Payment Services

Pagamenti sicuri tramite carta nel settore alberghiero

Una guida SIX Payment Services

Contenuto

Prefazione

Sempre più persone apprezzano la flessibilità e l'indipendenza del pagamento con carta, sia dietro che davanti alla reception.

Per continuare a spostare l'ago della bilancia verso i vantaggi, desideriamo mostrarvi la migliore procedura corretta per effettuare pagamenti senza contanti e fornirvi indicazioni preziose. Inoltre, è necessario osservare alcune misure di sicurezza, perché dove c'è il successo, non mancano mai i truffatori: particolarmente nel settore alberghiero, negli ultimi anni gli episodi di truffa sono aumentati.

Azienda leader nel campo dei pagamenti senza contanti, SIX Payment Services si sente in dovere di assistervi concretamente nella gestione efficiente di pagamenti con carta oltre che in materia di sicurezza dei dati delle carte di credito.

Processo di prenotazione semplice

Passo dopo passo

SIX ha sviluppato un processo di prenotazione studiato appositamente per le esigenze del settore alberghiero e offre inoltre la procedura di pagamento con token (dati sostitutivi). Così, i processi sono contraddistinti da una maggiore sicurezza dei dati e accompagnati da ulteriori vantaggi utili. Vi ricordiamo che la funzione sul vostro terminale (ep2) deve essere attivata. Se ancora così non fosse, vi invitiamo a informarvi presso SIX.

Stato	Procedura al terminale di pagamento	Osservazioni
Prenotazione via telefono, posta, e-mail o portale online. Titolare della carta e carta di pagamento non si trovano sul posto.	Prenotazione*	All'atto della prenotazione viene generato un token PAN con relativa data di scadenza. Questi sono annotati sulla ricevuta.**
Check-in: titolare della carta e carta di pagamento si trovano sul posto.	Prenotazione*	Attivare di nuovo una prenotazione sul terminale di pagamento e leggere la carta di pagamento. Verrà generato un nuovo token PAN con relativa data di scadenza.
	Annullamento prenotazione	Infine, annullare la prima prenotazione al terminale di pagamento, affinché l'importo venga prenotato sulla carta una volta sola.
In caso di prolungamento del soggiorno	Aumento prenotazione	
Check-out	Registrazione prenotazione	Non è tassativo leggere la carta di pagamento, neanche per pagamenti DCC. **Importante:** Dopo questo processo, la prenotazione originale ed eventuali aumenti di prenotazione vengono registrati e cancellati in automatico. Pertanto, non è necessario eseguire alcun annullamento della prenotazione.

* se non è già presente una prenotazione online con addebito della carta già eseguito.

** Il token PAN è un numero di 19 cifre, originato casualmente e non identificabile, che sostituisce il numero originale della carta. Solo SIX può identificare a quale numero originale di carta appartiene il token PAN. Per ciascun token PAN viene generata una data di scadenza casuale che, per motivi di sicurezza, non corrisponde a quella sulla carta di pagamento originale.

Vantaggi del processo di prenotazione con SIX

La carta di pagamento deve essere letta solo al check-in, mentre al check-out non è più necessaria.

Al check-out è possibile eseguire anche la conversione di valuta dinamica (DCC) senza leggere ancora la carta.

I dati della carta vengono trasmessi con lo standard sicuro EMV e «tokenizzati», ossia sostituiti da dati casuali non identificabili. Giacché queste informazioni non sono sensibili, l'adempimento dei requisiti PCI DSS viene notevolmente semplificato.

Suggerimenti

Se possibile, al momento del check-in leggere la carta di pagamento con il chip o la banda magnetica. Così, in caso di danni, trasferirete la responsabilità alla banca di emissione della carta.

Con la procedura DCC al check-out offrite ai vostri ospiti la possibilità di pagare nella valuta della carta. L'ospite deve avere la possibilità di confermare il proprio consenso premendo un tasto sul terminale di pagamento. Informate l'ospite della procedura DCC facendogli semplici domande, per esempio: Possiamo regolare il pagamento direttamente in sterline (valuta della carta)?

Informate il vostro ospite del fatto che, al momento della prenotazione, l'importo della prenotazione è stato riservato sulla sua carta di credito e scalato dal limite di utilizzo della stessa (ma non è stato addebitato sulla carta).

