo en cumplimiento en comercio exterior y aduanas.