CASO DE ESTUDIO

MERCURY PROCESSING SERVICES INTERNATIONAL PROTEGE SU CRECIMIENTO GRACIAS A UNA PROTECCIÓN DE DATOS CONFORME AL RGPD Y A LA PCI

Mercury Processing Services International es una empresa de procesamiento de pagos con sedes en Croacia y Eslovenia. Prestan servicio a más de 5,6 millones de cuentas en los sectores financiero y bancario en Europa, Oriente Medio y África, procesando de media 1,5 millones de transacciones al día. Los conocimientos tecnológicos son el principal impulso para mejorar y enriquecer sus relaciones comerciales, así como la principal fuente de todas las innovaciones que brindan a la industria de los pagos.

DESAFÍO: PROTECCIÓN DE DATOS CONFORME A LA PCI Y AL RGPD

El proyecto comenzó planteando la exigencia de la PCI sobre proteger los datos de titulares de tarjeta, aumentándose más adelante para abarcar la protección de otros datos a fin de cumplir con el RGPD.

Conforme al requisito 3.4 de la PCI, los datos de titulares de tarjeta deben hacerse ilegibles en el lugar en el que se almacenen. Los datos de titulares de tarjeta se refieren al número de tarjeta (PAN) y a cualquier dato que pueda vincularse directamente con un PAN específico, como el nombre del titular.

Los requisitos del RGPD van un paso más allá, ya que requieren una protección similar para los datos personales. Los datos personales tienen un alcance mucho más amplio que los datos de titulares de tarjeta y se definen como cualquier dato que pueda asociarse con una persona real, como el nombre, la dirección, la nacionalidad, los datos biométricos, etc.

Además, tanto el RGPD como la PCI DSS hacen hincapié en que los datos sensibles solo sean visibles cuando sea necesario dentro de la organización y para sus socios. Esto significa que deben hacerse ilegibles dentro de la organización para evitar una exposición accidental a miembros del personal y socios.

Mercury necesitaba una solución que protegiese correctamente todos esos tipos de datos no solo en aras del cumplimiento, sino también para contar con otra capa de protección que dejara los datos inservibles para posibles hackers. Los hackers están constantemente ideando nuevas formas de introducirse en los sistemas, por lo que es esencial que en la estrategia de seguridad de la organización se priorice una solución centrada en los datos para que, en caso de filtración, los datos a los que se ha accedido no sean aprovechables.

DATOS DE INTERÉS

- Este procesador de pagos que maneja 1,5 millones de transacciones al día ahora cumple con los requisitos de seguridad de la PCI y el RGPD al hacer ilegibles los datos sensibles.
- Una protección eficiente de los datos permitirá a Mercury procesar un volumen aún mayor de transacciones.
- Solución altamente flexible y escalable implementada de forma rápida y sencilla.

PROTEJA SU CRECIMIENTO CON COMFORTE

Con más de 20 años de experiencia en la protección de datos en sistemas críticos, comforte es el socio ideal para organizaciones que quieren proteger su activo más valioso: los datos. La suite de protección de datos de comforte, SecurDPS, se ha desarrollado desde cero para resolver de la mejor manera posible los problemas relacionados con la seguridad de los datos en un mundo marcado por las innovaciones digitales, la cada vez mayor independencia de los clientes y las continuas disrupciones tecnológicas.

Estamos a su disposición para ayudarle a proteger su crecimiento mediante nuestra experiencia, nuestra innovadora suite tecnológica y nuestro soporte local.

Para saber más, póngase en contacto con un representante de comforte visitando www.comforte.com/contact/.

SOLUCIÓN

Mercury eligió SecurDPS de comforte para proteger sus datos por el hecho de que cumplía con sus requisitos sobre protección de datos y podía implementarse de manera rápida y sencilla sin necesidad de interrumpir la actividad.

