Ciberseguridad - Contraseñas y Contraseñas en Frase (Criterio 4.8)

Última actualización: 15 de mayo de 2020

El programa de Asociación Aduana-Comercio contra el Terrorismo (CTPAT) no es más que uno de los múltiples niveles de la estrategia para el control de carga del Departamento de Aduanas y Protección Fronteriza de los Estados Unidos (CBP). A través de este programa, CBP trabaja con la comunidad comercial para fortalecer las cadenas de suministro internacionales y mejorar la seguridad fronteriza de los Estados Unidos.

Con el fin de mejorar la comunicación con sus miembros, CTPAT resalta de manera rutinaria asuntos de interés, abarcando temas de seguridad, hasta el reconocimiento de las mejores prácticas implementadas por los miembros para abordar sus preocupaciones y desafíos en materia de seguridad de la cadena de suministro.

Este boletín de CTPAT destaca el importante papel que juega el uso correcto de contraseñas y contraseñas en frase construidas adecuadamente, para ayudar a mantener una postura sólida entorno a la ciberseguridad. El criterio mínimo de seguridad 4.8 que aborda los requisitos para el uso de contraseñas, es obligatorio y exige a todos los miembros que hagan tres cosas para proteger el acceso a sus sistemas de Tecnología de la Información (TI):

1. Las personas con acceso a los sistemas de TI deben usar cuentas asignadas individualmente.
2. El acceso a los sistemas de TI debe protegerse de la infiltración mediante el uso de contraseñas seguras, contraseñas en frase, u otras formas de autenticación, y debe protegerse el acceso de los usuarios a los sistemas de TI.
3. Las contraseñas y/o contraseñas en frase, deben cambiarse lo antes posible si hay evidencia que han sido comprometidas o existe una sospecha razonable de que están siendo comprometidas.

La Guía de implementación para el criterio 4.8 recomienda que se otorgue acceso al usuario a través de un proceso de autenticación de dos factores (2FA) o de autenticación de múltiples factores (MFA). MFA es el más seguro porque requiere que un usuario presente dos o más pruebas (credenciales) para autenticar la identidad de la persona durante el proceso de inicio de la sesión. El uso de una contraseña segura o contraseñas en frase es un tipo de autenticación.

Contraseñas y contraseñas en frase: las contraseñas se componen generalmente de no más de 10 letras, números y símbolos. Este es un ejemplo de una contraseña segura: AT% ^ 8gr $.

Una contraseña en frase, por otro lado, es más larga que una contraseña y contiene espacios entre palabras. Una contraseña en frase puede o no ser una oración coherente; pueden ser simplemente cuatro o cinco palabras que no están relacionadas de ninguna manera. El tema común es que una contraseña en frase obliga al usuario a utilizar un mínimo de 12 caracteres, lo que hace básicamente imposible que un algoritmo pirata adivine la contraseña en frase. Este es un buen ejemplo de una contraseña en frase fuerte: sentado en la silla roja de la cocina, observé el bosque.

Ciberseguridad - Contraseñas y Contraseñas en Frase (Criterio 4.8)

Última actualización: 15 de mayo de 2020

CTPAT ahora recomienda que sus miembros usen contraseñas en frase en lugar de contraseñas simples. Esto se basa en las recomendaciones de expertos en el sector público y privado. Aquí hay cuatro razones por las cuales su empresa debería usar contraseñas en frase en lugar de contraseñas simples:

1. Las contraseñas en frase son más fáciles de recordar que las contraseñas simples.
2. Las contraseñas son relativamente fáciles de adivinar o descifrar. Los delincuentes en línea utilizan herramientas de piratería de última generación que les permiten descifrar incluso las contraseñas más complicadas. Las contraseñas en frase, por otro lado, son mucho más difíciles de descifrar porque las herramientas de descifrado de contraseñas se descomponen alrededor de 10 caracteres.
3. No es necesario cambiar las contraseñas en frase debidamente construidas, a menos que el usuario sospeche que la contraseña en frase se ha visto comprometida o existe un compromiso.
4. Los principales sistemas operativos, incluidos Windows, Linux y Mac, admiten el uso de contraseñas en frase, lo que les permite tener hasta 127 caracteres de longitud.

Para aquellos miembros de CTPAT que eligen continuar usando contraseñas simples, se deben seguir las siguientes recomendaciones para ayudar a fortalecer esas contraseñas y mantenerlas seguras. Según la orientación actual del Instituto Nacional de Estándares y Tecnología (NIST), no es necesario cambiar las contraseñas regularmente si se cumplen estas mismas recomendaciones:

- No usar contraseñas que se basen en información personal o a las que se pueda acceder o adivinar fácilmente. Evitar el uso de cumpleaños, nombres de mascotas, películas y libros favoritos que se pueden encontrar mediante una búsqueda rápida en los sitios de redes sociales. Se debe prohibir a los usuarios usar sus nombres o el nombre de la empresa para construir una contraseña.

