FUNDAMENTOS DE LA SEGURIDAD DE DATOS DE PAGO

Acceso remoto seguro

¿CUÁL ES EL RIESGO?

#1

el punto de entrada de ataques contra los comerciantes físicos es por acceso remoto inseguro

(Prácticas recomendadas sobre tecnología para accesos remotos)

El acceso remoto inseguro es una de las causas principales de compromiso de datos de las empresas.

A menudo, los proveedores de puntos de venta (POS) apoyan o resuelven problemas de los sistemas de pago de los comerciantes desde su oficina, no en la ubicación del negocio. Lo hacen a través de Internet y por productos que se llaman software de "acceso remoto". Muchos de estos productos siempre estan encendidos o disponibles – y eso significa que el proveedor puede acceder a sus sistemas de manera remota en cualquier momento.

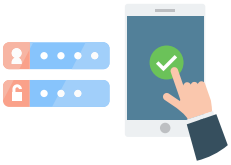
Muchos de estos proveedores utilizan contraseñas muy conocidas para el acceso remoto, lo que facilita a los hackers el acceso a sus sistemas. Buscan en Internet las empresas con sistemas vulnerables de acceso remoto y, una vez dentro, utilizan malware para robar los datos de tarjetas de pago.

PRÁCTICAS RECOMENDADAS PARA EL ACCESO REMOTO

Para minimizar el riesgo de que se produzcan vulnerabilidades de datos, es importante que usted gestione cómo y cuando los proveedores pueden acceder a sus sistemas. ¡Permita el acceso remoto solo cuando sea necesario!

Limite el uso del acceso remoto

Pregunte a los proveedores cómo se habilita el acceso remoto cuando lo soliciten en forma específica y cómo deshabilitarlo cuando no es necesario.



Solicite el uso de autenticación de factores múltiples

Si debe permitir el acceso remoto, solicite a sus proveedores que utilicen la autenticación de factores múltiples para dar soporte a su negocio.

Solicite identificaciones únicas

Si debe permitir el acceso remoto, asegúrese de que sus proveedores utilicen identificaciones de acceso remoto que sean únicas para su negocio y que sean las mismas que las que utilizan con otros clientes.

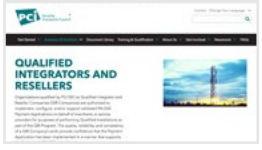
La autenticación de factores múltiples protege el acceso remoto de su negocio al solicitar un nombre de usuario y contraseña, además de otros factores (como una tarjeta inteligente o llave electrónica). Una llave electrónica es un dispositivo práctico que se conecta a una computadora para permitir el acceso a herramientas inalámbricas de software, etc.

RECURSOS

Visite **pcissc.org/Merchants** donde encontrará más recursos

El recurso preguntas que debe hacer a sus proveedores del PCI SSC puede ayudar a las empresas a obtener la información que requieren de sus proveedores terceros.

La Guía de pagos seguros proporciona a las empresas la información básica de seguridad para protegerse contra el robo de datos de pago.



La lista de integradores calificados de PCI y revendedores (QIR) es un recurso que las empresas pueden aprovechar para encontrar instaladores de servicios de pago que hayan recibido capacitación del PCI Security Standards Council sobre acceso remoto seguro y otros fundamentos de seguridad de datos de pago.

Vea este video rápido animado para que conozca la forma en que las empresas pueden minimizar las posibilidades de una vulnerabilidad a sus datos permitiendo el acceso remoto solo cuando sea necesario y utilizando autenticaciones de factores múltiples.

PCI Security Standards Council