Payments to grow your world

PCI Basics per esercenti e-commerce

WORLDLINE

Questa presentazione si applica agli esercenti che accettano pagamenti online.

Indice dei contenuti.

1. Cosa significa “e-commerce”?
2. Cosa deve fare ogni esercente?
3. Quali principi fondamentali degli standard si applicano a voi?

Maggiori informazioni sui singoli SAQ per gli esercenti di e-commerce.

4. SAQ A
5. SAQ A-EP
6. SAQ D

7. Quali sono i requisiti?
8. Scansione ASV (Approved Scanning Vendor), test di penetrazione, rilevamento/prevenzione delle intrusioni e monitoraggio dell’integrità dei file.
9. Dove posso trovare maggiori informazioni?

Cosa significa e-commerce?

In poche parole, è quando si ricevono i dati della carta per via elettronica.

- Il cliente interagisce con il vostro web shop.
- Il cliente usa un'applicazione mobile per inviare i dati ai sistemi da voi controllati.

Se avete esternalizzato le vostre piattaforme di e-commerce, siete comunque responsabili della conformità PCI.

- La parte terza a cui ci si rivolge potrebbe essere già conforme allo standard PCI.
- Se non sono conformi, tutto ciò che fanno è incluso nella valutazione.

Se avete un sito internet, potete gestirlo in molti modi.

- Voi controllate l'hardware e il sito internet.
- Vi rivolgete a un service provider per creare e gestire il vostro sito internet.
- Avete un web shop su uno dei tanti "marketplace".

I pagamenti possono essere elaborati in diversi modi.

- Il vostro sito internet elabora la transazione e poi invia i dettagli all'acquirer.
- Il vostro sito internet non memorizza i dati, ma li accetta e li invia all'acquirer per elaborarli.
- Il vostro sito internet non accetta direttamente i dati della carta; quando il cliente effettua un pagamento, il vostro sito reindirizza l'input all'acquirer per l'elaborazione. Il vostro sito non interagisce in alcun modo con i dati della carta.

Cosa deve fare ogni esercenti?

Se non siete conformi allo standard PCI, **potreste essere soggetti a sanzioni imposte dai brand di carte di credito** e noi **potremmo non essere più in grado di elaborare i pagamenti** per vostro conto, poiché non avete convalidato la vostra sicurezza in materia di pagamenti.

Lo standard PCI DSS comprende diverse centinaia di requisiti, dal momento che copre ogni possibile attività che rientra nel campo di applicazione della valutazione.

Per i requisiti che si applicano alla sua azienda è necessario un tasso di conformità del 100%.

Lo standard si applica a tutti, i singoli requisiti possono essere contrassegnati con la dicitura “Non applicabile” se vi sono motivi per applicarli, ma questo deve essere giustificato.

La valutazione annuale è una convalida della conformità, ma è necessario essere sempre conformi.

Le entità più grandi (che elaborano oltre 1 milione di transazioni all’anno) possono essere obbligate a far eseguire la valutazione annuale da un ISA o da un QSA.

Le entità più piccole possono essere in grado di autovalutarsi senza bisogno di un ISA o di un QSA.

Quali principi fondamentali degli standard si applicano a voi?

Per gli esercenti più piccoli, il Consiglio PCI ha creato una serie di questionari di autovalutazione (Self-Assessment Questionnaires, SAQs) che si rivolgono a modelli aziendali specifici.

Esistono due alternative per gli **esercenti con sistemi di e-commerce**:

1) **SAQ A:** Esercenti card-not-present (e-commerce o vendite per corrispondenza/telefono) che hanno completamente esternalizzato tutte le funzioni relative ai dati dei titolari di carta a service provider terzi convalidati PCI DSS, senza archiviazione, elaborazione o trasmissione elettronica dei dati dei titolari di carta nei sistemi o nei locali dell'esercente.

2) **SAQ A-EP:** Esercenti di e-commerce che affidano tutta l'elaborazione dei pagamenti a terze parti convalidate PCI DSS, che hanno un sito internet che non riceve direttamente i dati dei titolari di carta ma che può avere un riscontro sulla sicurezza delle operazioni di pagamento. Nessuna memorizzazione, elaborazione o trasmissione elettronica dei dati dei titolari di carta nei sistemi o nella sede dell'esercente.

Qualora nessuna di queste descrizioni descriva la situazione esatta, allora l'esercente dovrà utilizzare il SAQ D.

Maggiori informazioni sui singoli SAQ per gli esercenti di e-commerce.

SAQ A.

Se soddisfate i criteri per la compilazione di un SAQ A, allora la vostra attività è soggetta a quanto segue:

CRITERI PER LA SAQ A:

- Esercenti card-not-present (e-commerce o vendite per corrispondenza/telefono) che hanno completamente esternalizzato tutte le funzioni relative ai dati dei titolari di carta a service provider terzi convalidati PCI DSS, senza archiviazione, elaborazione o trasmissione elettronica dei dati dei titolari di carta nei sistemi o nei locali dell'esercente.
- Quando si raggiunge la fase di pagamento in una transazione, il vostro sito internet non esegue alcuna funzione, esso reindirizza il titolare della carta al vostro processore di pagamento o visualizza un iFrame del processore di pagamento e tutti i dati della transazione sono limitati a questo frame.

