RISORSE PER LA PROTEZIONE DEI PAGAMENTI PER PICCOLI ESERCENTI

Domande da chiedere ai vostri fornitori

VERSIONE 1.0 | GIUGNO 2016

PCI Security Standards Council®

Introduzione

Questo documento è stato preparato come ausilio per proprietari e operatori di piccole attività commerciali. Queste domande da chiedere ai vostri fornitori e provider di servizi hanno lo scopo di assistervi nella comprensione del modo in cui tali entità supportano la protezione dei dati delle carte di pagamento dei vostri clienti.

Domande da chiedere ai vostri fornitori è stato sviluppato come supplemento alla *Guida ai pagamenti sicuri*, parte di Risorse di protezione dei pagamenti per piccoli esercenti. Fate riferimento alla *Guida ai pagamenti sicuri* e alle altre Risorse di protezione dei pagamenti per piccoli esercenti ai seguenti:

RISORSA	URL
Guida ai pagamenti sicuri	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemi di pagamento comuni	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossario dei termini sulla sicurezza dei pagamenti e delle informazioni	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Fornitori e provider di servizi e come operano

I piccoli esercenti/aziende potrebbe contattare diversi fornitori o provider di servizi di pagamento ed è importante che gli esercenti comprendano il tipo di fornitore con cui collaborano e assicurarsi che il fornitore abbia eseguito le operazioni corrette per la protezione dei dati delle carte di pagamento.

La tabella alla pagina 2 descrive i tipi più comuni di fornitori e provider di servizi di pagamento e cosa gli esercenti devono cercare in ogni fornitore.

La tabella che inizia a pagina 3 fornisce agli esercenti domande che possono chiedere ai loro fornitori o provider di servizi per comprendere qual'è il ruolo del fornitore o provider di servizi nella protezione dai dati delle carte di pagamento.

Fornitori e provider di servizi

La tabella seguente descrive i tipi più comuni di fornitori e provider di servizi di pagamento e cosa gli esercenti devono cercare in ogni fornitore.

TIPO DI FORNITORE/ PROVIDER DI SERVIZI	FUNZIONE	STANDARD O PROGRAMMA PCI	CERCATE:
Fornitore dell'applicazione di pagamento	Vendono e supportano le applicazioni che memorizzano, elaborano e/o trasmettono i dati dei titolari di carta.	Standard di protezione dei dati per le applicazioni di pagamento (PA-DSS)	L'applicazione si trova nell' List of PCI PA-DSS of Validated Payment Applications (Elenco degli standard PCI PA-DSS delle applicazioni di pagamento convalidate).
Fornitore dei terminali di pagamento	Vende e supporta dispositivi utilizzati per accettare pagamenti con carta (ad esempio, un terminale di pagamento).	Sicurezza transazione PIN (PTS)	Il terminale di pagamento si trova nell' List of PCI Approved PTS Devices (Elenco dei dispositivi PTS approvati dal PCI).
Gli elaboratori di pagamenti, i provider di hosting/elaboratori e-commerce	Memorizza, elabora o trasmette i dati dei titolari di carta per conto vostro. Potrebbe anche essere l'host del vostro server/sito Web e-commerce e gestirlo e/o sviluppare e supportare il vostro sito Web.	Standard di protezione dei dati PCI (PCI DSS)	Richiedete il loro Attestato di conformità PCI DSS e chiedete se la sua valutazione include il servizio che utilizzate. Il provider di servizi si trova in uno dei seguenti elenchi: MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard) Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa) Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe)
Provider di software come servizio	Sviluppano, eseguono e/o gestiscono la vostra applicazione Web basata sul cloud o l'applicazione di pagamento (ad esempio, l'applicazione di biglietteria o prenotazioni online).	PCI DSS	Richiedete il loro Attestato di conformità PCI DSS e chiedete se la sua valutazione include il servizio che utilizzate. Il provider di servizi si trova in uno dei seguenti elenchi: MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard) Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa) Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe)
Responsabili dell'integrazione/rivenditori	Installano le applicazioni di pagamento convalidate dagli standard PA-DSS per vostro conto.	Responsabili dell'integrazione e rivenditori qualificati (QIR)	Chiedete se il fornitore è un responsabile dell'integrazione o rivenditore PCI qualificato (QIR). Il fornitore si trova sull'List of PCI QIRs (Elenco dei QIR PCI).
I provider di servizi che soddisfano i requisiti PCI DSS	Gestiscono/operano i sistemi o i servizi per vostro conto (ad esempio la gestione del firewall, i servizi di patching/AV).	PCI DSS	Richiedete il loro Attestato di conformità PCI DSS e chiedete se la sua valutazione include il servizio che utilizzate. Il provider di servizi si trova in uno dei seguenti elenchi: MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard) Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa) Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe)

Domande

La tabella seguente contiene una serie di domande che gli esercenti possono chiedere ai loro fornitori/provider di servizi per stabilire se sono stati introdotti i controlli corretti per la protezione dei dati delle carte di pagamento.