Indicazioni importanti

È consentito emettere accrediti solo sulla stessa carta che è stata addebitata originariamente. Non eseguire in nessun caso un accredito su altre carte di credito, di debito o conti bancari.

Procedura al terminale

Guida rapida

Prenotazione

1. Selezionare «Prenotazione»
2. Inserire l'importo da riservare e autorizzare
3. Leggere la carta al terminale
4. Confermare l'importo con PIN o firma
5. Verrà stampata la ricevuta di «prenotazione»

Aumento prenotazione

1. Sotto «Altre transazioni», richiamare il tipo di prenotazione «Aumento prenotazione»
2. Inserire l'importo di cui deve essere aumentata la prenotazione
3. Inserire il «Numero riferimento trx»
4.1 Carta presente sul posto: leggere la carta al terminale
4.2 Carta non presente sul posto: selezionare «manuale» e immettere il token PAN e la data di scadenza del token
5. Confermare l'importo
6. Verrà stampata la ricevuta di «aumento di prenotazione»

Registrazione (prenotazione)

1. Selezionare «Registrazione prenotazione»
2. Inserire l'importo finale (l'importo della differenza verrà autorizzato successivamente in automatico)
3. Selezionare «manuale»
4. Inserire il «Numero riferimento trx»
5. Verrà chiesto il numero della carta
   > Immettere il token PAN
6. Verrà chiesta la data di scadenza
   > Inserire la data di scadenza del token
7. Verranno richiesti i codici di sicurezza CVC2/CVV2
   > Premere il tasto «OK»
8. Controllare l'importo finale e, in caso di ospite straniero, selezionare DCC. L'ospite stesso deve confermare DCC premendo un tasto. Non sarà necessario leggere alcuna carta.

No show (mancato arrivo)

Procedimento analogo al processo di «Registrazione prenotazione» con le seguenti variazioni:

– è consentito addebitare al massimo l'importo di un pernottamento
– annotare a mano «no show» nella riga della firma della ricevuta

Accredito

1. Selezionare «Accredito»
2. Inserire la password per il terminale di pagamento e premere «OK»
3. Inserire l'importo e premere «OK»
4. Inserire la data della transazione originaria
5. Introdurre la carta e premere «OK»
6. Verrà stampata la ricevuta di «accredito»

Prenotazione (addebito a saldo)

1. Selezionare «Prenotazione»
2. Inserire l'importo dell'addebito a saldo
3. Selezionare «manuale»
4. Verrà richiesto il numero della carta
   > Immettere il token PAN
5. Verrà richiesta la data di scadenza
   > Inserire la data di scadenza del token
6. Verranno richiesti i codici CVC2/CVV2
   > premere «OK»
7. Non offrire la procedura DCC, poiché il titolare della carta non può confermarla premendo un tasto
8. Scrivere «Signature on File» (firma su file) nella riga della firma sulla ricevuta

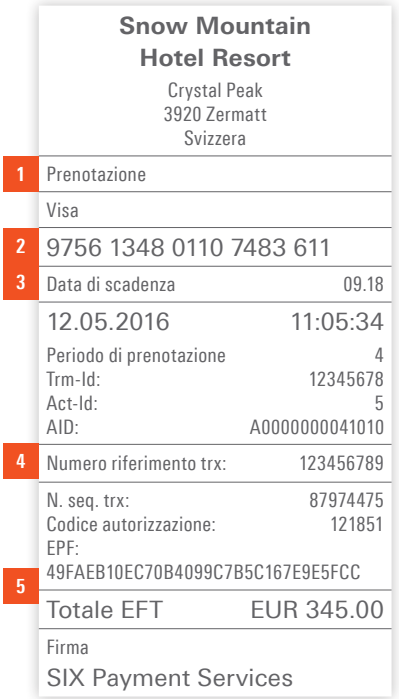
Annullamento prenotazione

1. Sotto «Altre transazioni», selezionare il tipo di prenotazione «annullamento pren.»
2. Inserire il «Numero riferimento trx»

3.1 Carta presente sul posto:
– leggere la carta al terminale
– la prenotazione verrà annullata

3.2 Carta non presente sul posto:
– selezionare «manuale»
– verrà chiesto il numero della carta
  > Immettere il token PAN
– verrà chiesta la data di scadenza
  > Inserire la data di scadenza del token
– Verranno chiesti i codici di sicurezza CVC2/CVV2 > premere «OK»