- Las contraseñas no pueden contener palabras del diccionario.

- Verificar las contraseñas nuevas y existentes con una base de datos actualizada de manera contínua sobre las contraseñas en lista negra. Las contraseñas regulares que tienen alrededor de 8 caracteres siguen siendo muy fáciles de descifrar y cada vez se muestran más descifradas en la web oscura. Esencialmente, están en las listas negras que usan los piratas informáticos y también los gerentes de TI para completar en sus sistemas de verificación de listas negras.

- Cuando el usuario intenta ingresar una nueva contraseña, esa contraseña deberá ser verificada por un sistema automatizado de TI. Estas verificaciones del departamento de TI deben realizarse cuando se crean las contraseñas, y deben seguir realizándose de manera contínua, preferiblemente a diario. Estas verificaciones deben ser realizadas frente a una base de datos en vivo, y no en una lista estática. La contraseña segura de ayer, puede no ser segura hoy, debido a una nueva violación o fuga de información.

- Tener un proceso documentado en caso de que se detecte una contraseña comprometida.

- Usar diferentes contraseñas para diferentes cuentas.

- No permitir que un usuario elija una contraseña que sea la misma que cualquiera de sus últimas cuatro contraseñas.

Ciberseguridad - Contraseñas y Contraseñas en Frase (Criterio 4.8)

Última actualización: 15 de mayo de 2020

- Requerir que las páginas de inicio de sesión de la cuenta utilicen cifrado, incluida una dirección URL que comience con "https". La "s" indica un sitio seguro o encriptado en lugar de "http", que no está encriptado. Buscar también el icono del candado en la barra del navegador. Si el ícono del candado aparece en la página web, pero no en la barra del navegador, podría tratarse de un gráfico insertado por un ciberdelincuente para engañar y que usted se sienta seguro. Además de esto, se debe mover el mouse sobre el enlace para ver la dirección. Si tiene alguna duda sobre si el sitio al que planea acceder es legítimo o no, comuníquese con la compañía para confirmar la página de inicio de sesión real.

Las contraseñas y frases de contraseña seguras son sin duda esenciales para la seguridad, pero no tienen ningún valor si los usuarios no aprenden cómo protegerlas y usarlas con prudencia. Los usuarios deben estar debidamente capacitados sobre cómo generar contraseñas seguras y mantenerlas seguras. Nunca deben compartir sus contraseñas o frases de contraseña con nadie. No escriba contraseñas en notas adhesivas y no las pegue en monitores u otras superficies que estén al aire libre. Si los usuarios no pueden recordar sus contraseñas, pueden escribir sugerencias para ayudarlos a recordarlas, pero estas sugerencias deben almacenarse de forma segura, por ejemplo, en un cajón cerrado. También se puede usar un administrador de contraseñas cifradas. Además de mantener seguras las contraseñas / frases, nunca deje los dispositivos informáticos sin protección.

La ciberseguridad es una responsabilidad compartida. Sólo se necesita una computadora infectada para comprometer potencialmente miles y quizás millones de otras. Pero al final del día, la seguridad cibernética se trata en última instancia de las personas. La tecnología más impresionante y sofisticada no tiene valor si no es operada y mantenida por usuarios informados y conscientes. Por lo tanto, capacitar a sus empleados en ciberseguridad es fundamental.

Recursos:
STOP. THINK. CONNECT. https://www.stopthinkconnect.org/, esta es la campaña global de concientización de seguridad en línea para ayudar a todos los ciudadanos digitales a mantenerse más seguros y protegidos en línea.

Como asesor de riesgos de la Nación, la Agencia de Seguridad de la Infraestructura y Ciberseguridad (CISA) brinda amplios conocimientos y prácticas de seguridad en torno a la ciberseguridad y la infraestructura a sus partes interesadas, comparte ese conocimiento para permitir una mejor gestión del riesgo y lo pone en práctica para proteger los recursos esenciales de la Nación. CISA mantiene el Sistema Nacional de Concienciación Cibernética. Sus cinco productos ofrecen una variedad de información para usuarios con experiencia técnica variada. Una suscripción a cualquiera o todos los productos del Sistema Nacional de Concienciación Cibernética garantiza que tenga acceso a información oportuna sobre temas de seguridad y amenazas. Para obtener más información suscríbase, visitando https://www.us-cert.gov/ncas.

Programa CTPAT

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