DOMANDA *Posta dall'esercente al fornitore*	**RISPOSTA DEL FORNITORE DESIDERATA**	**AZIONE SUGGERITA** *A seconda della risposta del fornitore*
COME PROTEGGERE LA VOSTRA SOLUZIONE O PRODOTTO?		
1. La vostra soluzione/prodotto garantisce la cattura e trasmissione sicura dei dati dei titolari di carta?	**Per transazioni di pagamento con carta eseguite di persona:** **SÌ** • Controllate qui se il terminale di pagamento è approvato dal PCI PTS: List of PCI Approved PTS Devices (Elenco dei dispositivi PTS approvati dal PCI) E/O • Controllate qui se l'applicazione di pagamento è convalidata dagli standard PCI PA-DSS: List of PCI PA-DSS of Validated Payment Applications (Elenco degli standard PCI PA-DSS delle applicazioni di pagamento convalidate) O • Controllate qui se la soluzione di cifratura è convalidata da PCI P2PE: List of PCI P2PE Validated Solutions (Elenco di soluzione convalidate PCI P2PE)	Se **NO**, chiedere la Domanda 2.
	Per transazioni di pagamento con carta non presente (incluso l'e-commerce, ordine via posta/telefono): **SÌ** • Controllate qui se l'applicazione di pagamento è convalidata dagli standard PCI PA-DSS: List of PCI PA-DSS of Validated Payment Applications (Elenco degli standard PCI PA-DSS delle applicazioni di pagamento convalidate) O • Controllate qui se il provider di servizi è un provider di servizi conforme a PCI DSS: MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard) Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa) Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe))	

Domande

DOMANDA *Posta dall'esercente al fornitore*	RISPOSTA DEL FORNITORE DESIDERATA	AZIONE SUGGERITA *A seconda della risposta del fornitore*
COME PROTEGGERE LA VOSTRA SOLUZIONE O PRODOTTO? *continua*		
2. Il nostro contratto con lei (il fornitore) include clausole che dichiarano che lei manterrà la conformità PCI DSS per il vostro prodotto/servizio (o viene convalidato dagli standard PCI DSS)?	**SÌ** I fornitori con prodotti/soluzioni che sono o diventeranno conformi agli standard PCI DSS non dovrebbero aver problemi con l'inclusione di tale stato in un contratto scritto. Per ulteriori informazioni sulle prove da trovare in relazione ai prodotti/soluzioni conformi agli standard PCI DSS, fate riferimento alla Domanda 1 di cui sopra.	Se **NO**, prendete in considerazione un altro fornitore o un'altra soluzione.
3. Il vostro prodotto/soluzione memorizza le informazioni delle carte di pagamento in locale (presso la sede del mio negozio)?	**NO** Se sì, gli esercenti possono prendere in considerazione una soluzione di tokenizzazione o di cifratura per una sicurezza migliore dei dati delle carte di pagamento. Consultate la *Guida ai pagamenti sicuri* per ulteriori informazioni relative alla cifratura e alla tokenizzazione.	Se **SÌ**, l'esercente deve confermare con il fornitore che i dati vengono memorizzati in base ai requisiti PCI DSS. Altrimenti, prendete in considerazione un altro fornitore.
4. Il vostro prodotto/soluzione protegge le informazioni delle carte di pagamento con una cifratura solida?	**SÌ** La cifratura è un modo di proteggere le informazioni al fine di ridurre il rischio che vengano rubate. Se potete, selezionate List of PCI P2PE Validated Solutions (Elenco di soluzione convalidate PCI P2PE), dove i dati delle carte sono protetti non appena li ricevete e vengono protetti mentre si muovono attraverso la vostra rete.	Se **NO**, prendete in considerazione un altro fornitore o un'altra soluzione.

