Indicazioni sull'osservanza delle disposizioni di sicurezza PCI DSS per i partner contrattuali

A livello mondiale, i partner contrattuali che trasmettono, elaborano o memorizzano i dati delle carte sono tenuti ad osservare le direttive di sicurezza definite nel Payment Card Industry Data Security Standard (PCI DSS). Qualora queste venissero disattese, PostFinance ha la facoltà di recedere dal contratto con effetto immediato e di rivalersi sul partner per eventuali sanzioni e risarcimenti.

Le seguenti indicazioni sono, in qualità di direttive tecniche e organizzative, parte integrante e vincolante del contratto di accettazione riguardante le Soluzioni di pagamento Combo con PostFinance.

In cosa consiste lo standard PCI DSS?
PCI DSS comprende 12 requisiti vincolanti, che devono garantire la tutela dei dati delle carte durante l'elaborazione, la memorizzazione e la trasmissione. L'applicazione di PCI DSS è regolata dai programmi di sicurezza delle organizzazioni che emettono le carte. Tra essi AIS di Visa, SDP di Mastercard® nonché i corrispondenti programmi di American Express, Discover (Diners Club) e JCB.

Perché è stato introdotto lo standard PCI DSS?
Negli ultimi anni i furti di dati delle carte sono aumentati in maniera costante. Il successivo impiego abusivo dei dati rubati ha causato danni considerevoli a tutte le parti coinvolte.

Qual è lo scopo dello standard PCI DSS?
Con lo standard PCI DSS le organizzazioni delle carte vogliono incrementare ulteriormente la sicurezza dei pagamenti con le carte e, quindi, tutelare con maggiore efficacia i commercianti, i titolari di carte e l'intero settore dal furto e dall'abuso dei dati delle carte.

Chi è tenuto ad osservare lo standard PCI DSS?
Lo standard PCI DSS obbliga i partner contrattuali che trasmettono, elaborano o memorizzano dati di carte a livello mondiale ad adottare e osservare misure di sicurezza efficaci.

I partner contrattuali sono inoltre responsabili che tali direttive di sicurezza vengano osservate anche da parte di imprese terze da loro incaricate, quali provider di servizi di pagamento (PSP) o data storage entity (DSE), che trasmettono, elaborano o memorizzano dati a loro nome.

Chi è responsabile dell'osservanza dello standard PCI DSS?
Per principio risiede nella responsabilità propria di ciascun partner contrattuale rispettare le disposizioni di sicurezza. Le organizzazioni delle carte, tuttavia, esigono che i partner contrattuali dichiarino (facciano certificare) le misure di sicurezza adottate. L'entità di una dichiarazione (certificazione), dipende dalla quantità di transazioni effettuate e dalla misura in cui un partner contrattuale entra in contatto con i dati delle carte durante la trasmissione, l'elaborazione e la memorizzazione.

Quali varianti di certificazione esistono?
Il PCI DSS è supportato dalle seguenti tre varianti di certificazione (cfr. anche la tabella alla pagina successiva):

- **Self-Assessment Questionnaire (SAQ)**
  Richiede la compilazione di un questionario di autovalutazione.
- **Network Scan**
  Un'azienda di certificazione accreditata (Approved Scanning Vendor) esegue trimestralmente e previo accordo con il partner contrattuale attacchi simulati al sistema per individuarne eventuali punti deboli.
- **On-Site Audit**
  I partner contrattuali con un volume elevato di transazioni o i partner contrattuali che sono stati vittime di un furto di dati delle carte sono tenuti a compilare un ROC (Report on Compliance). I risultati devono essere esaminati e confermati da un QSA (Qualified Security Assessor) o da un auditor qualificato (ISA – Internal Security Assessor).

Se un partner contrattuale non soddisfa tutti i criteri di certificazione, è tenuto a perfezionare, senza indugio, le misure di sicurezza nei settori contestati.

Chi sostiene i costi della certificazione?
I costi delle misure di certificazione sono interamente a carico del partner contrattuale e/o dei terzi incaricati; lo stesso vale per i costi inerenti la rimozione delle defezioni riscontrate nei controlli di certificazione.

