safetica

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

Cómo ayuda Safetica a cumplir con PCI-DSS

Versión: 2022-08-08

Introducción a PCI DSS

¿Qué es PCI DSS?

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un conjunto de estándares de seguridad diseñados para garantizar que todas las empresas que aceptan, procesan, almacenan o transmiten información de tarjetas de crédito mantengan un entorno seguro.

¿A quién se aplica el PCI DSS?

El PCI DSS se aplica a CUALQUIER organización, independientemente del tamaño o número de transacciones, que acepte, transmita o almacene cualquier dato del titular de la tarjeta.

¿Qué significa "datos del titular de la tarjeta"?

El Consejo de Normas de Seguridad (SSC) de PCI define los "datos del titular de la tarjeta" como el número de cuenta principal (PAN) completo o el PAN completo junto con cualquiera de los siguientes elementos:

- Nombre del titular de la tarjeta
- Fecha de caducidad
- Código de servicio

Los datos de autenticación confidenciales, que también deben protegerse, incluyen datos completos de banda magnética, CAV2, CVC2, CVV2, CID, PIN, bloques de PIN y más.

¿Las organizaciones que utilizan terceros (procesadores) tienen que ser compatibles con PCI DSS?

Sí. El simple hecho de utilizar un tercero (procesador) no excluye a la empresa del cumplimiento de PCI DSS. Puede reducir su exposición al riesgo y, en consecuencia, reducir el esfuerzo para validar el cumplimiento. Sin embargo, eso no significa que puedan ignorar el PCI DSS.

¿Cuáles son las sanciones por incumplimiento?

Las marcas de pago pueden, a su discreción, multar a un banco adquirente de $5,000 a $100,000 por mes por violaciones del cumplimiento de PCI. Lo más probable es que los bancos pasen esta multa hasta que finalmente llegue al comerciante. Además, lo más probable es que el banco termine su relación o aumente las tarifas de transacción. Las sanciones no se discuten abiertamente ni se publicitan ampliamente, pero pueden ser

catastróficas para una pequeña empresa. Es importante estar familiarizado con el acuerdo de su cuenta comercial, que debe describir su exposición.

Desafíos relacionados y cómo Safetica ayuda a superarlos

1. Cumplimiento de la política de seguridad de la empresa

PCI requiere que cree e implemente políticas de seguridad de la información bien definidas, alineadas y actualizadas para proteger los datos confidenciales de los titulares de tarjetas. Esto se puede hacer fácilmente sobre el papel, pero es difícil hacer cumplir estas políticas a nivel de TI.

Safetica permite monitorear las operaciones de los usuarios en toda la organización. Puede reconocer información financiera confidencial y generar informes sobre cómo se procesan los datos.

Con base en su clasificación de datos, Safetica puede aplicar políticas de DLP y, por lo tanto, hacer cumplir las políticas de seguridad seleccionadas y el comportamiento deseado del usuario cada vez que los usuarios interactúan con información personal o financiera. Esto ayuda a los empleados a seguir las mejores prácticas y evitar métodos no seguros o prohibidos de almacenamiento y trabajo con datos confidenciales.

2. Protección de datos del titular de la tarjeta

Los dueños de negocios que almacenan información del titular de la tarjeta están obligados a protegerla. La recomendación clave es almacenarlos como datos cifrados para que sean indescifrables incluso para alguien que irrumpa en la red o el almacenamiento.

Mediante la inspección de contenido con OCR, Safetica puede clasificar automáticamente los datos de PCI-DSS y aplicar políticas de DLP que definen dónde se pueden almacenar dichos datos, dónde pueden fluir y cómo. Esto garantiza un almacenamiento seguro y limita el acceso solo al personal crítico.

Safetica también administra el cifrado de almacenamiento (Microsoft Bitlocker) en toda la organización para garantizar que cualquier PHI almacenada en reposo esté protegida en caso de que el dispositivo de punto final se vea comprometido físicamente. Las claves de cifrado se comparten de forma segura entre los dispositivos protegidos inscritos, lo que

elimina la necesidad de que los usuarios las conozcan o compartan, lo que puede introducir un factor de riesgo humano.