Domande

DOMANDA *Posta dall'esercente al fornitore*	RISPOSTA DEL FORNITORE DESIDERATA	AZIONE SUGGERITA *A seconda della risposta del fornitore*
QUANTO SICURA È L'INSTALLAZIONE DEL MIO PRODOTTO?		
5. Se il fornitore installa un'applicazione di pagamento List of Validated Payment Applications (Elenco delle applicazioni di pagamento convalidate) dell'Ente PCI, chiedete: È lei un responsabile dell'integrazione o rivenditore PCI qualificato (QIR)?	**SÌ** Un QIR è formato e qualificato dall'Ente per installare e integrare le applicazioni di pagamento PA-DSS e le sue installazioni forniscono la certezza che l'applicazione di pagamento PA-DSS sia stata implementata in maniera che supporti la conformità agli standard PCI DSS. Controllate qui se il fornitore si trova nell'elenco: List of PCI QIRs (Elenco dei QIR PCI).	Se **NO**, ponete le domande di approfondimento che trovate a sinistra.
Domande di approfondimento se la risposta alla domanda è NO: Se l'applicazione che il fornitore installa non è stata convalidata da PCI SSC o se il fornitore non è un QIR, chiedete: • Fornisce il supporto durante l'installazione per assicurare che la nostra implementazione soddisfi i requisiti di PCI DSS? • Fornisce una guida all'implementazione? • Fornisce l'assistenza all'installazione per assicurare che i dati delle carte siano protetti ovunque siano stati salvati, elaborati o trasmessi?	**SÌ** Il fornitore deve aver definito i processi per assistervi nell'installazione della soluzione in conformità ai requisiti PCI DSS. Un'installazione non corretta può rendere la soluzione vulnerabile alla compromissione dei dati. Quella che volete è una dichiarazione del fornitore che spieghi come vi aiuterà nell'assicurarvi che i requisiti PCI DSS vengano o che possano essere soddisfatti per il prodotto/soluzione.	Se **NO**, prendete in considerazione un altro fornitore.

Domande

DOMANDA *Posta dall'esercente al fornitore*	RISPOSTA DEL FORNITORE DESIDERATA	AZIONE SUGGERITA *A seconda della risposta del fornitore*
MI FORNISCE UN'ASSISTENZA E MANUTENZIONE CONTINUE PER IL PRODOTTO/SOLUZIONE? SE SÌ, COME?		
6. Il suo prodotto/soluzione viene installato/a sulla mia rete o i miei sistemi?	**SÌ** Il fornitore deve deve fornire una manutenzione e assistenza continue per gli aggiornamenti del software e le patch di sicurezza. Inoltre, deve fornire e offrire assistenza per future release di versioni. È nel vostro miglior interesse servirvi di fornitori che supportino completamente i loro prodotti e vi assistano con installazioni/patch che garantiscano che le modifiche eseguite al sistema siano conformi ai requisiti PCI.	Se la risposta è **SÌ**, consultate le domande di approfondimento, a sinistra. Se **NO**, passate alla Domanda 7.
Domande di approfondimento se la risposta alla domanda è SÌ: • Installa le patch e gli aggiornamenti al sistema/soluzione? • Lo fa in modo che soddisfino i requisiti agli standard PCI DSS? • Come mi invierà le notifiche; come vengono rese disponibili le patch e che assistenza fornisce?	**SÌ** Se la soluzione non viene mai aggiornata, potrebbe diventare vulnerabile a future compromissioni.	Se **NO**, prendete in considerazione un altro fornitore.
7. La soluzione viene installata sui sistemi di proprietà del e mantenuta (eseguita) dal provider di servizi?	**SÌ** Questo viene considerato un servizio gestito. Se il provider di servizi esegue la soluzione, richiedete il loro Attestato di conformità PCI DSS e chiedete se la sua valutazione include il servizio che utilizzate.	Se **SÌ**, ponete le domande di approfondimento che trovate a sinistra. Se **NO**: se il servizio gestito non è conforme agli standard PCI DSS, prendete in considerazione un'altra soluzione.
Domande di approfondimento se la risposta alla domanda è**SÌ**: L'ambiente del provider di servizi è conforme agli standard PCI DSS?	Verificate che il provider di servizi si trovi in uno dei seguenti elenchi: MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard) Visa's Global Registry of Service Providers (Registro globale dei provider di servizi di Visa) Visa Europe's Registered Member Agents (Agenti membri registrati di Visa Europe)	

