comforte

CASO DE ESTUDIO

UNO DE LOS MÁS GRANDES MINORISTAS DE LA MODA EN MUNDO ELIGE LA TOKENIZACIÓN

El cifrado es un método eficaz y seguro para proteger los datos, especialmente los que se encuentran en reposo. En entornos de pago de gran volumen, en tiempo real, la tokenización es el método de protección de datos elegido por muchos de los principales minoristas, bancos y compañías de tarjetas de crédito de todo el mundo, porque ofrece protección de primera línea con un impacto mínimo en la velocidad de procesamiento. Un minorista de la moda de alto perfil eligió la solución de tokenización de Comforte fácil de implementar para agregar una capa adicional de protección a su red de pagos, mientras mantiene el alto nivel de servicio que esperan sus clientes.

PERFIL DEL CLIENTE

En la mayoría de las tiendas minoristas, cada vez que un cliente usa una tarjeta de pago, los detalles de la transacción se almacenan en un sistema informático central para facilitar el intercambio de dinero por los artículos vendidos. A menos que el minorista subcontrate el procesamiento de pagos a un proveedor de servicios, el almacenamiento de los detalles de la transacción se consideraran una operación comercial normal.

Este importante minorista de moda en los EE. UU. no es la excepción. Con cerca de 900 tiendas en América del Norte, el aceptar tarjetas de pago ha sido durante mucho tiempo un elemento básico como parte de la experiencia de sus clientes: la empresa ha aceptado pagos de las principales marcas de tarjetas (Visa, MasterCard, Amex y Discover) además de tener su propia tarjeta de crédito de marca privada por más de 30 años.

RETOS

Los detalles de las transacciones que son almacenados contienen datos de la tarjeta de pago junto con otra información de identificación personal, que son un objetivo muy atractivo para los hackers y otros delincuentes que buscan robar datos valiosos. En la dark web y en sitios web clandestinos, los detalles de las tarjetas de crédito y débito robadas se venden por grandes sumas de dinero y se utilizan para comprar artículos ilegales y se explotan para otros fines delictivos. Esta es la razón por la cual los hackers intentan incesantemente infiltrarse y extraer datos valiosos de empresas de todos tamaños y de todas las industrias. La violación y filtración de datos se ha convertido prácticamente en un hecho de la vida y, tarde o temprano, la mayoría de las empresas lo experimentarán al menos una vez. A pesar de su fuerte postura de seguridad de datos, esta empresa minorista altamente reconocida y confiable finalmente fue atacada e infiltrada, lo que llevó a su equipo de seguridad de datos a tomar medidas inmediatas y agregar una capa adicional de protección que evitaría violaciones similares y potencialmente mayores en el futuro. A la luz de los acontecimientos recientes, estas medidas de seguridad adicionales fueron rápidamente aprobadas por el consejo directivo.

Como parte de su programa de seguridad de datos existente, el minorista ya utilizaba cifrado para proteger los números de las tarjetas de pago, así como un número de identificación interno único asociado con cada tarjeta de pago. Uno de los desafíos que enfrentaron fue la de extender la protección para que incluyera información personal como nombres, direcciones, fechas de nacimiento, etc. de sus valiosos clientes. Si bien los números de tarjetas de pago son un objetivo obvio, los delincuentes siempre buscan nuevas formas de extraer valor de cualquier tipo de datos a los que logran acceder. Por lo tanto, la nueva solución, tenía que simplificar el proceso de escalamiento y extender la protección a formas adicionales de datos según lo requieran las nuevas situaciones y las circunstancias cambiantes.

DATOS RELEVANTES

- La protección de datos se extendió más allá de los PAN (números de cuenta principales) para incluir datos personales
- Alto nivel de seguridad como con el cifrado, pero ahora con una carga reducida en los recursos de TI
- Auditorías de PCI más rápidas al sacar datos confidenciales del alcance
- La gestión de llaves de cifrado ya no es necesaria para los datos tokenizados
- La tokenización se adaptó fácilmente a los sistemas de seguridad de datos existentes
- Las herramientas escalables de protección de datos facilitarán el cumplimiento normativo cruzado

ASEGURE SU CRECIMIENTO CON COMFORTE

Con más de 20 años de experiencia en protección de datos en sistemas verdaderamente críticos, Comforte es el socio perfecto para las empresas que desean proteger su activo más valioso: los datos. La suite de protección de datos de Comforte, SecurDPS, se ha creado desde cero para abordar mejor la seguridad de los datos en un mundo impulsado por las innovaciones comerciales digitales, clientes empoderados e interrupciones tecnológicas continuas.

Estamos aquí para ayudarlo a asegurar su crecimiento brindando experiencia, un conjunto de tecnología innovadora y soporte local.

