Payment Services

Direttiva concernente il rispetto delle prescrizioni di sicurezza della Payment Card Industry («Direttiva PCI»)

1. Preambolo

Gli attacchi contro i sistemi informatici sono aumentati in tutto il mondo. In particolare i dati delle carte sono per gli aggressori un obiettivo conveniente ed allettante. Per questo motivo, le organizzazioni internazionali di carte, in collaborazione con gli specialisti della sicurezza dei dati e rappresentanti del commercio, hanno congiuntamente creato il Payment Card Industry Security Standards Council. Questa organizzazione definisce vari standard di sicurezza dei dati (p.es. Payment Card Industry Data Security Standard [in seguito «PCI DSS»] ed il Payment Application Data Security Standard [in seguito «PA DSS»]), che sono vincolanti per tutte le parti contrattuali («PC») e gli attori coinvolti nell'esecuzione o memorizzazione dei dati delle carte di credito. Per il mancato rispetto di questi standard possono venire inflitte ad SIX Payment Services SA (di seguito «SPS») da parte delle organizzazioni carte internazionali multe sostanziose e/o richieste di risarcimento dei danni.

2. Campo d'applicazione

La direttiva concernente il rispetto delle prescrizioni di sicurezza Payment Card Industry vincola tutti i PC di SIX Payment ed è parte integrante del contratto di accettazione per le transazioni in presenza del titolare e/o il commercio a distanza. Alla direttiva sottostanno anche eventuali mandatari o fornitori del PC non appena essi elaborano, memorizzano o memorizzano parzialmente dati rilevanti del pagamento. Il PC è tenuto a trasferire gli obblighi di cui alla presente direttiva ad eventuali terzi fornitori di servizi così come monitorarne l'osservanza.

3. Memorizzazione dei dati

3.1 Divieto di memorizzazione dei dati

E in tutti i casi vietata qualsivoglia memorizzazione di dati sensibili delle carte (archiviazione dei dati a breve ed a lungo termine in forma elettronica o fisica), ad eccezione che per l'ottenimento immediato di un'autorizzazione. Fanno parte della categoria di dati sensibili della carta i dati della banda magnetica della carta (dati Track2), il codice di sicurezza della carta (CVC2/CVV2) e tutti i dati associati con il numero di identificazione personale (NIP) del titolare della carta.

3.2 Restrizioni per la memorizzazione dei dati

Il numero della carta (di solito a sedici cifre) può essere memorizzato elettronicamente solo in forma criptata ed particolarmente sicura. Ciò vale anche per la data di scadenza ed il nome del titolare della carta, se vengono conservati insieme con il numero della carta. Documenti fisici che contengono le informazioni di cui sopra possono essere conservati solo in modo particolarmente sicuro. La memorizzazione dei dati deve essere limitata al minimo necessario per l'attività.

3.3 Altri dati

Altri dati del titolare della carta memorizzati devono venire protetti da accessi non autorizzati dall'interno e dall'esterno per mezzo di adeguate misure di sicurezza logica e fisica.

4. Certificazione Payment Card Industry Data Security Standard

Il Payment Card Industry Data Security Standard comprende un insieme di regole vincolanti per tutte le parti che elaborano, memorizzano o modificano dati delle carte. Il PCI DSS è definito dal PCI Security Standards Council e viene regolarmente aggiornato. Ulteriori informazioni sono disponibili direttamente sul sito ufficiale del PCI Security Standards Council: https://www.pcisecuritystandards.org.

In genere tutti i PC di SPS sono obbligati a certificarsi nei confronti del PCI DSS mediante le misure di certificazione prescritte. SPS è autorizzata a richiedere una certificazione PCI DSS alla conclusione del contratto o in qualsiasi momento nel corso della durata del contratto. Una non-certificazione del PC nonostante sollecito scritto di SPS o l'inesistenza di una relativa certificazione è ragione di disdetta straordinaria senza preavviso.

I requisiti per ottenere la certificazione variano a seconda del volume delle transazioni (v. cifra 4.2).

4.1 Obbligo di certificazione
Sottostanno all'obbligo di ottenere e mantenere una certificazione PCI DSS tutti i PC con un contratto di accettazione per il commercio a distanza e più di 20 000 transazioni all'anno con MasterCard (incl. Maestro) e/o carte Visa.
Sottostanno all'obbligo di ottenere e mantenere una certificazione PCI DSS tutti i PC con un contratto di accettazione per transazioni in presenza del titolare e più di 1 000 000 transazioni all'anno con MasterCard (incl. Maestro) e/o carte Visa.

Tutti i partner contrattuali con un contratto di accettazione per transazioni a distanza sono tenuti a ottenere e mantenere una certificazione PCI DSS qualora gestiscano nei loro sistemi alcuni o tutti i dati delle carte.

4.2 Ottenimento e mantenimento della certificazione PCI DSS
La certificazione PCI DSS dipende dal numero di transazioni elaborate ogni anno. A seconda del numero di transazioni vengono prese regolarmente misure di certificazione differenti. Queste sono le seguent:

Livello	Descrizione	Misure di certificazione	Obbligo di certificazione
1	- PC con più di 6 milioni di transazioni all'anno con MasterCard (incl. Maestro) e Visa attraverso tutti i canali di distribuzione - PC con perdita di dati/attacco hacker avvenuto con successo	- On-Site Audit annuale da parte di QSA - Network-Scan trimestrale da parte di ASV	Obbligo
2	- PC con 1 a 6 milioni di transazioni all'anno con MasterCard (incl. Maestro) e Visa attraverso tutti i canali di distribuzione (transazioni in presenza del titolare e/o per commercio a distanza)	- On-Site Audit annuale da parte di QSA oppure Self Assessment Questionnaire annuale da parte di un collaboratore accreditato ISA - Network-Scan trimestrale da parte di ASV	Obbligo
3	- PC con 20 000 a 1 milione di transazioni e-commerce all'anno con MasterCard o Visa	- Self Assessment Questionnaire annuale - Network-Scan trimestrale da parte di ASV	Obbligo
4	- PC con transazioni e-commerce che gestiscono i dati delle carte nei loro sistemi	- Self Assessment Questionnaire annuale - Network-Scan trimestrale da parte di ASV	Obbligo
5	- Tutti i PC restanti	- Self Assessment Questionnaire annuale - Network-Scan trimestrale da parte di ASV	Su richiesta SIX Payment Services SA

Definizione dei termini Cifra 8

4.3 Dovere di informazione
Il PC deve informare regolarmente e senza solleciti SPS sui risultati delle misure di certificazione. Questo include la messa a disposizione dei Reports on Compliance (ROC) e, ove ciò sia previsto come misura di certificazione, dei risultati dei Network-Scans e Self-Assessment Questionnaires.

Il PC è tenuto ad informare SPS prontamente e senza solleciti qualora non possa essere mantenuto il livello di certificazione PCI DSS richiesto (a causa di modifiche del sistema, di risultati negativi nella certificazione, o simili). Cambiamenti dei fornitori di servizi terzi sono da notificare immediatamente ad SPS.

Se applicazioni di terzi fornitori di servizi sono coinvolti nel modello di licenza, nell'esecuzione o memorizzazione dei dati delle carte, queste applicazioni sono da segnalare ad SPS.

Il PC dà la facoltà ad SPS di chiedere informazioni sul livello di certificazione direttamente presso gli organismi di certificazione.

5. Payment Application Data Security Standard (PA DSS)

Le applicazioni (ad esempio le applicazioni Webshop, sistemi Customer Relationship Management, sistemi Hotel Property Management) che vengono vendute, trasferite o concesse in licenza a terzi, soggiacciono, fatte salve le eccezioni, ai requisiti PA DSS. Applicazioni di pagamento interne all'attività sviluppate dai PC o fornitori di servizi terzi che non sono venduti o concessi in licenza a terzi, non sono soggette ai requistiti PA DSS.

Dal **01.07.2012** tutte le applicazioni che vengono utilizzate in un modello di licenza da terzi fornitori di servizi o applicazioni standardizzate o acquistate, che operano o memorizzano i dati delle carte devono avere una certificazione PA DSS. Tutte le applicazioni certificate PA DSS sono pubblicate sul sito web del PCI Security Standards Council.

6. Terzi fornitori di servizi

Terzi fornitori di servizi sono società esterne che per conto del PC gestiscono, memorizzano o trasferiscono i dati delle carte (p.es. Payment Service Provider, Webhosting-Provider, portali per le prenotazioni).

Tutti i terzi fornitori di servizi incaricati dal PC devono essere provvisti in qualsiasi momento di certificazione PCI DSS e riconosciuti e registrati tramite le organizzazioni internazionali di carte. SPS può vietare l'impiego di un terzo fornitore di servizio in qualsiasi momento o combinarlo con singole restrizioni. In generale possono venire impiegati solo i terzi fornitori di servizi che sono elencati nella lista dei terzi fornitori di servizi autorizzati pubblicata da SPS.

7. Terminali POS

Tutti i terminali POS utilizzati devono disporre di certificazioni PCI PTS valide.

8. Definizioni

Memorizzazione dei dati
La memorizzazione dei dati comprende la memorizzazione dei dati in forma elettronica o fisica, sia a lungo termine che a breve termine (memorizzazione temporanea).

Qualified Security Assessor (QSA)
Un Qualified Security Assessor è una persona fisica accreditata dalla PCI Security Standards Council che abbia diritto di condurre presso il PC o un terzo una verifica e redigere un Report of Compliance (ROC).

Approved Scanning Vendor (ASV)
Un Approved Scanning Vendor è una società di sicurezza che è stata accreditata dal PCI Security Standards Council ed esegue scansioni della rete.

Network-Scan
Un Network-Scan è un attacco Haking effettuato periodicamente e previo accordo con il PC, in modo da individuare le possibili debolezze nel sistema del PC. Un Network-Scan può venire effettuata solo da un da un Approved Scanning Vendor.

On-Site Audit
Un On-Site Audit è una verifica dal PC o terzo fornitore di servizi in merito alla conformità agli standard PCI DSS da parte di un Qualified Security Assessor. Il risultato viene trascritto in un Report on Compliance.

Self Assessment Questionnaire (SAQ)
Un Self Assemssment Questionnaire è un auto-dichiarazione in materia di conformità agli standard PCI DSS. Per un SAQ deve essere compilato un questionario di sicurezza dettagliato. È certificato colui che può rispondere a tutte le domande con un Sì, rispettivamente, con «non si applica».

Report on Compliance (ROC)
Un Report on Compliance viene redatto da un Qualified Security Assessor dopo un On-Site Audit e conferma la piena conformità agli standard PCI DSS.

Internal Security Assessor Program (ISA)
L'Internal Security Assessor Program messo a disposizione dal PCI Security Standards Council Security si rivolge al personale interno specializzato del PC ed offre un programma completo di formazione in merito ai requisiti PCI DSS. Il programma si conclude con un esame di accreditamento. L'accreditamento deve essere ripetuto annualmente.

110.0901.04 CHE_IT/06.2018

SIX Payment Services SA
Hardturmstrasse 201, Casella postale
8021 Zurigo

www.six-payment-services.com/welcome