Domande

DOMANDA *Posta dall'esercente al fornitore*	RISPOSTA DEL FORNITORE DESIDERATA	AZIONE SUGGERITA *A seconda della risposta del fornitore*
MI FORNISCE UN'ASSISTENZA E MANUTENZIONE CONTINUE PER IL PRODOTTO/SOLUZIONE? *continua*		
8. Ha bisogno dell'accesso remoto al mio sistema/soluzione di pagamento per supportarlo?	**NO** L'accesso remoto viene spesso utilizzato nelle violazioni dei dati dei pagamenti. La funzionalità dell'accesso remoto deve essere limitata all'utilizzo in tempi brevi e disabilitata in qualsiasi altro momento.	Se **NO**, passate alla Domanda 9. Se **SÌ**, ponete le domande di approfondimento che trovate a sinistra.
Domande di approfondimento se la risposta alla domanda è SÌ: • Ha bisogno che l'accesso remoto sia sempre attivo?	**NO** La funzionalità dell'accesso remoto deve essere limitata all'utilizzo in tempi brevi e disabilitata in qualsiasi altro momento.	Se **SÌ**: Se è necessario che l'accesso remoto sia sempre attivo, prendete in considerazione un altro fornitore o un'altra soluzione.
• Quali passi eseguite per proteggere le connessioni in accesso remoto?	**Il vostro fornitore deve utilizzare l'autenticazione a più fattori E nome utente e password diversi per ogni cliente a cui accede in remoto.** Le connessioni in accesso remoto possono essere protette mediante l'uso di ID utente e password univoci per ogni persona che utilizza il sistema. Inoltre, devono essere utilizzate più modalità di verifica dell'identità della persona che accede al sistema (autenticazione a più fattori). I fornitori che utilizzano nome utente/password univoche per ognuno dei loro clienti, impediscono che una compromissione di uno dei loro clienti diventi una compromissione di numerosi o di tutti i loro clienti mediante l'uso di nome utente e password comuni.	Se il prodotto/soluzione non offre un'autenticazione a più fattori per l'accesso remoto, prendete in considerazione un'altra soluzione.
9. È necessaria l'integrazione con i miei altri sistemi (ad esempio terminali di pagamento, credito residuo) o con altri sistemi che contengono i dati dei titolari di carta?	**NO** Un terminale di pagamento indipendente è più facile da proteggere di un sistema di pagamento più complesso che potrebbe avere numerosi sistemi collegati. Se la soluzione richiede l'integrazione con altri sistemi, semplifica il vostro ambiente di elaborazione e/o come apporterà valore alla vostra azienda? Bisogna che la vostra azienda abbia un grande bisogno di integrazione, dato che l'utilizzo di una soluzione integrata accrescerà l'ambito PCI DSS, poiché rende il vostro ambiente dei dati dei titolari di carta più grande e più complesso. MasterCard's List of Compliant Service Providers (Elenco di provider di servizi conformi di MasterCard)	Se **SÌ**, prendete in considerazione un altro fornitore o prodotto a meno che la vostra azienda non abbia una forte necessità di avere una soluzione più complessa, con connessioni ad altri sistemi.

Domande

DOMANDA *Posta dall'esercente al fornitore*	RISPOSTA DEL FORNITORE DESIDERATA	AZIONE SUGGERITA *A seconda della risposta del fornitore*
COSA ACCADE SE SI VERIFICA UNA VIOLAZIONE DEI DATI?		
10. Nel caso in cui si verifichi una violazione dei dati e il vostro prodotto o la vostra soluzione ne sono interessati: • Se io dovessi subire penali, lei offre assistenza e protezione? • Come e quando mi notifica se si verifica una violazione? • Che tipo di monitoraggio delle violazioni dei dati e delle attività sospette fornisce?	**SÌ** Il fornitore/provider di servizi deve fornire l'assistenza nel caso di violazione dei dati dei titolari di carta. Il fornitore/provider di servizi deve voler collaborare con un investigatore di scienza forense, se vi sono domante relative al servizio gestito o alla soluzione fornita. Il fornitore/provider di servizi deve indennizzare l'esercente nel caso in cui quest'ultimo subisca penali a causa di violazioni e che venga stabilito che la soluzione dello stesso fornitore ne sia la causa principale.	Se **NO**, prendete in considerazione un altro fornitore o un'altra soluzione.
11. Il fornitore/provider di servizi dispone di un'assicurazione che copra le violazioni dei dati relativi al suo prodotto o alla sua soluzione?	**SÌ** Il fatto che il fornitore/provider di servizi disponga di un'assicurazione dimostra che ha preso in considerazione le proprie responsabilità legali relative alle violazioni dei dati delle carte di pagamento. Se **SÌ**, informatevi a proposito dell'ambito della copertura e se la vostra implementazione verrà coperta.	Se **NO**: se il fornitore non dispone di assicurazione o non ha intenzione di auto-assicurarsi, prendete in considerazione la possibilità di acquistare un'assicurazione vostra o di utilizzare un altro fornitore.
12. Il fornitore/provider di servizi fornisce assistenza nel notificare i miei clienti nel caso si verifichi una violazione dei dati e il suo prodotto ne è la causa principale?	**SÌ** Il fornitore/provider di servizi deve voler assistere gli esercenti nella notifica di violazioni quando il suo sistema di pagamento ne è la causa principale.	Se **SÌ**, ponete le domande di approfondimento che trovate a sinistra. Se **NO**: se il fornitore non fornisce assistenza con la notifica, dovreste sviluppare un piano per la notifica e/o prendere in considerazione un altro fornitore.
Se **SÌ**, fino a che punto fornisce assistenza con la notifica? • Lei copre i costi? • Invia le notifiche? • Fornisce il monitoraggio del credito per i clienti interessati?		