Ricevuta



Snow Mountain Hotel Resort
Crystal Peak
3920 Zermatt
Svizzera

1 Prenotazione

Visa

2 9756 1348 0110 7483 611

3 Data di scadenza 09.18

12.05.2016 11:05:34

Periodo di prenotazione 4
Trm-Id: 12345678
Act-Id: 5
AID: A0000000041010

4 Numero riferimento trx: 123456789

N. seq. trx: 87974475
Codice autorizzazione: 121851
EPF:
5 49FAEB10EC70B4099C7B5C167E9E5FCC

Totale EFT EUR 345.00

Firma
SIX Payment Services

1 Tipo di prenotazione
2 «Numero carta token»
3 «Data di scadenza token»
4 Numero di riferimento della transazione
5 Importo totale

Garanzia di prenotazione con carta di credito

Procedura corretta

In caso di prenotazione con carta di credito (Visa, Mastercard, UnionPay, JCB, Diners Club Card o Discover Card), è possibile garantire il primo pernottamento.

Prenotazione

Al momento della prenotazione, chiedete all'ospite le seguenti informazioni:
- nome, cognome (come indicati sulla carta)
- indirizzo di fatturazione
- numero carta di credito e data di scadenza
- numero telefonico, indirizzo postale, indirizzo e-mail
- data di arrivo e durata del soggiorno

Date all'ospite le seguenti informazioni, possibilmente in forma scritta:
- prezzo a pernottamento per la categoria di cameradesiderata e totale della fattura (IVA inclusa)
- indirizzo esatto dell'hotel
- codice di prenotazione (assegnato dall'hotel)
- condizioni di annullamento del vostro hotel, in particolare il termine ultimo di annullamento senza spese
- che una volta scaduto il termine di annullamento, o se le condizioni di annullamento non venissero rispettate, gli sarà addebitato un pernottamento tasse incluse

Annullamento

In linea di principio, siete obbligati ad accettare tutti gli annullamenti che vi pervengono entro le 18 ora locale del giorno di arrivo programmato. Se questo periodo di annullamento non è sufficiente, potete spostarlo a massimo 72 ore prima dell'arrivo programmato del cliente. In questo caso, dovete indicare in forma scritta al vostro ospite questo particolare termine di annullamento. Fate espressamente riferimento alla data concreta e all'ora di questo termine.
- Eseguite un «annullamento prenotazione» al terminale di pagamento
- Dovete comunicare al titolare della carta il numero di annullamento (emesso dall'hotel)

No show (mancato arrivo)

Se l'ospite non si presenta e non ha neanche annullato per tempo la prenotazione, potete addebitare sulla sua carta di credito i costi relativi a un pernottamento, tasse incluse, ed emettere la relativa ricevuta.
- Eseguite una «prenotazione» pari all'importo corrispondente
- Al posto della firma del titolare della carta, inserite a mano la nota «No show» nella riga della firma

Suggerimento

Chiedere all'ospite di firmare una dichiarazione di consenso nella quale egli acconsente alle vostre condizioni di annullamento.

Importante

Qualora il titolare della carta dovesse contestare di aver eseguito lui stesso la prenotazione alberghiera, potreste non avere diritto ad alcun risarcimento.

Prenotazione con acconto con carta di credito (Advance Deposit)

Procedura corretta

Se per una prenotazione desiderate chiedere un acconto, potete farlo sulla carta di credito dell'ospite. Esistono due possibilità: al terminale di pagamento oppure online. In entrambe le opzioni è importante seguire esattamente i seguenti passaggi per evitare di dover fornire chiarimenti o riprenotazioni.