Para obtener más información, comuníquese hoy mismo con un representante de Comforte visitando: **www.comforte.com/contact.**

> *Estuvimos encantados de trabajar con comforte para expandir nuestros sistemas de protección de datos. Su equipo de profesionales dedicados, realmente se tomó el tiempo para entender completamente nuestros requerimientos y siempre estuvieron dispuestos a dar el extra para que este proyecto se hiciera correctamente. Su apoyo continuo será un activo invaluable a futuro.*
>
> *– CISO, un Importante Minorista de la Moda*

Además, el minorista tiene un volumen de transacciones muy alto que se ejecuta en una infraestructura de nube híbrida. Esto significa que la activación del cifrado para todos los datos de los clientes en su entorno complejo habría agregado una demanda mayor a sus sistemas. El cifrado es excelente para proteger los datos en reposo; sin embargo, para poder utilizar los datos para los procesos comerciales estándar, es necesario que el descifrado se produzca en determinadas etapas. Los procesos de cifrado y descifrado consumen potencia informática adicional y pueden afectar la velocidad y el rendimiento de las transacciones. Durante las horas pico cuando los clientes visitan sus tiendas, su volumen de transacciones puede llegar a más de 800 transacciones por segundo colectivamente desde todos los dispositivos POS (Punto de Venta) en las tiendas, así como también las transacciones en línea. Lo último que quería hacer este minorista era arriesgarse a retrasar las autorizaciones en su punto de venta, ya que esto podría perjudicar su servicio al cliente de renombre mundial.

El cifrado y el descifrado también aumentan las operaciones de TI, específicamente la gestión de llaves de cifrado. Como práctica común en el procesamiento de cifrado, las responsabilidades de la gestión de llaves de cifrado requieren actualizar y reemplazar las llaves de cifrado cada cierto tiempo (también llamadas llaves rotativas), para reducir la posibilidad de exposición de datos en caso de pérdida o robo de las llaves de cifrado. El minorista espera que sus volúmenes crezcan año tras año; por lo tanto, era natural que esperaran que sus operaciones y la funcionalidad de la gestión de llaves también crezcan. Para poner este esfuerzo en perspectiva, según el volumen anual de este minorista, rotar las llaves de cifrado en un billón de tarjetas de pago cada año no era una tarea que quisieran continuar.

SOLUCIÓN

Tokenización

El minorista eligió la tokenización para proteger los datos confidenciales en toda su empresa. La tokenización reemplaza los elementos sensibles de los datos confidenciales con un valor sustituto sin valor explotable, también conocido como token. Se diferencia del cifrado clásico en que no requiere llaves de cifrado ni gestión de llaves. Esto hace que la tokenización sea un método de protección de datos ideal para empresas que están en crecimiento y que manejan grandes volúmenes de transacciones, porque, sin la necesidad de una gestión de llaves, hay menos riesgo de exposición de datos confidenciales y un menor impacto operativo, ya que no es necesario planificar ni financiar la gestión de llaves de cifrado.

Preservación del Formato

Otro requisito importante era que cuando los datos confidenciales estuvieran protegidos, deberían de permanecer en el mismo formato para que el minorista aún pueda usarlos en toda su empresa y recibir los mismos resultados. Por ejemplo, la tokenización reemplaza un número de tarjeta de crédito de 16 dígitos con un token de 16 dígitos, que se puede utilizar para procesar un pago sin tener que exponer el número original de 16 dígitos en ningún paso del proceso. El mismo principio se puede aplicar a otras formas de datos confidenciales, como nombres, fechas de nacimiento, números de teléfono, etc. Esto permite que el minorista mantenga la usabilidad de los datos a lo largo del ciclo de vida de cada cliente, a través de sus aplicaciones y servicios, y proporciona una capa adicional de seguridad para evitar incidentes de exposición de datos e infracciones.

Prueba de Concepto

El minorista realizó un proyecto de prueba de concepto (POC) con la solución de tokenización de comforte y quedó muy satisfecho con los resultados, ya que pudo cumplir con todos sus requisitos en términos de velocidad, seguridad y preservación de formato.

> *En comforte, nuestra misión es brindar soluciones para proteger los datos que se les han confiado a las empresas. Estamos muy emocionados de continuar con esa misión, agregando la tokenización al cinturón de herramientas de seguridad de la información de este importante minorista y ayudando a mantener seguros los datos de sus clientes leales.*
>
> *– Michael Deissner, Director General de comforte AG*

BENEFICIOS

La tokenización es reconocida por el PCI Security Standards Council (Consejo de Normas de Seguridad PCI) como un enfoque sólido para la protección de datos del titular de la tarjeta. La nueva tokenización ha permitido al minorista cumplir con PCI DSS, pero ahora a un costo mucho menor.

Reducción del alcance de la auditoría PCI

Dos beneficios adicionales resultaron del cambio a la tokenización como método de protección de datos.
En primer lugar, el minorista puede reducir el alcance de las auditorías de seguridad a las que se somete cada año. Por lo general, las auditorías de seguridad para el cumplimiento de PCI DSS requieren que la auditoría incluya todos los sistemas que contienen los datos originales del titular de la tarjeta de pago. Dado que el proceso de tokenización reemplaza los datos originales con un token, la mayoría de los sistemas pueden quedar fuera del alcance de la auditoría de seguridad, ya que los datos originales ya no existen. De hecho, tiendas enteras podrían quedar fuera del alcance, lo que redujo en gran medida el tiempo y el costo de las auditorías.

Cumplimiento normativo cruzado

Además, la tokenización posiciona al minorista para estar listo para responder a otras leyes de privacidad de datos que rodean el procesamiento de información de identificación personal (PII). En los EE. UU., cada estado ha promulgado - o publicará - leyes de privacidad de datos que protegen los datos de los clientes. En función de cómo el minorista utilice los datos personales de sus clientes, puede estar sujeto a leyes de privacidad de datos adicionales en el futuro con diferentes requisitos. La tokenización cumple el acto de reemplazar datos confidenciales con valores sustitutos y, si existieran nuevas leyes de privacidad de datos que el minorista debiera de cumplir en el futuro, extender la protección a datos adicionales seria solo cuestión de hacer un llamado a la API.