FORTRA

GUÍA (Powertech)

Novedades sobre el Estándar de Seguridad de Datos PCI 3.2

Si usted trabaja para una empresa que procesa tarjetas de crédito y débito, ya debe estar familiarizado con las exigencias para cumplir con PCI DSS. El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es una norma de Seguridad de la Información, exclusiva para organizaciones que procesan tarjetas de crédito o débito.

Se trata de una regulación dinámica que se actualiza con frecuencia, de acuerdo al surgimiento de nuevas amenazas de Seguridad o para aclarar cuestiones que generaron confusión en versiones anteriores. La versión 3.2 de PCI DSS fue anunciada en abril de 2016, de modo que muchas empresas se encuentran en plena transición de 3.1 a 3.2. Si bien PCI DSS 3.1 venció en octubre de 2016, todos los requisitos actualizados pasaron a formar parte de las mejores prácticas hasta el 1o de febrero de 2018, cuando se convertirán en obligatorios. Existe solo una excepción: la fecha límite para migrar de SSL y de la anterior TLS, se pospuso hasta junio de 2018.

Estar al día en el cumplimiento de PCI DSS, lo ayudará a evitar costosas multas y a proteger a su empresa de una potencial filtración de datos. A continuación, le explicamos lo que necesita saber para estar listo para PCI DSS 3.2.

PCI 3.2

Implicaciones para las soluciones de Transferencia Gestionada de Archivos

Fecha límite para cumplir con PCI DSS 3.2: **1º de FEBRERO de 2018**

¿Por Qué se Actualiza PCI DSS?

La Seguridad Informática evoluciona constantemente para abarcar nuevas tecnologías y amenazas. El ***PCI Security Standards Council*** actualiza las regulaciones de PCI DSS para abordar estas nuevas preocupaciones y proporcionar mayor claridad con respecto a los requisitos existentes.

En esta oportunidad, algunos sectores se sorprendieron con el lanzamiento de una versión 3.2, en lugar de una versión 4. Sin embargo, sucede que PCI DSS ya es un estándar lo suficientemente avanzado como para requerir actualizaciones de base, como las que tuvieron lugar en el pasado. Es probable que las futuras modificaciones de PCI DSS también sean graduales.

¿Quién Debe Cumplir con el Nuevo Estándar

Toda organización que procese datos de titulares de tarjetas debe estar atenta al cumplimiento de PCI DDS. Sin embargo, no todos los requisitos de PCI DSS aplican a todas las empresas. Si bien algunos de los cambios de la versión 3.2 abarcan a todas las entidades, varias actualizaciones están destinadas específicamente a proveedores de servicios. El Anexo A3, DESV, se aplica solamente a entidades designadas por las marcas de pago o a adquirientes que necesiten evaluación adicional.

¿Cuáles son las diferencias en PCI DSS Versión 3.2?

Si bien se reelaboraron ligeramente muchos requisitos para dar mayor claridad o para tomar en cuenta los cambios en la terminología de la industria, son cinco las actualizaciones principales para las cuales las empresas deben estar preparadas. Las tres que se aplican a todas las empresas son la autenticación multi-factor, la migración de SSL y TLS, y el almacenamiento del número de cuenta primaria (PAN). Si usted es proveedor de servicios o integra la categoría DESV (Validación Suplementaria de las Entidades Designadas), también deberá tener en cuenta otras cuestiones.

Autenticación Multi-Factor

La protección del acceso administrativo al entorno de datos del titular de la tarjeta (CDE) es fundamental. Independientemente del método utilizado para obtener acceso a una red, el objetivo de un intruso normalmente es encontrar un dispositivo desde el que pueda obtener derechos administrativos. Una vez que los obtiene, puede moverse en toda la red, obteniendo acceso a otros equipos hasta llegar a los datos del titular de la tarjeta. La autenticación multi-factor proporciona protección adicional en los puntos cruciales.