Prenotazione

Al momento della prenotazione, chiedete all'ospite le seguenti informazioni:
- nome, cognome (come indicati sulla carta)
- indirizzo di fatturazione
- numero carta di credito e data di scadenza
- numero telefonico, indirizzo postale, indirizzo e-mail
- data di arrivo e durata del soggiorno

Date all'ospite le seguenti informazioni, possibilmente in forma scritta:
- prezzo a pernottamento per la categoria di camera desiderata e totale della fattura (IVA inclusa)
- indirizzo esatto dell'hotel
- codice di prenotazione (assegnato dall'hotel)
- condizioni di annullamento del vostro hotel, in particolare il termine ultimo di annullamento senza spese
- importo dell'acconto che addebiterete sulla sua carta di credito (non deve superare il prezzo per 14 notti). Nella conferma, rinunciate a indicare il numero di carta di credito completo e indicate al massimo le ultime quattro cifre.
- che l'acconto sarà detratto dal conteggio finale
- che l'alloggio sarà tenuto libero per lui/lei nel periodo coperto dall'acconto
- che l'acconto sarà trattenuto, in tutto o in parte, dopo la scadenza del termine di annullamento oppure se le condizioni di annullamento non sono state rispettate

Suggerimento

Chiedere all'ospite di firmare una dichiarazione di consenso nella quale egli acconsente alle vostre condizioni di annullamento.

Registrazione dell'acconto al terminale di pagamento

- eseguire una «prenotazione» al terminale di pagamento
- Sulla ricevuta, scrivere a mano «Advance Deposit» (acconto) nella riga della firma
- Siete obbligati a far pervenire all'ospite una conferma scritta di versamento dell'acconto e una copia della ricevuta di prenotazione entro tre giorni lavorativi.
- La conferma di versamento dell'acconto che emetterete dovrà contenere i seguenti dati:
  - nome hotel
  - nome, indirizzo di fatturazione e numero telefonico del titolare della carta
  - data di arrivo previsto
  - importo dell'acconto
  - data della transazione
  - codice di prenotazione dell'acconto (assegnato dall'hotel)
  - termine ultimo per l'annullamento
  - condizioni di annullamento concordate
  - indicazioni su diritti e doveri nei versamenti di acconti con carte di credito

Registrazione dell'acconto online

Avete questa possibilità se possedete un pacchetto E-Commerce adeguato di SIX Payment Services. Se sì, potete creare un'offerta dell' importo dell'acconto nel backoffice dell'applicazione, che farete pervenire all'ospite via e-mail, o che l'ospite prenoterà sul vostro negozio online.

In entrambi i casi, il vostro ospite sarà reindirizzato alla finestra di pagamento, nella quale potrà inserire i dati della propria carta. Dopodiché, l'ospite sarà invitato a immettere la propria password nella finestra 3-D-Secure, così potrete assicurarvi che l'ospite abbia eseguito la prenotazione personalmente. Nel backoffice potete visionare ed elaborare la prenotazione effettuata.

Annullamento al terminale di pagamento e online:

- comunicate al titolare della carta il codice di annullamento (assegnato dall'hotel) e ricordategli di conservare il codice per eventuali chiarimenti
- sulla conferma di versamento dell'acconto, apporre la nota «cancelled» e il codice di annullamento
- calcolate l'importo da rimborsare
- eseguite un accredito al terminale di pagamento
- inviate all'ospite entro tre giorni lavorativi una copia delle due ricevute (ricevuta di prenotazione Advance Deposit e ricevuta di accredito dell'annullamento) accompagnata da un testo che spiega che è stato eseguito un accredito

Importante

In linea di principio, l'ospite ha diritto alla camera o categoria di camera da lui prenotata. Se la camera prenotata dal cliente non è disponibile al suo arrivo, siete obbligati ad accreditargli tutto l'acconto versato.

Le transazioni svolte mediante registrazione manuale dei dati della carta comportano rischi a carico dell'hotel. In particolare quando a posteriori dovesse risultare che i dati della carta sono stati utilizzati abusivamente senza il consenso del titolare della carta. Potete ridurre notevolmente i rischi elaborando online il versamento dell'acconto.

Addebiti posticipati (Late Charges)

Procedura corretta

Se dopo il check-out constatate che nel conteggio finale si sono originati costi non considerati, potete addebitare la carta di credito in un secondo momento.

Prenotazione/Check-in

Per effettuare addebiti posticipati, dovete spiegare al cliente, al più tardi check-in, le Condizioni generali di contratto e i relativi costi aggiuntivi. Per questo, vi consigliamo di far firmare all'ospite, preferibilmente durante la prenotazione, una dichiarazione di consenso, in cui egli acconsente alle condizioni di annullamento e alle CGC.