3. Visibilidad de los datos

Es muy importante saber dónde se almacenan sus datos confidenciales y los datos confidenciales del titular de la tarjeta y cómo sus empleados procesan dichos datos. Debe asegurarse de que el procesamiento de datos sea seguro y reducir el riesgo de fuga de datos.

El monitoreo y la auditoría detallados de los archivos y las operaciones de los usuarios de Safetica proporcionan una visión general de los flujos de información, el almacenamiento de datos confidenciales críticos e información detallada sobre:

- ¿Con qué partes externas y almacenamientos exactos se ha contactado?
- cuál de ellos recibió los datos confidenciales de la organización.

4. Notificación de fuga de datos

Si experimenta un evento de seguridad relacionado con la fuga de datos del titular de la tarjeta, debe ser informado del incidente de inmediato para que pueda reaccionar y minimizar cualquier impacto, o mejor aún, evitar que la información se filtre.

En el caso de un incidente de seguridad de datos real o intentado, el sistema de alerta por correo electrónico en tiempo real de Safetica notifica al personal correspondiente. Informa rápidamente del incidente y proporciona suficientes detalles para que puedan evaluar el impacto de la situación y tomar medidas de seguimiento.

Safetica también proporciona amplios registros de auditoría sobre operaciones realizadas con datos confidenciales. Esto ayuda a identificar la profundidad de la infracción, los documentos confidenciales afectados y las personas afectadas.

Con la integración de API, todos los registros también se pueden enviar a SIEM o herramientas de análisis de datos, por ejemplo, Power BI o Tableau.

Casos de uso clave

El banco necesita proteger los datos de los clientes

Un banco europeo con un entorno corporativo compuesto por empleados internos, contratistas externos y socios comerciales debe respaldar la protección de la confidencialidad bancaria, PCI-DSS y GDPR.

Problema: Una empresa con un entorno complejo con miles de usuarios internos y externos, endpoints (clientes pesados), clientes ligeros (Citrix) tiene una necesidad crítica de mantener contenida de forma segura toda la información sensible/confidencial que suele estar relacionada con los clientes bancarios. El objetivo es crear un entorno de desarrollo seguro y el perímetro seguro definitivo desde el que los datos no deben filtrarse bajo ninguna circunstancia. Para proteger los datos en los endpoints y en la nube, se requiere la integración con otros sistemas. Sin embargo, la protección de datos no debe ir en detrimento de la productividad de los empleados en los mostradores.

Solución

- Safetica ONE Enterprise, con clasificación de datos basada en el contenido y el contexto, detecta datos confidenciales basados en diccionarios integrados y palabras clave personalizadas, pero también permite la clasificación de usuarios y la justificación de las operaciones de datos confidenciales requeridas. La integración con Microsoft 365 y Microsoft Information Protection es compatible con la seguridad de los datos en la nube y la seguridad de los datos ya clasificados por el software elegido por la empresa.
- La protección del entorno de escritorio virtual evita la fuga de datos de producción en el entorno de prueba, pero también restringe el posible uso indebido de los datos del cliente por parte de los desarrolladores.
- Con el control de dispositivos, el banco tiene control sobre qué unidades flash USB se pueden usar en el perímetro seguro. BitLocker, administrado por Safetica Management Center, garantiza que todos los datos confidenciales y las unidades estén cifrados.
- El módulo UEBA opcional proporciona información más detallada sobre las aplicaciones que los usuarios estaban ejecutando y los sitios web que visitaron, y permite un control granular del uso permitido del sitio web.

Resultados: Con Safetica ONE Enterprise, el banco puede crear y mantener un perímetro seguro que evita la fuga de datos de los clientes y respalda la protección de la confidencialidad bancaria y el cumplimiento de PCI-DSS y GDPR.