INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Preparación de las instituciones financieras para cumplir la norma PCI DSS con Akamai

La norma PCI DSS v4.0 introduce los cambios más importantes en los estándares de seguridad del sector de las tarjetas de pago (PCI) desde 2004 y las instituciones financieras deben adaptarse rápidamente a ella para garantizar su cumplimiento. En este marco integral que establece el Consejo sobre Normas de Seguridad PCI, se recogen medidas rigurosas para proteger los datos de los titulares de tarjetas. Las soluciones de Akamai capacitan a las instituciones financieras para que cumplan estos requisitos en constante evolución mediante funciones de seguridad avanzadas, supervisión continua y pruebas de penetración sólidas. Nuestras herramientas están diseñadas para agilizar el cumplimiento, proteger la información de los clientes y ayudar a su institución a estar preparada para adoptar esta nueva norma antes de marzo de 2025, la fecha límite.

Cumplimiento sencillo de PCI DSS con un solo proveedor

Las instituciones financieras no solo tienen que formar a sus empleados y aplicar políticas corporativas para cumplir con la norma PCI DSS, sino que también necesitan un software de seguridad sofisticado para satisfacer la mayoría de los requisitos. Dada su enorme variedad, a menudo es necesario trabajar con distintos proveedores. Algunas situaciones podrían exigir un firewall y, otras, la gestión de identidades. Las instituciones que den con un único proveedor con tecnología integrada se beneficiarán de un proceso de auditoría más sencillo y de una mayor seguridad para la información financiera de sus clientes. Adoptar soluciones de ciberseguridad sólidas que cumplan con estos requisitos como parte de una estrategia de seguridad más amplia puede reducir los costes y la complejidad a largo plazo. La cartera de soluciones de Akamai aborda de forma exhaustiva los requerimientos actuales y futuros de PCI DSS para que la experiencia de las instituciones financieras sea perfecta.

Gestión del ámbito

Un reto importante para las instituciones financieras que desean cumplir con PCI DSS es la cuestión del ámbito de aplicación. Determinar qué aplicaciones y entornos de red se consideran "dentro del alcance" de PCI puede ser complejo, ya que se incluyen distintos tipos de infraestructura, tecnología y ubicaciones. A medida que estas instituciones van adoptando la infraestructura de nube y las aplicaciones basadas en el software como servicio (SaaS), este entorno híbrido de servicios en local y bajo demanda agrega una capa adicional de complejidad. Estas empresas, incluidas las de comercio electrónico de ampliación automática, pueden tener serias dificultades para ubicar una carga de trabajo concreta en un momento determinado.

Las instituciones financieras han recurrido a los firewalls internos, las redes de área local virtual (VLAN) y las listas de control de acceso para abordar el problema del ámbito de aplicación. Sin embargo, estas aplicaciones heredadas suelen tener problemas para adaptarse a los entornos híbridos, lo que plantea un mayor nivel de complejidad, tiempo de inactividad y sobrecarga operativa, además de introducir posibles brechas de seguridad.

Ventajas

- **Optimización de los flujos de trabajo de seguridad y cumplimiento**
- **Reducción del volumen de las auditorías con capacidades diseñadas específicamente para PCI**
- **Recepción y registro de alertas útiles relacionadas con el cumplimiento de PCI**
- **Protección de datos financieros confidenciales**
- **Aumento de la eficiencia operativa y reducción de los costes del cumplimiento**

Akamai Guardicore Segmentation ofrece visibilidad del entorno de datos del titular de la tarjeta y de sus límites, un paso fundamental en el proceso de cumplimiento. Esta visibilidad ayuda a las instituciones financieras a cumplir los múltiples requisitos de la norma PCI DSS y proporciona una supervisión completa de sus redes. Por ejemplo:

- El requisito 1.2.3 exige que las organizaciones tengan un diagrama de su red. En el panel de Akamai Guardicore Segmentation, se muestran todos los enlaces entre el entorno de datos del titular de la tarjeta y las demás redes, lo que ayuda a las instituciones financieras a cumplir este requisito.
- El requisito 1.2.4 obliga a las organizaciones a mantener un diagrama de flujo de datos en el que se muestre cómo se mueven los datos de las cuentas entre los distintos sistemas y redes. El panel de Akamai Guardicore Segmentation ayuda a las instituciones financieras a satisfacer este requisito al exponer las conexiones necesarias.

Gestión de los controles

- En el requisito 1.2.5, se especifica la necesidad de identificar, aprobar y contar con una justificación comercial clara para todos los servicios, protocolos y puertos permitidos. Akamai Guardicore Segmentation ayuda a las instituciones financieras a cumplir este requisito mediante la implementación de políticas que se aplican de forma universal y que determinan los protocolos o servicios permitidos y no permitidos.

Gestión de la protección en el lado del cliente

Las instituciones financieras que aceptan datos de tarjetas de pago no son solo responsables de sus propios entornos. Aunque el uso de JavaScript en el desarrollo web moderno ha supuesto innovación y coherencia, también ha acarreado problemas para los procesadores de tarjetas de pago. Estas instituciones tienen enormes dificultades para supervisar y gestionar JavaScript debido a su ejecución descentralizada en el lado del cliente y las dependencias de terceros. Los atacantes han explotado este punto ciego mediante la inyección de código nocivo en los sitios web del lado del cliente para robar datos confidenciales. La popularidad de estos tipos de ataques, incluidos el robo de información web, el formjacking y los de tipo Magecart, ha crecido, lo que ha dado lugar a nuevos requisitos relacionados con la protección en el lado del cliente y la supervisión de scripts.