Dopo la partenza

- eseguire una «prenotazione» al terminale di pagamento
- segnare «Signature on File» nella riga della firma
- se la prenotazione o l'autorizzazione vengono negate, contattate il titolare della carta e chiedetegli un altro metodo di pagamento
- inviate al titolare della carta le seguenti informazioni:
  - copia della ricevuta con la nota «Signature on File» nella riga della firma
  - copia della(e) fattura(e) sui costi aggiuntivi dettagliati per esteso

Importante

I costi aggiuntivi registrati successivamente devono riferirsi solo alla camera, al cibo o alle bevande. Queste registrazioni supplementari possono aumentare l'importo della fattura alberghiera al massimo del 15%.

Se i costi aggiuntivi ammontano a oltre il 15% o se si generano costi a causa di perdita, furto o danni nella camera d'hotel, questi possono essere registrati solo se avrete contattato ancora l'ospite dopo la partenza e vi sarete accordati con lui. Il consenso ad addebitare questi costi sulla carta deve essere presente in forma scritta.

Protezione efficace dei dati della carta grazie a PCI DSS

Il Payment Card Industry Data Security Standard (PCI DSS) è un regolamento nel sistema di pagamento elettronico che si riferisce allo svolgimento in sicurezza di transazioni con carte e il cui rispetto viene richiesto tassativamente dalle maggiori organizzazioni di carte – Visa, Mastercard, JCB International, American Express e Discover Financial Services. Il regolamento viene pubblicato e perfezionato dal Payment Card Industry Security Standards Council.

Tutte le aziende che archiviano, trasmettono o elaborano dati di carte devono rispettare le direttive di sicurezza di questo regolamento. Se i requisiti non vengono rispettati, le organizzazioni di carte possono vietare in ultima istanza l'accettazione di pagamenti con carta.

Il regolamento ha lo scopo di proteggervi dalle conseguenze spiacevoli di un furto dei dati di una carta; una perdita di dati di una carta è legata, oltre che a perdite finanziarie, anche a danni per la reputazione.

Questo regolamento è costituito da dodici gruppi di requisiti e si riferisce all'infrastruttura IT, ai processi e ai collaboratori del vostro hotel:

Requisito 1: installazione e mantenimento di una configurazione di firewall per la protezione dei dati dei titolari di carte

Requisito 2: non utilizzare nessuna delle impostazioni standard per password di sistema e altri parametri di sicurezza forniti dal gestore

Requisito 3: protezione di dati archiviati dei titolari di carte

Requisito 4: crittografia dei dati dei titolari di carte quando vengono trasmessi in reti pubbliche aperte

Requisito 5: protezione di tutti i sistemi da malware e aggiornamento regolare di software antivirus e programmi

Requisito 6: sviluppo e manutenzione di sistemi e applicazioni sicuri

Requisito 7: limitazione dell'accesso a dati di titolari di carte a seconda del bisogno di informazioni commerciali

Requisito 8: identificazione e autenticazione dell'accesso a componenti di sistema

Requisito 9: limitare l'accesso fisico a dati di titolari di carte

Requisito 10: perseguimento e monitoraggio di tutto l'accesso a risorse di rete e dati di titolari di carte

Requisito 11: collaudo regolare dei sistemi e processi di sicurezza

Requisito 12: mantenimento di una direttiva di sicurezza delle informazioni per tutto il personale.

Il rispetto dei requisiti viene controllato mediante tre misure di validazione:

– gli hotel con più di 6 mln di transazioni l'anno o partner contrattuali che sono stati vittime di un furto di dati di carta eseguono un On-Site Audit. Questo deve essere eseguito da un auditor specializzato oppure da un'impresa di certificazione accreditata (QSA – Qualified Security Assessor).
– gli hotel con meno di 6 mln di transazioni l'anno possono dichiarare il rispetto delle direttive mediante un questionario di autovalutazione (SAQ – Self-Assessment Questionnaire). A seconda della forma di accettazione della carta esistono versioni corrispondenti di questo documento SAQ.
– Per hotel la cui infrastruttura viene a contatto con dati di carta esistono inoltre i cosiddetti network scans. Ogni trimestre e dopo essersi accordato con voi, un ASV (Approved Scanning Vendor) eseguirà attacchi di hackeraggio amichevoli allo scopo di rilevare tempestivamente eventuali punti deboli.

