ALERTA CTPAT

Amenazas Cibernéticas – La Nube y Conexiones Remotas

Última actualización: Enero 22, 2021

Con el fin de mejorar la comunicación con nuestros miembros, el programa Alianza Aduanas Comercio Contra el el Terrorismo (CTPAT) destaca de manera periódica temas referentes a la seguridad con el propósito de aumentar la sensibilización y constante vigilancia por parte de los asociados hacia la seguridad de la cadena de suministro. Esta Alerta CTPAT destaca las amenazas que enfrentan las compañías miembros al utilizar soluciones tecnológicas a través de la nube y/o compañías que tienen empleados trabajando de manera remota.

Debido a la pandemia del COVID-19, muchos de nuestros miembros han transferido parte de su personal a la modalidad de teletrabajo o a la informática remota. Informes recientes de fuentes abiertas sugieren que muchas empresas permitirán a sus empleados trabajar de forma remota e incluso de forma permanente aún después de que desaparezca la amenaza del COVID-19.

Desde el inicio de la pandemia, actores que presentan amenazas han intentado aprovechar las debilidades asociadas con las configuraciones remotas de los computadores y han dirigido una serie de acciones adversas a través de ataques de phishing por correo electrónico (y vía teléfono), a los empleados. Históricamente ha sido una táctica común de los hackers el de explotar desastres, pandemias y grandes eventos políticos con el fin de lograr lanzar campañas de phishing convincentes. A nivel mundial, las empresas han reportado un aumento en intrusiones no autorizadas en la red, así como la pérdida de datos y el pago de rescate de información.

Las empresas pueden optar por llevar a cabo parte o la mayoría de sus procesos a través de soluciones y sistemas basados en la nube. Entre los servicios que utilizan sistemas en la nube se encuentran, por ejemplo, el despacho de camiones, la planificación de recursos empresariales, el almacenamiento de archivos y el correo electrónico empresarial. Algunos miembros de CTPAT han declarado que debido a que gran parte de sus transacciones comerciales se realizan a través de sistemas en la nube, no consideran estar obligados a seguir o a implementar algunos o todos los criterios mínimos de seguridad (CMS) cibernéticos. Esto no podría estar más lejos de la verdad, ya que al operar a través de la nube, a cualquier nivel, no exime al miembro CTPAT sobre su responsabilidad de adherirse a los CMS y seguir prácticas razonables y efectivas de ciberseguridad.

A principios de este mes, la Agencia de Seguridad de la Ciberseguridad e Infraestructura (CISA), una agencia que forma parte del Departamento de Seguridad Nacional de los Estados Unidos (DHS), publicó el Informe de Análisis AR21-013A*: Fortaleciendo las Configuraciones de Seguridad para Defensa Contra los Ataques a Servicios en la Nube*. Según este informe, "actores de amenazas están utilizando el phishing y otros actos ilícitos para aprovecharse de las malas prácticas en la configuración de los sistemas en la nube de las víctimas." En otras palabras, la CISA sostiene que las empresas que operan con sistemas en la nube aún están en riesgo de amenazas cibernéticas.

Por ejemplo, la CISA ha observado cómo criminales utilizan correos electrónicos de phishing con enlaces maliciosos para adquirir credenciales (lo que significa que los hackers envían correos electrónicos de phishing con enlaces dañinos y utilizan herramientas sofisticadas para extraer/robar las combinaciones de nombre de usuario y contraseña) de las cuentas de servicios en la nube.

Traducción al Español realizada por World BASC Organization para CBP. Su versión en inglés es el referente oficial.

ALERTA CTPAT

Amenazas Cibernéticas – La Nube y Conexiones Remotas

Última actualización: Enero 22, 2021

Los criminales cibernéticos incluyen enlaces en sus correos electrónicos phishing para que aparezcan como mensajes seguros o correos electrónicos confiables para que le den la información de inicio de sesión de una cuenta de servicio de archivos y alojamiento en la nube. Ver enlace al anuncio del FBI sobre "spoofing" o suplantación al final de esta alerta.

Todos los miembros de CTPAT deberán asegurarse que sus empleados estén entrenados de manera adecuada respecto a las campañas de phishing y las amenazas asociadas con la suplantación de dominio en la red (dirección web).

- Los Puntos de Contacto de CTPAT deben hablar sobre esta Alerta CTPAT y el informe de la CISA con su personal encargado de los Sistemas de Tecnologías de la Información (IT) (https://us-cert.cisa.gov/ncas/analysis-reports/ar21-013a). Los criterios de ciberseguridad del programa deben revisarse para determinar si, basándose en esta información, existen debilidades asociadas con los sistemas de conexión remota. Esta alerta afecta varios de los criterios de seguridad cibernética de CTPAT.