El requisito 8.3 de la versión anterior de PCI DSS establecía que las organizaciones debían incorporar autenticación de doble factor para un acceso remoto que se origine desde afuera de la red. En la versión 3.2, el término “autenticación de dos factores” se cambió por “autenticación multi-factor” para establecer la posibilidad de contar con más de dos formas de autenticación. Además, el requisito se amplió para incluir a todos los accesos administrativos individuales sin consola, así como a todos los accesos remotos al CDE. Con este cambio, quienes permitan cualquier clase de acceso sin consola necesitarán autenticación multi-factor, independientemente de si ese acceso es remoto desde la propia red de la organización, o desde el CDE.

Las actualizaciones de requisitos de PCI DSS 3.2 relacionadas con la autenticación multi-factor, migración de SSL y TLS, y el alcance a proveedores, ***APLICAN A TODAS LAS ORGANIZACIONES***

Migración de SSL y TLS Anterior

La capa de puertos seguros (SSL) apareció en la década de 1990 y creció hasta convertirse en un estándar de seguridad ampliamente aceptado. Sin embargo, ahora se considera que SSL tiene varias vulnerabilidades. En 1999, la versión 3.1 de SSL fue lanzada como seguridad de la capa de transporte (TLS) 1.0. Si bien TLS mejoró la seguridad de SSL, TLS versión 1.0 (y en algunos casos 1.1) ya no es considerada sólida. La versión 3.2 de PCI DSS requiere que las organizaciones se enfoquen en contar con un sólido protocolo criptográfico, que implique al menos TLS 1.1, aunque se recomienda firmemente que sea TLS 1.2.

Esto aplica para algunos requisitos de PCI DSS que exigen sólida criptografía o características adicionales de seguridad como los requisitos 2.2.3, 2.3 y 4.1. La versión 3.2 de PCI DSS exige que todos los proveedores de servicios hayan implementado un servicio seguro para junio de 2016.

*El **30 DE JUNIO DE 2018** es la fecha límite para migrar las implementaciones de TLS existentes a versiones de TLS más recientes*

Otras entidades no deben utilizar SSL ni el anterior TSL en ninguna nueva implementación. Las organizaciones tienen tiempo hasta el 30 de junio de 2018 para incorporar las versiones actuales de TLS sobre las implementaciones existentes. Antes de esa fecha, las implementaciones existentes que utilizan SSL o la anterior TLS deben ejecutar un Plan Formal de Migración y Mitigación de Riesgos.

Cumplimiento de PCI DSS para Proveedores de Servicios

Los proveedores de servicios tienen un papel fundamental para sus clientes en la protección de datos de los titulares de tarjetas, y las debilidades en sus prácticas de seguridad han sido un factor común de las filtraciones.

Según un estudio de Ponemon Institute, casi la mitad de los profesionales especializados en riesgo afirma que su organización experimentó una filtración de datos a causa de uno de sus proveedores. El 73% considera que está aumentando la cantidad de incidentes de seguridad informática que involucran a los proveedores, mientras que el 65% considera que es difícil gestionar los incidentes de seguridad que implican a sus proveedores.

PCI DSS 3.2 presenta varios requisitos nuevos de seguridad para proveedores de servicios, principalmente para aquellos que tengan mayor responsabilidad en la seguridad de sus clientes.

Los proveedores de servicios ahora tendrán que detectar y notificar a los clientes de los sistemas de control de seguridad que presentan fallas críticas. Cada seis meses, deberán realizar una prueba de penetración de terceros, en lugar de hacerlo solo una vez al año, como exigía la versión anterior de PCI DSS. Además, deben realizar revisiones trimestrales de los empleados y sus respectivos accesos al CDE. Finalmente, los proveedores de servicios tendrán también que proporcionar documentación acerca de su arquitectura de encriptación.

Validación Suplementaria de las Entidades Designadas (DESV)

La DESV o Anexo A3 de PCI DSS versión 3.2, aplica solo a entidades designadas por una marca de pago o adquirentes que necesiten validación adicional. Por ejemplo, esto podría ser necesario porque están almacenando y transmitiendo especialmente un gran volumen de datos de titulares de tarjetas de crédito o porque han tenido algún problema en el pasado, como una filtración. Sin embargo, se recomienda que todas las organizaciones sigan los procedimientos detallados.

