Payment Services

Scheda informativa sullo standard di sicurezza PA-DSS

Lo standard di sicurezza Payment Application Data Security Standard (PA-DSS) valido in tutto il mondo, consiste in una serie di norme di sicurezza per la realizzazione delle applicazioni di pagamento che memorizzano, elaborano o trasmettono i dati delle carte durante le operazioni di pagamento.

L'impiego di applicazioni di pagamento certificate PA-DSS consente di ridurre notevolmente il rischio di furto dei dati delle carte. Inoltre, PA-DSS agevola la procedura di ottenimento e l'osservanza dello standard di sicurezza PCI DSS (Payment Card Industry Data Security Standard) per le aziende.

Qui di seguito abbiamo raccolto per voi le principali informazioni sul programma PA-DSS.

Perché è stato introdotto PA-DSS?

Dall'analisi di diversi casi di furti di dati risulta che questi atti illeciti sono riconducibili in buona parte alla scarsa protezione delle applicazioni di pagamento. Per questo motivo, nel 2008 è stato introdotto lo standard di sicurezza unitario PA-DSS in vigore a livello internazionale.

Qual è lo scopo di PA-DSS?

L'utilizzo di applicazioni di pagamento certificate è volto a ridurre il rischio di furto di dati delle carte. PA-DSS sostiene gli offerenti di soluzioni nella realizzazione di nuove applicazioni di pagamento e aiuta gli esercenti a raggiungere la conformità PCI DSS (Payment Card Industry Data Security Standard).

Che cosa comprende PA-DSS?

Lo standard comprende 14 requisiti principali e circa 90 requisiti dettagliati che fungono da guida per gli offerenti di soluzioni nello sviluppo di applicazioni di pagamento più sicure. I requisiti di sicurezza sono focalizzati essenzialmente sui seguenti ambiti: realizzazione, processi, implementazione, codificazione e accessi.

Chi deve attuare i requisiti previsti da PA-DSS?

Sono tenuti ad attuare i requisiti PA-DSS gli offerenti di soluzioni nell'ambito delle applicazioni di pagamento che memorizzano, elaborano o trasmettono i dati delle carte. Le precitate applicazioni devono essere parte integrante dei processi di autorizzazione e/o dell'elaborazione dei pagamenti ed essere vendute a terzi.

Chi è responsabile dell'osservanza dei requisiti di PA-DSS?

In primo luogo, sono gli offerenti di soluzioni a dover garantire la conformità delle applicazioni di pagamento ai requisiti PA-DSS. I partner di distribuzione, gli integratori e i partner contrattuali che acquistano, vendono o installano le applicazioni di pagamento devono, da parte loro, verificare che le applicazioni in uso siano provviste della certificazione PA-DSS.

Quali tipi di applicazioni sottostanno ai requisiti di PA-DSS?

- Le applicazioni in serie che vengono vendute e installate a/presso terzi.
- Le applicazioni di pagamento modulari (solo i moduli con funzioni di pagamento).
- I terminali di pagamento autonomi che:
  1. sono collegati al sistema o alla rete dell'esercente
  2. non sono collegati solo all'elaboratore dei pagamenti (acquirer)
  3. non garantiscono una procedura sicura di gestione a distanza dell'applicazione di pagamento
  4. memorizzano i dati sensibili delle carte (dati presenti sulla banda magnetica, CVV2, CVC2, CAV2, CID o PIN) dopo il processo di autorizzazione.

Quali tipi di applicazioni non sottostanno ai requisiti di PA-DSS?

1. Le soluzioni individuali specifiche dei clienti (nessuna distribuzione)
2. Le applicazioni realizzate ad hoc dagli esercenti destinate esclusivamente all'uso interno
3. I sistemi operativi (Windows, Unix, ecc.), le banche dati, i sistemi di gestione (back office) e simili.

Queste applicazioni vengono verificate nel corso della certificazione PCI DSS dell'esercente.

Chi è autorizzato a rilasciare le certificazioni PA-DSS?

Le applicazioni di pagamento possono essere rilasciate e certificate esclusivamente da soggetti appositamente qualificati per la verifica della sicurezza (PA-QSA – Payment Application Qualified Security Assessor). Questi enti di certificazione sono accreditati dal PCI Council. L'elenco di tutti i PA-QSA riconosciuti è consultabile sui seguenti siti:
https://www.pcisecuritystandards.org/security_standards/vpa/

Per quanto tempo è valido il certificato PA-DSS?

Lo standard viene ridefinito ogni tre anni e viene pubblicata una nuova versione. La validità della certificazione scade ogni tre anni dopo la pubblicazione della nuova versione standard. Quindi, la conformità è garantita per almeno tre anni.

Tuttavia, le applicazioni di pagamento devono essere autenticate a scadenza annuale. Se sono state apportate delle modifiche all'applicazione di pagamento, a seconda dell'adeguamento, è imperativo procedere a una nuova convalida di un ente PA-QSA.

Quanto costa la certificazione e chi se ne assume i costi?

I costi della certificazione variano a seconda dell'applicazione di pagamento. Oltre alle dimensioni e alla complessità dell'applicazione di pagamento, è determinante anche la scelta dell'ente di certificazione (PQ-QSA).

A certificazione avvenuta, per l'inserimento nell'elenco del PCI Council va corrisposto l'importo di USD 1250 per ogni applicazione di pagamento. In seguito, ogni anno andrà pagata una tassa amministrativa di USD 500 per ogni applicazione di pagamento.

Dove trovo ulteriori informazioni su PA-DSS?

Per maggiori informazioni su PA-DSS consultate il sito web del PCI Council:
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Si consiglia inoltre il webinar relativo all'argomento PA-DSS:
http://www.webcastgroup.com/client/start.asp?wid=0800522084108

Qui trovate l'elenco di tutte le applicazioni di pagamento certificate:
https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

110.0115.04 CHE_IT/04.2012

Referente personale: www.six-payment-services.com/contatto

SIX Payment Services SA
Hardturmstrasse 201
8005 Zurigo
Svizzera

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Lussemburgo