Andare sul sicuro

In riferimento alla sicurezza sono ambite soluzioni che escludono che il vostro hotel venga a contatto con dati di carta completi e non criptati. Così potete assicurarvi che la vostra certificazione sia molto meno impegnativa.

I seguenti suggerimenti vi aiutano a ridurre il rischio di un furto di dati da carte e l'impegno della certificazione:

Server PCI Proxy

Le piattaforme di prenotazione sono partner di distribuzione importanti. Sfortunatamente, non tutte sono sempre sicure: spesso, trasmettono dati sensibili non crittografati – per e-mail o tramite interfacce XML.

In tal caso, il dispendio per adempiere alle disposizioni di sicurezza PCI DSS aumenta notevolmente. Per evitare questo dispendio aggiuntivo, esiste un'alternativa semplice e vantaggiosa: il server PCI Proxy. Questo server intercetta i dati di carte diretti a voi dalla piattaforma di prenotazione e li sostituisce con un numero casuale non identificabile (token). I relativi dati sensibili della carta vengono salvati in un ambiente certificato a norma PCI DSS. Ciò vi offre il vantaggio di una validazione più semplice e la possibilità di eseguire tranquillamente prenotazioni su portali.

Software alberghiero – Property Management System (PMS)

Verificate se il vostro software alberghiero è certificato in conformità allo standard PA-DSS (Payment Application Data Security Standard). In tal modo, potete essere certi che i dati delle carte di pagamento siano archiviati in maniera criptata secondo i parametri. Vi consigliamo di contattare il vostro provider di PMS.

Outsourcing

Se non potete rinunciare al salvataggio elettronico di dati di carte, chiarite con il vostro fornitore di servizi la possibilità di un'esternalizzazione (outsourcing). Se il fornitore di servizi si assume il salvataggio di dati di carte di pagamento, dovrà soddisfare tutti i requisiti attinenti allo standard PCI DSS. Richiedete il corrispondente documento dimostrativo (certificato). Assicuratevi che il vostro partner e fornitore di servizi ottemperi alla certificazione PCI.

Portale web SAQ

SIX Payment Services opera in cooperazione con un partner un portale web SAQ (Self-Assessment Questionnaire).

Il portale vi conduce gradualmente attraverso tutti i processi necessari per la certificazione PCI DSS. Nell'archivio documentale del portale è possibile anche visualizzare e scaricare tutti i documenti prodotti durante l'esecuzione, come l'attestato di certificazione, il Self-Assessment (autovalutazione) e, se pertinente per voi, i risultati delle scansioni della rete.

Il portale è disponibile gratuitamente per tutti i clienti SIX.

In caso di domande tecniche o riguardanti i contenuti, vi invitiamo a rivolgervi direttamente al team PCI di SIX: pci-support.ch@six-payment-services.com

Secure PayGate

Se accettate prenotazioni via telefono, fax, e-mail o posta, i vostri ospiti possono pagare anticipatamente online in modo rapido, comodo e sicuro, senza che il vostro hotel venga a contatto con dati di carte di pagamento. La soluzione si chiama Secure PayGate.

Secure PayGate coniuga i vantaggi della cosiddetta transazione Mail/Phone Order con la sicurezza di una transazione Secure E-Commerce protetta da password. Ciò comporta per voi maggiore sicurezza e comodità di svolgimento.

Potete trovare maggiori informazioni su Secure PayGate su: **www.paymentforyou.com**

Suggerimento

Offrite ai vostri ospiti il pagamento con la procedura 3-D Secure.
Così vi assicurate in qualità di hotel che l'ospite abbia eseguito lui stesso la prenotazione, per cui il carico della responsabilità s'inverte a vostro favore.

