DESCRIZIONE DELLA SOLUZIONE AKAMAI

Preparazione delle istituzioni finanziarie per la conformità al PCI DSS con Akamai

Poiché il PCI DSS v4.0 apporta i cambiamenti più significativi agli standard di sicurezza nel settore delle carte di pagamento dal 2004, le istituzioni finanziarie devono adattarsi tempestivamente per rimanere conformi. Questo sistema completo, stabilito dal PCI Security Standards Council, impone misure rigorose per la proteggere i dati dei titolari di carte di credito. Le soluzioni di Akamai consentono alle istituzioni finanziarie di soddisfare questi requisiti in continua evoluzione tramite avanzate funzioni di sicurezza, un monitoraggio continuo e solidi test di penetrazione. I nostri strumenti sono progettati per semplificare il processo di conformità, salvaguardare le informazioni sui clienti e aiutare le istituzioni a prepararsi entro marzo 2025, come previsto dal PCI.

Conformità unificata: semplificare il processo del PCI DSS con un unico provider

Sebbene la conformità al PCI DSS comprenda la formazione dei dipendenti e le policy aziendali, le istituzioni finanziarie devono fare affidamento su sofisticati software di sicurezza per soddisfare la maggior parte dei requisiti, che, vista la loro natura onnicomprensiva, spesso implicano la necessità di collaborare con più provider. Alcuni requisiti possono richiedere un firewall, mentre altri riguardano la gestione delle identità. Le istituzioni finanziarie che riescono a trovare un unico provider con strumenti tecnologici integrati possono trarre vantaggio non solo da un processo di audit più semplice, ma anche da una maggiore sicurezza per le informazioni finanziarie dei propri clienti. L'adozione di solide soluzioni per la cybersicurezza in grado di soddisfare i requisiti richiesti come parte di una strategia di sicurezza più ampia può ridurre costi e problemi nel lungo termine. Akamai dispone di una gamma di soluzioni in grado di soddisfare pienamente i requisiti del PCI DSS esistenti e futuri, offrendo un'eccellente experience alle istituzioni finanziarie.

Vantaggi

- **Semplificazione dei workflow di sicurezza e conformità**
- **Riduzione dell'onere degli audit con funzionalità PCI dedicate**
- **Ricezione e registrazione di avvisi utili sulla conformità al PCI**
- **Protezione dei dati finanziari sensibili**
- **Miglioramento dell'efficienza operativa e riduzione dei costi legati al processo di conformità**

Definizione dell'ambito

Una sfida significativa per le istituzioni finanziarie che cercano di soddisfare i requisiti del PCI DSS è la questione dell'ambito. Le applicazioni e gli ambienti di rete considerati "nell'ambito" dalle normative PCI possono risultare piuttosto complessi ed estendersi su diversi tipi di infrastrutture, tecnologie e posizioni. Poiché le istituzioni finanziarie hanno adottato l'infrastruttura cloud e le applicazioni basate sul modello SaaS, questo ambiente ibrido costituito da servizi on-premise e on-demand aggiunge un ulteriore livello di complessità. Le istituzioni finanziarie, specialmente quelle con una scalabilità automatica delle attività di e-commerce, trovano particolarmente difficile sapere dove si trova un dato carico di lavoro in uno specifico momento.

Le istituzioni finanziarie hanno adottato firewall interni, VLAN ed elenchi di controllo degli accessi per risolvere la questione dell'ambito. Tuttavia, queste applicazioni tradizionali spesso non riescono a tenere il passo con gli ambienti ibridi, il che introduce un ulteriore livello di complessità, problemi di downtime e maggiori costi operativi, lasciando, nel contempo, falle nella sicurezza.

Akamai Guardicore Segmentation offre visibilità sull'ambiente dei dati dei titolari di carte di credito (CDE) e sui suoi confini: una fase cruciale nel processo di conformità. Questa visibilità aiuta le istituzioni finanziarie a soddisfare diversi requisiti del PCI DSS e offre una supervisione completa della loro rete, come ad esempio:

- Il requisito 1.2.3 richiede alle organizzazioni di stilare un diagramma delle loro reti. Il dashboard di Akamai Guardicore Segmentation visualizza tutti i collegamenti esistenti tra il CDE e le altre reti, aiutando le istituzioni finanziarie a soddisfare questo requisito.
- Il requisito 1.2.4 richiede alle organizzazioni di stilare un diagramma di flusso che illustra lo spostamento dei dati degli account tra sistemi e reti. Il dashboard di Akamai Guardicore Segmentation aiuta le istituzioni finanziarie a verificare questo requisito visualizzando i collegamenti necessari.

Definizione dei controlli

- Il requisito 1.2.5 specifica la necessità di identificare, approvare e giustificare chiaramente tutti i protocolli, le porte e i servizi consentiti. Akamai Guardicore Segmentation aiuta le istituzioni finanziarie a soddisfare questo requisito implementando le policy universalmente applicate al fine di stabilire quali protocolli o servizi siano consentiti o meno.

Definizione della protezione lato client

Le istituzioni finanziarie che accettano i dati delle carte di pagamento non sono solo responsabili dei loro ambienti. L'utilizzo di JavaScript nel moderno sviluppo web ha introdotto elementi di innovazione e coerenza, ma ha anche creato problemi per i responsabili del trattamento dei dati delle carte di pagamento. Grazie alla sua esecuzione lato client decentralizzata e alle dipendenze di terze parti, JavaScript risulta estremamente difficile da monitorare e da gestire per le istituzioni finanziarie. I criminali hanno sfruttato questo punto cieco per iniettare codice dannoso nei siti web lato client allo scopo di rubare dati sensibili. Questi tipi di attacchi, inclusi web skimming, formjacking e Magecart, sono diventati sempre più popolari fino ad arrivare ai nuovi requisiti relativi ai sistemi di protezione lato client e al monitoraggio degli script.