ESEMPI DI REQUISITI PER LA SAQ A:

- Nessuna memorizzazione elettronica dei dati della carta.
- I sistemi sono protetti e aggiornati.
- Gli script caricati ed eseguiti nel browser del titolare della carta durante la procedura di pagamento sono gestiti, controllati e autorizzati.
- Scansioni esterne di vulnerabilità ("ASV") condotte almeno ogni trimestre.
- I file critici sui sistemi dell'esercente vengono monitorati e vengono emessi avvisi e risposte in caso di modifiche.

Maggiori informazioni sui singoli SAQ per gli esercenti di e-commerce.

SAQ A-EP.

Se soddisfate i criteri per la compilazione di un SAQ A-EP, allora la vostra attività è soggetta a quanto segue:

CRITERI PER SAQ A-EP:

- Esercenti di e-commerce che affidano tutta l'elaborazione dei pagamenti a terze parti convalidate PCI DSS, che hanno un sito internet che non riceve direttamente i dati dei titolari di carta ma che può avere un riscontro sulla sicurezza delle operazioni di pagamento. Nessuna memorizzazione, elaborazione o trasmissione elettronica dei dati dei titolari di carta nei sistemi o nella sede dell'esercente.

- Il sito internet dell'esercente controlla la pagina di pagamento, ma il sito internet non esegue alcuna elaborazione; tutti i dati vengono inviati al processore di pagamento (ad esempio, direct POST).

ESEMPI DI REQUISITI PER SAQ A-EP:

- Nessuna memorizzazione elettronica dei dati della carta.
- I sistemi sono protetti e aggiornati.
- Laddove è necessario, viene implementato un sistema antivirus.
- Il software viene sviluppato e patchato in modo sicuro.
- Gli script caricati ed eseguiti nel browser del titolare della carta durante la procedura di pagamento sono gestiti, controllati e autorizzati.
- Dal 2024: è stato implementato un metodo tecnico per rilevare e prevenire gli attacchi basati sul Web.
- L'accesso ai sistemi è limitato e protetto.
- L'attività dell'utente e gli eventi del sistema vengono registrati e conservati.
- Scansioni esterne di vulnerabilità ("ASV") condotte almeno ogni trimestre.
- I test di penetrazione vengono eseguiti almeno una volta all'anno.
- I sistemi di rilevamento/prevenzione delle intrusioni sono implementati per avvisare e/o prevenire gli accessi non autorizzati.
- I file critici sui sistemi dell'esercente vengono monitorati e vengono emessi avvisi e risposte in caso di modifiche - File Integrity Monitoring ("FIM").

Maggiori informazioni sui singoli SAQ per gli esercenti di e-commerce.

SAQ D.

Se non soddisfate i criteri di tutti gli altri SAQ, allora il SAQ D e i seguenti si applicano alla vostra attività:

CRITERI PER IL SAQ D:

- Esercenti che non archiviano elettronicamente i dati del conto ma che non soddisfano i criteri di un altro tipo di SAQ.
- Esercenti con un sito che riceve transazioni in entrata attraverso canali elettronici, le elabora e poi inoltra i dati a un processore di pagamenti.
- Esercenti con più canali di accettazione dei pagamenti.
- Esercenti con archiviazione elettronica dei dati del conto.
- Nessun altro SAQ ammissibile.

IMPORTANTE PER SAQ D:

- Il SAQ D comprende la maggior parte dei requisiti e può richiedere l'assistenza di una risorsa interna o esterna per una valutazione adeguata.

Quali sono i requisiti?

Lo standard è strutturato in 12 sezioni, ognuna delle quali copre un aspetto specifico dei requisiti.

- Le dodici sezioni dello standard di seguito riportate rimangono sempre le stesse, ma ogni SAQ ha un numero predeterminato di requisiti.
- I singoli requisiti sono gli stessi indipendentemente dal modello di rendicontazione utilizzato, il Report on Compliance ("ROC") utilizzato dagli esercenti più grandi (che elaborano oltre 6 milioni di transazioni all'anno) li comprende tutti, il SAQ-D ne contiene la maggior parte, il SAQ-P2PE ne contiene pochissimi.