Cosa succede se un partner contrattuale non si sottopone alla certificazione?
Se un partner contrattuale che soggiace all'obbligo di certificazione non si sottopone alla stessa, PostFinance ha facoltà di recedere dal contratto con effetto immediato e di esigere il risarcimento dei danni per eventuali multe comminate dalle organizzazioni delle carte e crediti richiesti dalle emittenti delle carte.

Chi ha accesso ai dati di certificazione?
Soltanto il partner contrattuale e l'azienda certificatrice incaricata hanno accesso ai dati rilevati nell'ambito della certificazione. Tuttavia, il partner contrattuale è tenuto a spedire a PostFinance il riassunto degli esiti della certificazione. PostFinance e l'acquirer Worldline hanno inoltre accesso ai questionari di autovalutazione. Le organizzazioni delle carte ricevono invece soltanto valutazioni statistiche.

Con quale frequenza occorre rinnovare una certificazione?
Le misure di certificazione devono essere ripetute periodicamente secondo la tabella alla pagina successiva.

Il partner contrattuale è inoltre tenuto a comunicare tempestivamente a PostFinance eventuali modifiche intervenute che presentano una correlazione diretta con l'accettazione dei pagamenti mediante carta, come l'installazione di nuovo hardware o software, un nuovo sito Internet o il cambio del provider di servizi. In determinati casi può essere necessario rinnovare la certificazione.

Da quali aziende devono essere eseguite le misure di certificazione?
L'elenco di tutte le aziende di certificazione accreditate è disponibile in Internet:

- per l'esecuzione degli On-Site Audit:
  pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- per l'esecuzione dei Network Scans:
  listings.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

Dove reperire ulteriori informazioni sullo standard PCI DSS?
Ulteriori informazioni sullo standard PCI DSS sono disponibili sui siti Internet seguenti:

- Worldline:
  worldline.com/merchant-services/pci
- PCI Security Standards Council:
  pcisecuritystandards.org

Chi deve adottare quali misure di certificazione?

Level	Denominazione	Visa, Mastercard®/ Maestro, Diners/Discover	JCB	American Express
1	Commercianti con oltre 6 milioni di transazioni annue	On-Site Audit annuale [1]		
	Commercianti che hanno subito l'attacco di un hacker con un abuso di dati delle carte	Network Scan trimestrale		
	Commercianti con oltre 2,5 milioni di transazioni annue			On-Site Audit annuale Network Scan trimestrale
	Commercianti con oltre 1 milione di transazioni annue		On-Site Audit annuale Network Scan trimestrale	
2	Commercianti con 1 – 6 milioni di transazioni annue	Self-Assessment Questionnaire annuale [2] Network Scan trimestrale		
	Commercianti con 50'000 – 2,5 milioni di transazioni annue			Network Scan trimestrale
3	Commercianti che praticano e-commerce con 20'000 – 1 milione di transazioni annue	Self-Assessment Questionnaire annuale Network Scan trimestrale		
	Commercianti con meno di 50'000 transazioni annue			Network Scan trimestrale
4	Commercianti che praticano e-commerce con meno di 20'000 transazioni annue	Self-Assessment Questionnaire annuale	Self-Assessment Questionnaire annuale	
	Commercianti (escluso e-commerce) con meno di 1 milione di transazioni annue	Network Scan trimestrale	Network Scan trimestrale	

[1] Il commerciante può decidere se svolgere l'On-Site Audit con il supporto di un QSA (Qualified Security Assessor) o di un ISA (Internal Security Assessor).
[2] Le persone responsabili della compilazione del SAQ devono essere certificate come ISA (Internal Security Assessor).

Gli On-Site Audit e/o i Network Scan sono vincolanti solo per i partner contrattuali che elaborano, trasferiscono o memorizzano per via elettronica i dati delle carte. Indipendentemente da ciò consigliamo in special modo ai partner contrattuali in possesso di infrastrutture complesse di sottoporsi ugualmente a queste misure di convalida. I partner contrattuali sono tenuti in ogni caso a rispettare le direttive PCI DSS. Tuttavia, la certificazione che attesta tale rispetto deve essere prodotta dal partner contrattuale solo previa richiesta scritta da parte di PostFinance.

PostFinance SA
Mingerstrasse 20
3030 Berna

www.postfinance.ch

460.349 it (dok.pf/pf.ch) 02.2025