Seguridad centrada en los datos
SecurDPS reduce el riesgo empresarial y reemplaza los datos sensibles sin encriptar por un token que carece de sentido si se ve expuesto. Una estrategia de seguridad centrada en los datos protege los propios datos de manera que, incluso si fallan las demás medidas de seguridad, los datos esenciales sigan sin poderse aprovechar. Este enfoque cumple además con los requisitos de la norma PCI y del RGPD con respecto a datos no sensibles en componentes esenciales de la empresa.
Además, los datos tokenizados están protegidos frente a una exposición accidental a miembros del personal y proveedores externos no autorizados, ya que solo se puede acceder a ellos con una autorización pertinente. Esto ayuda a reducir la dependencia en controles compensatorios como medida temporal para superar auditorías de seguridad y cumple los requisitos de la PCI y el RGPD acerca de que los datos sensibles solo sean accesibles cuando sea necesario.

> *Los pagos digitales representan un mercado en constante crecimiento, de ahí la necesidad de prestar cada vez más atención a la seguridad de los datos. Mercury se esfuerza por permanecer a la vanguardia en este aspecto, por lo que hemos añadido otra capa de seguridad para proteger los datos de nuestros clientes. Esto nos brindará un impulso aún mayor a la hora de proporcionar servicios fiables de forma segura.*
>
> *– Jasna Fumagalli, director de cumplimiento, seguridad y gestión de riesgos de MPSI*

Protección de datos con un impacto mínimo
Mercury procesa una media de 1,5 millones de transacciones al día, por lo que necesitaba una solución que pudiese implementarse sin interrumpir su actividad y que no afectase al nivel de servicio. La tokenización ofrece protección sin los inconvenientes de rendimiento del cifrado clásico, preservando el formato y la utilidad de los datos protegidos de manera que los análisis y las aplicaciones empresariales puedan funcionar con tokens en lugar de datos sensibles sin encriptar.

Además, SecurDPS es altamente flexible y escalable, por lo que pudo implementarse sin hacer cambios en el código fuente. Esto supuso que la solución no solo pudiese ponerse en marcha en cuestión de semanas, sino que también se hizo sin que el nivel de servicio se viese afectado.

> *Estamos muy satisfechos con la disposición de comforte de gestionar cualquier solicitud que teníamos independientemente del lugar y la forma en que se plantearan. Su dedicación y diligencia fueron esenciales para el éxito de este proyecto.*
>
> *– Giovanni Cetrangolo, jefe de proyectos estratégicos e innovación de Mercury Processing Services International*

OBJETIVOS DEL PROYECTO

- Cumplir los principales requisitos en materia de seguridad de los datos del RGPD y de la PCI DSS
- Reducir el riesgo y el posible impacto de filtraciones de datos
- Proteger los datos sensibles para permitir una transferencia segura entre el personal y los socios
- Mantener el nivel de servicio

VENTAJAS

Las ventajas de este proyecto van más allá de cumplir los requisitos de la PCI y el RGPD sobre protección de datos. En el improbable caso de filtración de datos, todos los datos sensibles serán ilegibles y no serán aprovechables para los hackers, lo que reduce en gran medida el impacto de una posible filtración.

Además, los datos tokenizados ayudarán a proteger el crecimiento de Mercury, ya que ahora pueden intercambiar datos de forma mucho más fácil con socios y clientes, a la vez que mantienen los datos sensibles protegidos. Dado que ya no tienen que depender de controles compensatorios y pueden llevar a cabo su actividad de forma mucho más rápida, podrán sacar el máximo partido de un mercado en franca expansión y proporcionar servicios a más clientes que nunca.

> *En comforte nos enorgullecemos de nuestro historial de casos de éxito al proporcionar soluciones sólidas y fiables de seguridad de los datos a entidades financieras. Nos complace enormemente ayudar a Mercury a proteger sus datos y, en definitiva, a proteger su crecimiento.*
>
> *– Michael Deissner, director general de comforte*