CHECKLIST AKAMAI

Checklist per la sicurezza PCI DSS v4.0 JavaScript con Akamai Client-Side Protection & Compliance

Il PCI DSS (Payment Card Industry Data Security Standard) è uno standard di sicurezza globale sviluppato per migliorare la sicurezza online dei dati delle carte di pagamento e per facilitare l'adozione di misure di sicurezza coerenti a livello globale. Si tratta di uno degli standard di sicurezza più importanti, la cui conformità è richiesta da parte di tutte le organizzazioni che elaborano i dati delle carte di pagamento online.

L'ultimo aggiornamento del PCI DSS (disponibile solo in inglese), la versione 4.0, che entrerà in vigore nel 2025, include 12 importanti requisiti per la sicurezza dei dati e linee guida aggiornate per gestire le nuove minacce alla cybersicurezza in continua evoluzione. I due importanti requisiti 6.4.3 e 11.6.1, aggiunti al PCI PCI v4.0, riguardano la sicurezza e la protezione JavaScript dagli attacchi di web skimming lato client che rubano i dati sensibili degli utenti finali dal browser. Questi attacchi sono cresciuti in popolarità nel corso degli anni e le loro tecniche sofisticate li hanno resi sempre più difficili da rilevare. Le loro conseguenze possono risultare devastanti per le organizzazioni prese di mira: sanzioni salate, danni in termini di reputazione del brand e fiducia dei clienti, perdita di profitti e così via.

Esaminiamo ora una checklist dei nuovi requisiti di sicurezza degli script previsti dal PCI DSS v4.0 e come Client-Side Protection & Compliance si distingue dalla concorrenza.

I requisiti del PCI DSS v4.0	Come Client-Side Protection & Compliance può aiutarvi
Requisito 6.4.3: proteggere le applicazioni web rivolte al pubblico dagli attacchi ☑ Dovete implementare un metodo per verificare l'avvenuta autorizzazione di ogni script caricato ed eseguito nel browser ☑ Dovete implementare un metodo per garantire l'integrità di ogni script caricato ed eseguito nel browser ☑ Dovete mantenere un inventario di tutti gli script caricati ed eseguiti nel browser con una giustificazione scritta sul motivo per cui ogni script è necessario	**Autorizzare con un solo clic** ☑ Gestite facilmente gli script autorizzati all'esecuzione sulle pagine di pagamento del vostro sito web direttamente dallo strumento **Garantire un'integrità tempestiva** ☑ La tecnologia comportamentale analizza ogni script eseguito nel browser per rilevare e inviare avvisi su eventuali attività dannose o tentativi di esfiltrazione dei dati **Monitorare e mantenere automaticamente un inventario di tutti gli script** ☑ La presenza di giustificazioni predefinite e regole automatizzate consente di giustificare facilmente tutti gli script caricati ed eseguiti nel browser

Akamai

I requisiti del PCI DSS v4.0	Come Client-Side Protection & Compliance può aiutarvi

Requisito 11.6.1: rilevare e intervenire riguardo alle modifiche non autorizzate sulle pagine di pagamento

Dovete implementare un meccanismo di rilevamento delle operazioni di modifica e manomissione in grado di:

- ☑ Avvisare il personale dedicato in caso di modifiche non autorizzate (inclusi indicatori di compromissione ed operazioni di modifica, aggiunta ed eliminazione) apportate alle intestazioni HTTP e ai contenuti delle pagine di pagamento visualizzate sul browser del consumatore
- ☑ Valutare l'intestazione HTTP e le pagine di pagamento visualizzate

Le funzioni del meccanismo vengono eseguite almeno una volta ogni sette giorni o periodicamente (alla frequenza definita nell'analisi dei rischi specifici dell'entità, in base a tutti gli elementi riportati nel requisito 12.3.1)

Mantenere protette le pagine di pagamento

- ☑ Monitorate, analizzate e mitigate i tentativi di manomissione delle pagine di pagamento per garantire la sicurezza dei dati sensibili dei vostri utenti finali

Esaminare le modifiche non autorizzate in tempo reale con avvisi utili e immediati

- ☑ Con un rilevamento immediato, i team addetti alla sicurezza possono rispondere rapidamente alle modifiche o ai cambiamenti non autorizzati apportati alle intestazioni HTTP sulle pagine di pagamento

Proteggere con una difesa always-on

- ☑ Una protezione 24 ore su 24 tutela le interazioni degli utenti sulle pagine di pagamento

Akamai Client-Side Protection & Compliance fornisce un solido sistema di protezione dalle minacce JavaScript e offre una visibilità completa sulla superficie degli attacchi lato client per proteggere i dati sensibili nel browser. Le sue funzionalità appositamente progettate per il PCI DSS v4.0 aiutano i team addetti alla sicurezza e alla conformità a semplificare il processo di controllo del PCI DSS v4.0 e forniscono workflow dedicati per aiutarvi ad ottemperare ai requisiti di sicurezza degli script 6.4.3 e 11.6.1.

Akamai Client-Side Protection & Compliance dispone di opzioni di implementazione flessibili e non richiede l'attivazione dell'Akamai Connected Cloud.

Scoprite ulteriori informazioni sul modo con cui queste funzionalità possono aiutare la vostra organizzazione a conformarsi al PCI DSS v4.0.

 | Supporto | | Pubblicato 09/23