CASO DE ESTUDIO

GRAN BANCO INDIO IMPLEMENTA MEDIDAS DE SEGURIDAD CENTRADAS EN LOS DATOS Y CUMPLE LA NORMA PCI DSS

Uno de los mayores bancos de la India que presta servicio a cientos de millones de clientes en miles de sucursales ha implementado medidas de seguridad centradas en los datos. La empresa trabaja fundamentalmente con números de tarjeta (PAN), así como con otros tipos de datos personales para realizar sus operaciones financieras y para fines organizativos. Gran parte de esta información es considerada «sensible» conforme a la PCI DSS y requiere medidas adecuadas de protección de los datos. Sin ellas, esta importante empresa financiera corría riesgo de incumplimiento que podría haber provocado una serie de consecuencias financieras y legales.

DESAFÍOS

Con más de 100 millones de clientes, esta empresa financiera trabaja para ofrecer el mejor servicio posible a sus usuarios. Sin embargo, se enfrenta al desafío de comprender las tendencias, los patrones y los puntos de vista de su diversa clientela. Para superarlo, es fundamental un análisis de los clientes y así obtener información para la toma de decisiones comerciales estratégicas. Pero el banco se encontró con el problema de que muchos de los datos usados para el análisis (PAN, nombres de los clientes o caracteres de la pista 2) se consideraban «sensibles» en virtud de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), las cuales son impuestas por el Banco de la Reserva de la India a todas las entidades financieras.

La empresa financiera opera con distintos entornos de datos que entran dentro del ámbito PCI. BASE24, con la tecnología de ACI Worldwide, es una popular pasarela de pagos que el banco emplea para el procesamiento de transacciones en línea. Además, esta empresa también usa Golden Gate, una solución de replicación de datos creada por Oracle, para su entorno de producción. Para estas aplicaciones, el Banco de la Reserva de la India exige que cumplan con los requisitos PCI DSS los archivos de registro de las transacciones, los archivos de registro de las transacciones de PDV, los archivos de registro de la interfaz del host, los archivos de autorización de clientes, los archivos de almacenamiento y envío de la interfaz del host y los archivos de registro de los cajeros. Sin embargo, el principal problema era que la empresa usaba sistemas de archivo que contenían números de cuentas principales, números de tarjeta y otra información financiera con datos de identificación bancaria que planteaba dificultades para cumplir con la normativa.

«Trabajar con comforte y la implementación de su solución de seguridad de los datos nos ayudó a potenciar nuestra organización. Gracias a la tokenización pudimos mejorar nuestro enfoque de seguridad y solventar los obstáculos para el cumplimiento de la PCI. De cara al futuro, nuestra organización dispone de una buena tecnología de protección para gestionar de forma efectiva la información sensible e impulsar nuestras iniciativas de seguridad» - Director general de importante banco indio del sector público.

OBJETIVOS DE LA EMPRESA

- Lograr la certificación PCI
- Proteger los datos de titulares de tarjeta
- Mejorar las medidas de seguridad

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 comforte.com/contact

SOLUCIONES

Para superar los obstáculos con los datos sensibles, esta empresa financiera necesitaba una solución de seguridad de los datos con funciones como una tokenización que preservase el formato, la compatibilidad con archivos remotos, la gestión integral de claves, el control y la auditoría pormenorizados y la interacción fluida con soluciones de recuperación ante catástrofes a fin de proteger de la mejor manera posible la información personal y así lograr la certificación PCI. Por ello se decantó por SecurDPS NonStop de comforte para hacer frente a este desafío. Comforte fue capaz de lograr la integración de forma transparente en su aplicación BASE24 sin necesidad de cambios en el código fuente, completándose la implementación en un plazo de 2 meses sin que las operaciones estratégicas se viesen afectadas. Gracias a este método, comforte pudo tokenizar todos los PAN, nombres de clientes, caracteres de pista 2 y otros datos sensibles, lo cual ayudó a mitigar los riesgos de incumplimiento. Además, esto permitió a los responsables de los procesos basados en datos y de la toma de decisiones seguir con sus operaciones de manera habitual.

VENTAJAS

Gracias a la implementación de SecurDPS NonStop, este banco logró mejoras sustanciales en su sistema HPE NonStop mediante la tokenización de datos sensibles. Al lograr la certificación PCI pudieron evitar sanciones financieras de hasta 500 000 $ por incidente y otras pérdidas por fraude con números de tarjeta en caso de ataque o filtración de datos. Con la consolidación de la confianza de sus clientes a través de la protección de la información personal, la empresa financiera también refuerza sus pilares para lograr un crecimiento y una expansión constantes. De cara al futuro, la empresa puede proteger adecuadamente los números de tarjeta, los nombres de clientes, los caracteres de pista 2 y otros datos sensibles que surjan en sus aplicaciones BASE24 y Golden Gate, a la vez que cumple las exigencias de cumplimiento.

> *Trabajar con comforte y la implementación de su solución de seguridad de los datos nos ayudó a potenciar nuestra organización. Gracias a la tokenización pudimos mejorar nuestro enf*oque de seguridad y solventar los obstáculos para el cumpl*imiento de la PCI. De cara al futuro, nuestra organización dispone de una buena tecnología de protección para gestionar de forma efectiva la información sensible e impulsar nuestras iniciativas de seguridad.*
>
> *Director general de importante banco indio del sector público*