La DESV pretende que el cumplimiento del estándar PCI DSS se transforme en una práctica continua y no sea una molestia que se deba cumplir para sacar del medio y luego ser olvidada. El estudio más reciente de Verizon acerca del cumplimiento de PCI descubrió que solo el 29% de las empresas sigue cumpliendo el estándar un año después de

su validación. Las organizaciones comprendidas por la DESV deben implementar un programa de cumplimiento de PCI DSS y validar que se han incorporado las mejores prácticas de PCI DSS a las actividades comerciales usuales, entre otros requisitos.

¿Cómo afecta PCI DSS 3.2 a la Transferencia Gestionada de Archivos?

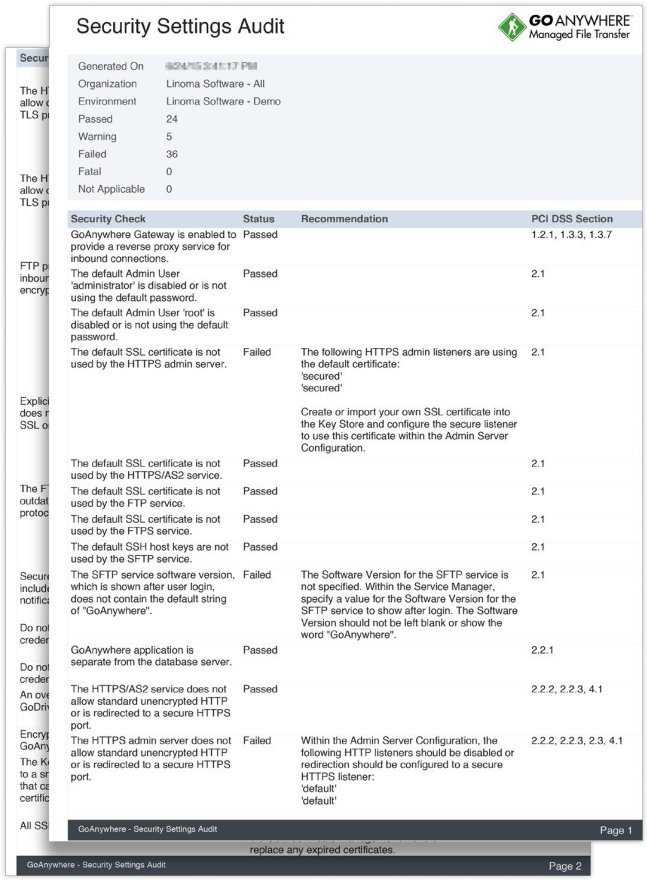
Casi todas las organizaciones se ocupan de transferencias de archivos, y si se le exige cumplir con PCI DSS, querrá asegurarse de que está utilizando una solución de transferencia gestionada de archivos que le permita cumplir con la nueva versión de la reglamentación.

¿Qué Significa?

En primer lugar, su software de transferencia gestionada de archivos (MFT) debe admitir TLS 1.1 y 1.2 para asegurar el cumplimiento y la actualización de los estándares de cifrado. En segundo lugar, la solución debe admitir seguridad basada en roles con autenticación multifactorial. PCI DSS exige autenticación multifactorial a nivel de la red o a nivel del sistema.

Su empresa quizás esté o no comprendida en la DESV, pero en cualquier caso, debe considerar cómo mantener el cumplimiento de PCI DSS durante todo el año sin sumar demasiado esfuerzo ni tiempo extra a la carga de trabajo de TI. Las sólidas soluciones de MFT agilizan el trabajo proporcionando las características de seguridad y los informes detallados que desean los auditores. Algunos softwares de MFT pueden ayudarlo a verificar fácilmente si sus transferencias de archivos cumplen con PCI DSS.

Si aún no ha implementado una solución de transferencia gestionada de archivos con la última versión 3.2 de PCI DSS, ahora es el momento perfecto. MFT lo ayudará a cumplir con esta versión de PCI DSS y con las futuras actualizaciones también, ya que una buena solución de transferencia gestionada de archivos continuará incorporando características de seguridad para mantenerse a tono con las amenazas vigentes.