La crescita costante della criminalità informatica continua a porre nel mirino dei truffatori anche il settore alberghiero. Dall'analisi degli episodi è risultato che gran parte degli attacchi avrebbe potuto essere sventata con i giusti meccanismi di sicurezza. I seguenti suggerimenti presi dallo standard di sicurezza internazionale PCI DSS sono importanti per voi quando dati di carte di pagamento si trovano sulla vostra infrastruttura (si raccomanda comunque la verifica anche indipendentemente da PCI DSS):

1. Modificate le impostazioni predefinite

I sistemi PMS e POS vengono configurati spesso da integratori con password standard. Se un criminale arriva a tale password, può facilitarsi l'accesso ai vostri sistemi. Per questo, non utilizzate mai la password standard fornita dal vostro provider. Prima dell'installazione di un'applicazione, definite una nuova password di complessità elevata: utilizzate caratteri maiuscoli e minuscoli oltre a numeri e caratteri speciali. La password deve essere lunga almeno otto caratteri.

2. Impostate il firewall in modo sicuro

Configurate il firewall in modo che il traffico di dati in entrata e in uscita sia limitato a quei servizi che sono necessari per l'esercizio dell'attività. Rendete i vostri sistemi PMS e POS non direttamente accessibili via Internet. Bloccate il traffico dei dati in entrata e filtrate quello dei dati in uscita. Questa misura limita notevolmente le attività di un aggressore.

3. Segmentazione di rete

Segmentate la vostra rete: impedite la comunicazione fra i sistemi che processano carte di pagamento e altri sistemi tramite firewall e router. Lo scopo è quello di vietare l'accesso diretto ai sistemi che elaborano carte di pagamento e ridurre così al minimo il rischio di un trafugamento di dati. Una rete non segmentata significa inoltre che occorre applicare lo standard PCI DSS a tutta la rete.

4. Installate un'autenticazione multifattore

Approntate un'autenticazione multi-fattore per tutte le soluzioni di accesso remoto, sia per i collaboratori interni che per i fornitori di servizi. La protezione con solo una password il più delle volte non basta a fermare i criminali. Combinate l'autenticazione via password con altri metodi: l'impiego di certificati PKI (Public Key Infrastructure) o token hardware è già diffuso oggi in molte imprese. Informatevi presso il vostro fornitore di soluzioni su possibili integrazioni.

5. Verificate i log

Assicuratevi di creare, monitorare e salvare i protocolli di eventi (log). Non pensate che i criminali agiscano solo di nascosto. Le vostre attività vengono registrate spesso nei log. Verificateli regolarmente, così potrete individuare precocemente il rischio e ridurlo al minimo.

6. Gestione di stampe e ricevute cartacee

Assicuratevi di conservare sotto chiave stampe, fax, ricevute contenenti dati di carte – in cassetti o armadi. I dipendenti devono essere sensibilizzati sulla gestione corretta di questi dati riservati ed è necessario definire e controllare quali dipendenti necessitino di accedere a questi documenti per espletare le propria attività. È necessario garantire inoltre lo smaltimento adeguato dei documenti.

7. Fornitori di servizi

Contattate i vostri fornitori di servizi che per vostro incarico trasmettono, elaborano o archiviano dati di carte e chiedete un attestato di conformità PCI. È necessario disciplinare la responsabilità congiunta. Tenete un elenco dei vostri fornitori di servizio per tenere la situazione sotto controllo.

Domande

Se avete domande in materia di sicurezza, il vostro provider di PMS e il team PCI di SIX saranno lieti di aiutarvi.

Payment Services

Dichiarazione di consenso
Autorizzazione per carte di credito (modello)

Con una dichiarazione di consenso, l'ospite manifesta il proprio accordo a eseguire eventuali prenotazioni legittime senza presentare fisicamente la carta. Qui di seguito troverete un modello corrispondente.

Nome del vostro hotel / Logo del vostro hotel: _____

Questo modulo deve essere custodito in un ambiente sicuro.

Kreditkarten-Autorisierung / Prise en charge / Credit Card Authorization

Karteninhaber / Nom du détenteur de la carte / Credit Card Holder _____ Zimmer / Chambre / Room _____

☐ Zahlung / Payment
oder / ou / or
☐ Garantie / Guarantee

Kartentyp / Type ☐ Visa ☐ Mastercard ☐ American Express ☐ Diners ☐ JCB ☐ UnionPay

Nummer / Numéro / Number _____ Verfallsdatum / Expiration _____

Für folgende Services / Pour les services suivants / For the following charges

Zimmer und Taxen / Chambres et Taxes / Room and Tax ☐
Express Check-Out ☐
Frühstück / Petit-déjeuner / Breakfast ☐
Übrige Gebühren / Autres charges / All incidentals ☐
Pagamento in valuta della carta (DCC - Dynamic Currency Conversion)* ☐

* Con la procedura DCC, il vostro pagamento sarà eseguito nella valuta della carta invece che nella valuta locale dell'hotel sopra indicato. Apponendo una crocetta sul servizio, date facoltà all'hotel su indicato di addebitare i pagamenti riportati nel presente documento nella valuta della carta. Il cliente è consapevole del fatto che sia l'importo finale da saldare, sia il cambio applicato al momento della firma della presente dichiarazione di consenso non sono ancora noti.