- El informe de la CISA describe varias de las acciones que las organizaciones pueden tomar para mitigar las amenazas y "…fortalecer las configuraciones de su información en la nube para protegerse, detectar y responder a potenciales ataques". A continuación se presentan algunas de las recomendaciones más importantes por parte de la CISA junto con su correspondiente criterio mínimo de seguridad (CMS) CTPAT.

  ✓ Aplíque la autenticación multifactor (MFA) / Implemente la MFA para todos los usuarios, sin excepción. Se debe exigir a todos los usuarios que tengan al menos un segundo factor para entrar en la red de una empresa, además de simplemente una contraseña o clave – CMS 4.8.

  ✓ Considere una política que no le permita a los empleados usar dispositivos personales para el trabajo. Como mínimo, utilice un sistema de administración de dispositivos móviles de confianza – CMS 4.10.

  ✓ Considere la posibilidad de restringir a los usuarios el reenvío de correos electrónicos a cuentas fuera de su dominio. Aunque esto no siempre es posible, considere agregar un encabezado a todos los correos electrónicos externos que deje claro que vinieron de fuera de la red de la empresa. Esto también debe significar que se debe prohibir a los empleados enviar correo electrónico desde la red de la empresa a su propia dirección de correo electrónico personal y viceversa. Además, considere prohibir a los empleados el acceso a su correo electrónico personal a través de la web desde los dispositivos de la empresa – MSC 4.1 y 4.5.

Traducción al Español realizada por World BASC Organization para CBP. Su versión en inglés es el referente oficial.

ALERTA CTPAT

Amenazas Cibernéticas – La Nube y Conexiones Remotas

Última actualización: Enero 22, 2021

- ✓ Permita a los usuarios a consentir sólo a aplicaciones integradas que hayan sido aprobadas previamente por un administrador. Restrinja a los empleados la descarga de programas, aplicaciones, etc. no autorizados o cambios en las conexiones de una aplicación a otra sin las aprobaciones necesarias. Esto también incluye desactivar o realizar cambios en el software antivirus instalado en sus dispositivos – MSC 4.1 y 4.5.

- ✓ Centrarse en la concientización y en la capacitación. Haga que los empleados sean conscientes de las amenazas, como las estafas de phishing y cómo éstas son transmitidas. La capacitación típicamente es una de las prioridades en la mayoría de las tareas cibernéticas por hacer y es considerada crucial. Muchos miembros prueban a sus empleados enviándoles correos electrónicos de phishing inofensivos periódicamente – MSC 12.1 y 12.8.

- ✓ Establezca prácticas para que los empleados sepan a quien contactar – sin la preocupación de culpabilidad –cuando vean actividades sospechosas o cuando crean que han sido víctimas de un ciberataque. Esto asegurará que la estrategia de mitigación apropiada y establecida pueda desplegarse de manera rápida y eficiente. Los empleados usualmente creen que al tener programas antivirus instalados en sus ordenadores y que por tener dicho software y la presencia de un departamento de IT, es suficiente para mantener su ordenador y su red seguros. Este no es siempre el caso. Debe motivarse a los empleados a que informen sobre las posibles actividades sospechosas – MSC 12.1.

Otros enlaces sobre Ciberseguridad

FBI – Spoofing of website addresses – Nota: Este Anuncio de Servicio Público fue publicado antes de las recientes elecciones, pero el documento sigue siendo de gran relevancia hoy en día. Este enlace abrirá un archivo adjunto pdf.

Stop. Think. Connect. – La Campaña STOP.THINK.CONNECT.™ Es una campaña nacional sobre concientización pública destinada a incrementar la concientización y conocimiento de las amenazas cibernéticas y a potencializar a los estadounidenses para que estén más seguros y más protegidos en línea. La ciberseguridad es una responsabilidad compartida. Cada uno de nosotros tiene que dar de su parte para mantener la seguridad en el Internet. Al tomar todos medidas sencillas de seguridad en línea, esto hará que el uso del Internet sea una experiencia más segura para todos.

CTPAT Cyber MSC Videos (YouTube) – Videos CTPAT y presentación de capacitación en PowerPoint que aborda específicamente cómo los miembros pueden cumplir con los criterios claves de seguridad cibernética.

Programa CTPAT

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW - Washington, DC 20229

Traducción al Español realizada por World BASC Organization para CBP. Su versión en inglés es el referente oficial.