PRINCIPI FONDAMENTALI	SEZIONI DELLO STANDARD
Costruire e mantenere una rete e dei sistemi sicuri	1. Installare e mantenere i controlli di sicurezza della rete. 2. Applicare una configurazione sicura a tutti i componenti del sistema.
Proteggere i dati del conto	3. Proteggere i dati del conto memorizzati. 4. Proteggere i dati dei titolari di carta con una crittografia forte durante la trasmissione su reti pubbliche e aperte.
Mantenere un programma di gestione delle vulnerabilità	5. Proteggere tutti i sistemi e le reti da software nocivi. 6. Sviluppare e mantenere sistemi e software sicuri.
Implementare forti misure di controllo degli accessi	7. Limitare l'accesso ai componenti del sistema e ai dati dei titolari di carta in base al principio "Need to Know". 8. Identificare gli utenti e autenticare l'accesso ai componenti del sistema. 9. Limitare l'accesso fisico ai dati dei titolari di carta.
Monitorare e testare regolarmente le reti	10. Registrare e monitorare tutti gli accessi ai componenti del sistema e ai dati dei titolari di carta. 11. Testare regolarmente la sicurezza dei sistemi e delle reti.
Mantenere una politica di sicurezza delle informazioni	12. Supportare la sicurezza delle informazioni con politiche e programmi organizzativi.

1. I SAQ richiedono che l'esercente indichi se il requisito è in vigore o meno.
2. L'esercente "attesta" la propria conformità attraverso un AOC („Attestation of Compliance").
3. Se si utilizza un service provider per svolgere alcune delle funzioni che rientrano nel campo di applicazione della valutazione, è necessario ottenere una copia del suo AOC per dimostrarne la conformità, poiché non si può affermare di essere conformi se non lo si è.
4. L'attestato AOC è valido per un anno. È necessario completare (non iniziare) la valutazione di rinnovo entro la data di scadenza dell'ultima valutazione.
5. Alcune valutazioni richiedono una scansione delle vulnerabilità effettuata da un fornitore ASV che dovrebbe essere incaricato dalla ditta.
   - Le scansioni devono essere effettuate almeno ogni trimestre.
   - La fase finale di una scansione ASV è "l'attestazione" da parte vostra: se non lo fate, non avete completato la scansione.

Lo scopo principale di PCI è quello di proteggere i dati delle carte di credito. Si consiglia vivamente di implementare controlli di sicurezza simili per proteggere gli altri asset e sistemi aziendali.

Scansione ASV, test di penetrazione, rilevamento/prevenzione delle intrusioni e monitoraggio dell'integrità dei file.

Uno o più di questi elementi potrebbero essere richiesti per la valutazione, a seconda del modello di rendicontazione utilizzato. Si tratta di attività fondamentalmente diverse, come spiegato di seguito.

- **ASV:** Nell'ambito dei requisiti PCI DSS, qualsiasi entità con indirizzi IP rivolti al pubblico deve sottoporsi a una scansione di sicurezza almeno ogni trimestre, eseguita da un fornitore di scansioni ASV approvato. Per superare la scansione non possono esserci problemi di sicurezza (vulnerabilità) identificati dalla scansione che non siano stati risolti.
  Nota: NON si tratta di un test di penetrazione approfondito, ma semplicemente della ricerca di problemi noti di software e configurazione come controllo della sicurezza di base.

- **Test di penetrazione:** Un tester esperto esegue una scansione per identificare eventuali punti deboli nei sistemi, proprio come una scansione ASV, ma poi si spinge oltre e cerca di sfruttare tali vulnerabilità. Si tratta di un passo avanti rispetto alla scansione ASV, ma la scansione ASV è comunque necessaria.
  Nota: La scansione ASV deve essere eseguita da un fornitore approvato elencato sul sito internet del Consiglio PCI. I tester di penetrazione non sono elencati dal Consiglio PCI, ma devono essere qualificati ed esperti nelle attività.

- **Sistemi di rilevamento/prevenzione delle intrusioni ("IDS/IPS"):** Si tratta di sistemi all'interno dell'ambiente che monitorano il traffico di rete in modo simile al software antivirus che controlla programmi e dati. I sistemi sono in grado di identificare il traffico "cattivo" noto e di avvisare o bloccare a seconda dell'implementazione. Questi sistemi sono "sempre attivi" e devono essere continuamente aggiornati, per garantire che dispongano dei dati più recenti sulle minacce e siano in grado di identificare le attività dannose.

- **Monitoraggio dell'integrità dei file (File Integrity Monitoring "FIM"):** Monitora i file sul sistema e segnala se sono cambiati rispetto alla versione "buona" conosciuta. In questo modo si identifica qualsiasi modifica dannosa ai file critici dei vostri sistemi.

Dove posso trovare maggiori informazioni?

Tutti gli standard sono gestiti dal Consiglio per gli standard di sicurezza PCI.
Sito ufficiale del Consiglio per gli standard di sicurezza PCI.

Cosa si può trovare nel sito internet del Consiglio?

- Copie scaricabili della guida sui tipi di SAQ
- SAQ attuali
- Domande frequenti
- Guida per gli esercenti
- Elenchi di fornitori/prodotti che sono stati certificati secondo vari standard PCI: PTS, ASV, P2PE
- E altro ancora.

Una delle missioni di Worldline è quella di **garantire e supportare i nostri esercenti a essere conformi a PCI DSS** con i requisiti e i regolamenti degli schemi di carte di credito.

Grazie.

Worldline.
Payments to grow your world.