PCI DSS v4.0 requerirá que las instituciones financieras realicen un seguimiento e inventario, y justifiquen todo el código JavaScript que se ejecute en las páginas de pago de su sitio web público. Según el requisito 6.4.3, deberán garantizar la integridad del comportamiento y la autorización de todos los scripts, así como proporcionar un inventario de estos scripts con una justificación por escrito de su necesidad concreta. Además, en virtud del requisito 11.6.1, estas instituciones deben detectar y responder a cualquier cambio no autorizado que se realice en sus páginas de pago. El navegador del consumidor debe alertar al personal autorizado sobre cualquier modificación, incluidos los indicadores de compromiso, cambios, adiciones o eliminaciones, en los encabezados HTTP y en el contenido de la página de pago.

> Gracias a Akamai Guardicore Segmentation hemos reducido significativamente nuestra superficie de ataque sin los costes ni retrasos asociados con la actualización de firewalls heredados.
>
> **– Dave Wigley,**
> **CISO de Daiwa Capital Markets Europe**

Resumen de los requisitos de PCI DSS v4.0 para las instituciones financieras

- Mantener un inventario y una justificación de cada uno de los scripts que se ejecutan en las páginas de pago.
- Asegurarse de que todos los scripts están autorizados y de que realizan las acciones para las que están pensados.
- Establecer mecanismos de detección, alerta y respuesta para abordar los cambios no autorizados en los scripts, la protección para evitar la manipulación y la exfiltración de datos en las páginas de pago.

Akamai Client-Side Protection & Compliance proporciona una amplia asistencia para ayudar a las instituciones financieras a cumplir los requisitos 6.4.3 y 11.6.1 del estándar PCI DSS v4.0. Realiza un seguimiento e inventario de todos los scripts de las páginas de pagos, mejorando su integridad y autorización. Los equipos de seguridad pueden justificar fácilmente la finalidad de los scripts que se ejecutan en las páginas de pago, con justificaciones predefinidas y reglas automatizadas. La solución también supervisa los cambios en los encabezados HTTP y en la protección de las páginas de pago para evitar una posible manipulación. Un completo panel y alertas específicas de PCI facilitan la respuesta rápida a eventos relacionados con el cumplimiento y proporcionan pruebas para auditoría.

Protección contra ataques

La protección de los datos del titular de la tarjeta es un principio fundamental de la norma PCI DSS, pero a medida que proliferan los ataques contra las API y aplicaciones web, también pueden convertirse en puntos de entrada para los atacantes. Para cumplir con la norma PCI DSS, las instituciones financieras necesitan contar con protecciones eficaces contra el malware, los ataques de día cero y otras actividades que puedan provocar filtraciones de datos.

El módulo de protección contra el malware de Akamai App & API Protector las ayuda a protegerse contra la filtración de los datos de las tarjetas de pago al analizar los archivos en el Edge de la red antes de que entren y comiencen a propagar el malware. Asimismo, las API pueden introducir nuevas vulnerabilidades que los atacantes que buscan datos de tarjetas de pago intentarán aprovechar. Muchas instituciones financieras ni siquiera saben cuántas API tienen, y mucho menos garantizan que estas sean seguras. Cualquier API que reciba o transmita datos del titular de una tarjeta entra dentro del ámbito de aplicación de la norma PCI DSS, por lo que estas instituciones deben supervisar el desarrollo y la autenticación de las API, así como protegerlas.

Akamai API Security automatiza la detección continua de API en todo su entorno. Asigna una puntuación de riesgo a la API y al terminal mediante la comparación de las API con la documentación existente y la notificación de los errores de configuración y de las vulnerabilidades a los equipos de seguridad, desarrollo y API. Esta automatización continua significa que las vulnerabilidades se evalúan cuando termina de actualizar su entorno de API.

Conclusión

Aunque el objetivo final de la implementación de los controles de PCI DSS es proteger los datos del titular de la tarjeta y, por tanto, a sus clientes y a su empresa, las instituciones financieras siguen teniendo que atender a las peticiones de los auditores. Por lo tanto, trabajar con un solo proveedor ofrece ventajas obvias. Al poder consultar vistas tanto en tiempo real como históricas de la red, podrá cumplir con muchos de los requisitos de auditoría de forma más rápida y sencilla. Además, al trabajar con un solo proveedor de liderazgo demostrado en el sector y con una base estable de clientes que han conseguido cumplir con los requisitos de PCI DSS, las implementaciones serán más fluidas, los procesos de auditoría más rápidos y dispondrá de asistencia constante para lograr el cumplimiento. La visibilidad completa y las soluciones integradas de Akamai ayudan a las instituciones financieras a optimizar las iniciativas de cumplimiento y a reforzar sus defensas ante unas amenazas en constante evolución.

Para obtener más información, visite akamai.com o póngase en contacto con su equipo de ventas de Akamai.