PCI Basics per esercenti con POS fisico

WORLDLINE

Questa presentazione si applica agli esercenti che accettano pagamenti con carta tramite POS fisico.

Indice dei contenuti.

Cosa significa POS fisico?

Non include:

- Le transazioni effettuate attraverso un sito web o un e-commerce “di proprietà” dell’esercente (anche se fornito da una terza parte), indipendentemente da chi inserisce il numero di carta.
- I pagamenti effettuati tramite un’applicazione mobile sul dispositivo del titolare della carta.

Include:

- Il titolare della carta presenta la carta o il suo telefono/orologio/tablet con wallet.
- Il pagamento viene elaborato tramite un dispositivo controllato dall’esercente, ad esempio un terminale di pagamento (indipendente, collegato a una piattaforma POS o a un telefono/tablet).
- Questo include i casi in cui l’esercente accetta il pagamento inserendo i dati della carta direttamente in una pagina web fornita dal proprio fornitore di servizi di pagamento, un “terminale virtuale” (di cui si parlerà più avanti).

Cosa deve fare ogni esercente?

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 dei 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.

I seguenti requisiti si applicano ai pagamenti con POS fisico:

- **SAQ B:** Esercenti che utilizzano solo macchine stampanti senza memorizzazione elettronica dei dati dei titolari di carta e/o terminali stand-alone, dial-out, senza memorizzazione elettronica dei dati dei titolari di carta.
- **SAQ B-IP:** Esercenti che utilizzano solo terminali di pagamento stand-alone, approvati dal PTS, con una connessione IP al processore di pagamento, senza memorizzazione elettronica dei dati dei titolari di carta.
- **SAQ C-VT:** Esercenti che inseriscono manualmente singole transazioni alla volta tramite tastiera con una soluzione di terminale virtuale basata su internet, fornita e ospitata da un service provider di terze parti convalidato PCI DSS. Nessuna memorizzazione elettronica dei dati dei titolari di carta.
- **SAQ C:** Esercenti con sistemi di applicazione di pagamento collegati a Internet, senza memorizzazione elettronica dei dati dei titolari di carta.
- **SAQ P2PE-HW:** Esercenti che utilizzano solo terminali di pagamento hardware inclusi e gestiti tramite una soluzione P2PE convalidata e inserita nell'elenco PCI SSC, senza memorizzazione elettronica dei dati dei titolari di carta.
- **SAQ SPoC:** Esercenti che utilizzano un dispositivo mobile commerciale off-the-shelf (ad esempio, un telefono o un tablet) con un lettore di carte sicuro incluso nell'elenco di soluzioni SPoC convalidate di PCI SSC. Nessun accesso ai dati di conto clear-text e nessuna memorizzazione elettronica dei dati del conto.

Qualora nessuna di queste descrizioni rispecchi la situazione esatta, l'esercente dovrá utilizzare un SAQ D.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

SAQ B.

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

CRITERI PER SAQ B:

- Esercenti che utilizzano solo macchine stampanti senza memorizzazione elettronica dei dati dei titolari di carta e/o terminali stand-alone, dial-out, senza memorizzazione elettronica dei dati dei titolari di carta.
- DEVE essere dial out, cioè collegato alla linea telefonica e NON a Internet.
- NESSUNA memorizzazione dei dati della carta.

ESEMPIO DI REQUISITO PER SAQ B:

- Monitoraggio e ispezione dei terminali di pagamento, formazione del personale per l'esecuzione delle ispezioni.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

SAQ B-IP.

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

CRITERI PER SAQ B-IP:

- Esercenti che utilizzano solo terminali di pagamento stand-alone, approvati dal PTS, con una connessione IP al processore di pagamento, senza memorizzazione elettronica dei dati dei titolari di carta.
- I terminali di pagamento sono collegati in rete al processore, ma non sono collegati ad altri sistemi all'interno della sede dell'esercente e non dipendono da altri dispositivi (ad esempio, computer, telefoni cellulari, tablet, ecc.) per connettersi al processore di pagamento.
- NESSUNA memorizzazione elettronica dei dati della carta.

ESEMPI DI REQUISITI PER SAQ B-IP:

- I terminali di pagamento sono certificati PTS.
- Gestione di reti e sistemi in modo sicuro.
- Monitoraggio e ispezione dei terminali di pagamento, formazione del personale per l'esecuzione delle ispezioni.
- Esecuzione di scansioni ASV (scansioni di vulnerabilità certificate) su base trimestrale su tutti gli indirizzi IP collegati a internet.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

SAQ C-VT.