Il PCI DSS v4.0 richiede alle istituzioni finanziarie di monitorare, inventariare e giustificare tutto il codice JavaScript eseguito sulle pagine di pagamento del sito web rivolte al pubblico. Nell'ambito del requisito 6.4.3, le aziende devono assicurare l'integrità comportamentale e l'autorizzazione di tutti gli script, nonché fornire un inventario di questi script con una giustificazione scritta delle loro singole necessità. Inoltre, nell'ambito del requisito 11.6.1, le istituzioni finanziarie devono rilevare e rispondere ad eventuali modifiche non autorizzate che sono state apportate alle loro pagine di pagamento. Il personale autorizzato deve essere avvisato in caso di eventuali modifiche (inclusi indicatori di compromissione ed operazioni di modifica, aggiunta o eliminazione) apportate alle intestazioni HTTP e ai contenuti delle pagine di pagamento visualizzate sul browser del consumatore.

Con Akamai Guardicore Segmentation, abbiamo ridotto in maniera significativa la nostra superficie di attacco, senza i costi e i ritardi associati all'aggiornamento dei firewall preesistenti.

- Dave Wigley,
CISO, Daiwa Capital Markets Europe

Riepilogando, il PCI DSS v4.0 richiede alle istituzioni finanziarie di:

- Stilare un inventario e una giustificazione di ogni script eseguito sulle pagine di pagamento
- Assicurarsi che tutti gli script siano autorizzati e che eseguano le azioni per cui sono stati progettati
- Stabilire i meccanismi di rilevamento, invio di avvisi e risposta necessari per gestire le modifiche non autorizzate che sono state apportate agli script, la manomissione dei sistemi di protezione e l'esfiltrazione dei dati sulle pagine di pagamento

Akamai Client-Side Protection & Compliance fornisce un ampio supporto per aiutare le istituzioni finanziarie a soddisfare i requisiti 6.4.3 e 11.6.1 del PCI DSS v4.0. La soluzione monitora e cataloga automaticamente gli script presenti sulle pagine di pagamento, migliorandone l'integrità e autorizzandone l'uso. I team addetti alla sicurezza possono giustificare facilmente lo scopo degli script eseguiti sulle pagine di pagamento con giustificazioni predefinite e regole automatizzate. Inoltre, la soluzione monitora le modifiche apportate alle intestazioni HTTP e ai sistemi di protezione delle pagine di pagamento per evitarne la manomissione. Un dashboard completo e avvisi PCI dedicati consentono di rispondere in modo rapido e semplice agli eventi correlati alla conformità e forniscono prove a scopo di controllo.

Protezione contro gli attacchi

La protezione dei dati dei titolari di carte di credito è un principio fondamentale del PCI DSS, ma, poiché le app web e le API continuano a proliferare, possono diventare anche punti di ingresso per i criminali. Per conformarsi al PCI DSS, alle istituzioni finanziarie servono solidi sistemi di protezione da malware, attacchi zero-day e altre minacce che possono condurre alla fuga di dati.

Akamai App & API Protector con il modulo Malware Protection può aiutare le istituzioni finanziarie a proteggersi dalla fuga dei dati delle carte di pagamento mediante la scansione dei file sull'edge della rete prima che riescano a penetrare nel sistema e a diffondere il malware. Le API possono introdurre nuove vulnerabilità che i criminali alla ricerca dei dati delle carte di pagamento tentano di sfruttare. Molte istituzioni finanziarie non conoscono neanche tutte le loro API, figuriamoci se possono attestare che sono sicure. Le API che ricevono o trasmettono i dati dei titolari di carte di credito rientrano nell'ambito del PCI DSS, pertanto, le istituzioni finanziarie devono monitorare lo sviluppo e l'autenticazione delle API e proteggerle.

Akamai API Security individua automaticamente e continuamente le API presenti in un ambiente, quindi assegna alle API e agli endpoint un punteggio di rischio confrontando le API rispetto alla documentazione esistente e allertando i team addetti alla sicurezza, allo sviluppo e alle API circa la presenza di vulnerabilità e configurazioni errate. Questa continua automazione implica una valutazione delle vulnerabilità una volta finalizzati gli aggiornamenti del patrimonio delle API.

Conclusione

Anche se l'obiettivo finale dell'implementazione dei controlli richiesti dal PCI DSS è proteggere i dati dei titolari di carte di credito (e, pertanto, salvaguardare i clienti e le aziende), le istituzioni finanziarie devono comunque soddisfare i requisiti dei revisori, un'area in cui l'utilizzo di un solo provider offre notevoli vantaggi. Con le viste cronologiche e in tempo reale della rete, potete soddisfare molti requisiti degli audit più rapidamente e facilmente. Inoltre, collaborare con un solo provider che vanta una leadership consolidata nel settore (e clienti che hanno soddisfatto i requisiti del PCI DSS) può agevolare le implementazioni, velocizzare gli audit e fornire un supporto costante nei processi di conformità. La visibilità completa e le soluzioni integrate di Akamai aiutano le istituzioni finanziarie a semplificare i processi di conformità e a rafforzare le loro difese dalle minacce in continua evoluzione.

Per ulteriori informazioni, visitate il sito akamai.com o contattate il team di vendita di Akamai.