Security Settings Audit

GO ANYWHERE Managed File Transfer

Generated On	[redacted]
Organization	Linoma Software - All
Environment	Linoma Software - Demo
Passed	24
Warning	5
Failed	36
Fatal	0
Not Applicable	0

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Passed		1.2.1, 1.3.3, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Passed		2.1
The default Admin User 'root' is disabled or is not using the default password.	Passed		2.1
The default SSL certificate is not used by the HTTPS admin server.	Failed	The following HTTPS admin listeners are using the default certificate: 'secured' 'secured' Create or import your own SSL certificate into the Key Store and configure the secure listener to use this certificate within the Admin Server Configuration.	2.1
The default SSL certificate is not used by the HTTPS/AS2 service.	Passed		2.1
The default SSL certificate is not used by the FTP service.	Passed		2.1
The default SSL certificate is not used by the FTPS service.	Passed		2.1
The default SSH host keys are not used by the SFTP service.	Passed		2.1
The SFTP service software version, which is shown after user login, does not contain the default string of "GoAnywhere".	Failed	The Software Version for the SFTP service is not specified. Within the Service Manager, specify a value for the Software Version for the SFTP service to show after login. The Software Version should not be left blank or show the word "GoAnywhere".	2.1
GoAnywhere application is separate from the database server.	Passed		2.2.1
The HTTPS/AS2 service does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Passed		2.2.2, 2.2.3, 4.1
The HTTPS admin server does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Failed	Within the Admin Server Configuration, the following HTTP listeners should be disabled or redirection should be configured to a secure HTTPS listener: 'default' 'default'	2.2.2, 2.2.3, 2.3, 4.1

GoAnywhere - Security Settings Audit Page 1

replace any expired certificates.

GoAnywhere - Security Settings Audit Page 2

Bonus: Para Suarios de GoAnywhere® MFT

Si usted es usuario de GoAnywhere MFT, tenemos buenas noticias para usted. GoAnywhere MFT proporciona herramientas para ayudarlo a que sus transferencias de datos cumplan con el estándar PCI DSS. GoAnywhere MFT admite TLS 1.1 y 1.2, y se puede integrar con LDAP y autenticación multifactorial RSA externa.

Más aún, el módulo de generación avanzada de informes de GoAnywhere MFT puede generar informes de auditoría de configuración de seguridad para que pueda saber fácilmente si la configuración de seguridad de su instalación GoAnywhere está completamente adaptada a los requisitos de PCI DSS. Además de la verificación del estado, el informe recomienda acciones y le permite saber a qué sección de PCI DSS corresponde la configuración.

El estándar PCI DSS continuará evolucionando, pero al implementar soluciones sólidas, los negocios de TI con visión de futuro pueden cumplir los requisitos actuales y preparar una base sólida para las futuras mejoras de seguridad.

Acerca de GoAnywhere MFT

***GoAnywhere® Managed File Transfer** es una solución empresarial para la gestión de transferencias de archivos, que agiliza, asegura y automatiza el intercambio de archivos entre los sistemas, empleados, clientes y socios comerciales de organizaciones de todos los tamaños. Para implementar localmente, en la nube o en entornos híbridos, esta solución proporciona un único punto de control que permite alcanzar fácilmente el cumplimiento de normativas, mejorar la seguridad de la información, y agilizar los procesos manuales.*

Acerca de Fortra

Más de 10 mil empresas alrededor del mundo confían en las soluciones y productos de Fortra para monitorizar y automatizar sus procesos, encriptar y asegurar sus datos, y gestionar el acceso de sus equipos a la información. Con su oferta de software y servicios, Fortra simplifica el día a día de los Departamentos de IT, y los ayuda a alinear sus objetivos con lo de Negocio.

Más información en www.fortra.com/es.

Obtenga más información acerca de las soluciones de seguridad de Fortra en
www.fortra.com/es

FORTRA

Fortra.com

Sobre Fortra

Fortra es una compañía de Ciberseguridad como ninguna otra. Hemos creado un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com/es.

 (fta-pt-wp-es-1122-r1-79d)