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

CRITERI PER SAQ C-VT:

- Esercenti che inseriscono manualmente singole transazioni alla volta tramite tastiera con una soluzione di terminale virtuale basata su internet, fornita e ospitata da un service provider di terze parti convalidato PCI DSS.
- NESSUNA memorizzazione elettronica dei dati dei titolari di carta.
- Viene utilizzata solo una pagina di pagamento fornita dal provider a cui si accede tramite browser.
- Il PC utilizzato non è collegato ad altri sistemi.
- Una transazione alla volta: nessun caricamento di file o elaborazione in batch.
- Non esistono altri metodi di pagamento.
- NESSUNA memorizzazione dei dati della carta.

ESEMPI DI REQUISITI PER SAQ C-VT:

- Gestione di reti e sistemi in modo sicuro.
- Installazione e manutenzione dell'antivirus su tutti i sistemi adeguati.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

SAQ C.

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

CRITERI PER SAQ C:

- Esercenti con sistemi di applicazione di pagamento collegati a Internet, senza memorizzazione elettronica dei dati dei titolari di carta.
- Applicazione singola eseguita su un singolo PC o altro dispositivo
- L'applicazione non memorizza i dati della carta.
- I singoli sistemi sono indipendenti, non sono collegati tra loro e le sedi sono isolate.
- NESSUNA memorizzazione dei dati della carta.

ESEMPI DI REQUISITI PER SAQ C:

- Gestione di reti e sistemi in modo sicuro.
- Utilizzo di una crittografia forte.
- Installazione e manutenzione dell'antivirus su tutti i sistemi adeguati.
- Sviluppare software in modo sicuro.
- Monitoraggio e ispezione dei vostri terminali di pagamento e formazione del personale per l'esecuzione delle ispezioni.
- Esecuzione di scansioni di vulnerabilità interne ed esterne su base trimestrale su tutti gli indirizzi IP e le reti collegate a internet.
- Monitoraggio dei sistemi e degli eventi di registro con avvisi in corso.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fsico.

SAQ PSPE-HW.

Se soddisfate i criteri per la compilazione di un SAQ P2PE-HW, allora la vostra attività è soggetta a quanto segue:

CRITERI PER SAQ P2PE-HW:

- Esercenti che utilizzano solo terminali di pagamento hardware inclusi e gestiti tramite una soluzione P2PE convalidata e inserita nell'elenco PCI SSC, senza memorizzazione elettronica dei dati dei titolari di carta.
- Solo l'elaborazione dei pagamenti viene effettuata utilizzando una soluzione P2PE elencata e certificata.
- Le versioni dei terminali, del firmware e delle applicazioni corrispondono esattamente all'elenco (Elenco ufficiale P2PE).

ESEMPI DI REQUISITI PER P2PE-HW:

- Implementare tutti i controlli previsti dal P2PE Implementation Manual (PIM) offerto dal fornitore.
- Monitoraggio e ispezione dei terminali di pagamento, formazione del personale per l'esecuzione delle ispezioni.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

SAQ SPoC.

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

CRITERI PER SAQ SPoC:

- Esercenti che utilizzano un dispositivo mobile commerciale off-the-shelf (ad esempio, un telefono o un tablet) con un lettore di carte sicuro incluso nell'elenco di soluzioni SPoC convalidate di PCI SSC. Nessun accesso ai dati del conto in chiaro e nessuna memorizzazione elettronica dei dati del conto.
- Solo l'elaborazione dei pagamenti viene effettuata utilizzando una soluzione SPoC elencata e certificata.
- Le versioni dei terminali, del firmware e delle applicazioni corrispondono esattamente all'elenco riportato sul sito ufficiale del Consiglio PCI.

ESEMPIo DI RICHIESTA PER SPoC:

- Monitoraggio e ispezione dei terminali di pagamento, formazione del personale per l'esecuzione delle ispezioni.

Maggiori informazioni sui singoli SAQ per gli esercenti con POS fisico.

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 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 memorizzazione elettronica dei dati del conto.
- Nessun altro SAQ ammissibile.

IMPORTANTE PER SAQ D:

- Un 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.

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.