Für folgende Gäste / Pour les hôtes suivants / For the following guests

Name / Nom / Name _____ Zimmer / Chambre / Room _____
Name / Nom / Name _____ Zimmer / Chambre / Room _____
Name / Nom / Name _____ Zimmer / Chambre / Room _____

Hiermit bestätige ich, dass nebst meiner Zimmerrechnung auch die auf diesem Formular markierten Zusatzkosten sowie die Zimmerrechnung für die anderen aufgeführten Gäste gemäss den allgemein gültigen Geschäftsbedingungen des Hauses zu Lasten meiner oben erwähnten Kreditkarte abgebucht werden dürfen.

Par la présente je confirme qu'en plus de la facture pour ma chambre, vous pouvez également déduire les coûts supplémentaires ainsi que les frais des chambres de nos invités figurant sur les documents joints. Selon les conditions générales nous vous autorisons à débiter ma carte de crédit mentionnée.

I hereby confirm that, excepting my room costs, the additional costs marked above and room costs for the other guests listed on this document can be charged to my above mentioned creditcard in accordance to the general business terms and conditions.

_____ _____
Ort, Datum / Lieu, date / Place, date Vorname, Name / Nom, prénom / Forename, last name

_____
Unterschrift / Signature

SIX Payment Services SA
Hardturmstrasse 201
Casella postale
CH-8021 Zurigo

Accordo per la protezione dei dati (campione)

In calce è riportato un esempio non vincolante di un possibile accordo per la protezione dei dati. Per avere una versione giuridicamente corretta vi preghiamo di rivolgervi ad un legale di vostra scelta.

La/Il sottoscritta/o, in base agli obblighi di riservatezza previsti contrattualmente e per legge, è tenuta/o a non rivelare fatti/informazioni di cui sia venuta/o a conoscenza o che siano stati comunicati nell'esercizio della sua attività presso l'*Hotel XY,* che non fossero di pubblico dominio, per i quali sussiste un interesse alla riservatezza e la confidenzialità dei quali, espressamente o tacitamente, rientri nella volontà dell'*Hotel XY*.

– Rientra nel segreto commerciale ogni informazione relativa all'oggetto, al contenuto e al funzionamento di mezzi e dispositivi tecnici o basati su software dell'*Hotel XY* e relativa all'organizzazione e allo svolgimento di ogni tipo di attività dell'*Hotel XY*.
– In particolare devono essere protetti tutti i dati personali dei clienti, inclusi i dati relativi alle carte di credito e di debito.

La violazione dell'obbligo di riservatezza può costituire, singolarmente o in forma cumulativa, una violazione del segreto d'affari o della legge di tutela dei dati personali. La relativa disposizione di legge è riportata in allegato a questa dichiarazione di riservatezza.

La/il sottoscritta/o è tenuta/o a considerare assolutamente confidenziali i fatti/le informazioni rilevanti dal punto di vista della riservatezza di cui sia venuta/o a conoscenza e a non utilizzarli per scopi diversi da quelli legati al compito affidatogli.

Luogo e data

Nome

Firma

1100116 CHE_IT/01.2018

Vi offriamo consulenza riguardo la soluzione per i pagamenti senza contanti più adatta a voi.

Per l'elenco degli interlocutori locali vi rimandiamo a www.six-payment-services.com/contatto

SIX Payment Services SA
Hardturmstrasse 201
Casella postale
CH-8021 Zurigo

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

SIX Payment Services (Austria) GmbH
Marxergasse 1B
AT-1030 Vienna
Austria

SIX Payment Services (Europe) S.A.
Succursale Germania
Theodor-Heuss-Allee 108
D-60486 Francoforte sul Meno