protel SPE / MPE

Fragen und Antworten zu PCI und protel

Warum ist PCI wichtig für mich als Hotelier?

Die “Payment Card Industry Data Security Standards” – kurz PCI DSS – sind die weltweit gültigen Sicherheitsstandards für den bargeldlosen Zahlungsverkehr der führenden internationalen Kreditkartenorganisationen. Dieser IT-Sicherheitsstandard definiert technische und betriebliche Anforderungen für die sichere Speicherung, Verarbeitung und Übermittlung von Karteninhaberdaten und ist für alle Unternehmen verbindlich, die im Zahlungsverkehr mit Kreditkartendaten arbeiten.

Die Einhaltung der Standards wird von den führenden Kartenorganisationen zwingend verlangt. Hotels, die sich nicht an diese Standards halten und sich nicht zertifizieren lassen, können im Schadensfall haftbar gemacht und von den Kreditkartenorganisationen in Regress genommen werden. Um gar nicht erst Gefahr zu laufen, sich mit Schadensersatzansprüchen und möglichen Reputationsschäden beschäftigen zu müssen, sollte ein Hotel den eigenen Betrieb PCI-DSS zertifizieren lassen. Die eigene Zertifizierung nach dem PCI Data Security Standard kann die Haftungsfrage im Schadensfall erheblich beeinflussen, wenn nachgewiesen werden kann, dass alle PCI-Sicherheitsstandards zum Zeitpunkt des Zwischenfalls eingehalten wurden.

Wer ist für die Erfüllung der PCI-Anforderungen verantwortlich?

Die Verantwortung für die Erfüllung und Einhaltung des PCI-Standards tragen alle Unternehmen, die Kreditkartenzahlungen akzeptieren. Möchte ein Betrieb konform zu den Anforderungen des PCI-Standards arbeiten, unterstützen ihn die Produkte und Dienstleistungen von protel dabei.

Ist mein Betrieb automatisch PCI konform, wenn ich mein protel PMS PCI-konform betreibe?

Nein, protel liefert Ihnen eine Softwarelösung, welche Ihnen die Möglichkeit zum PCI-konformen Arbeiten mit Ihrem protel PMS gibt. Um komplett PCI compliant zu sein, müssen alle Arbeitsprozesse und Abläufe im Hotel durchleuchtet und die gesamte IT-Umgebung hinsichtlich der PCI-Anforderungen überprüft werden. Hierbei helfen Ihnen Datenschutzbeauftragte mit Beratung und Umsetzungsvorschlägen.

Wie zertifiziert sich ein Betrieb nach PCI-DSS?

Die Zertifizierung eines Betriebs erfolgt nach einem SAQ genannten Selbstbeurteilungsfragebogen (Self Assessment Questionnaire). Es gibt unterschiedliche SAQ, die sich nicht nur anhand der Anzahl der Fragen unterscheiden, sondern auch darin, ob bzgl. der im Hotel verwendeten Geräte (PCs, Bezahlterminals, Internetverbindung, etc.) zusätzliche Voraussetzungen zu erfüllen sind. Im günstigsten Fall – nämlich bei Einsatz eines protel Interfacings zu einem P2PE Cloud-Bezahlsystem – kann der Nachweis durch einen jährlich auszufüllenden SAQ der niedrigeren Kategorie erfolgen (weitere Informationen zu Cloud-Bezahlsystemen siehe Abschnitt „Interfaces zu elektronischen Bezahlsystemen“).

Wie funktioniert PCI-DSS in protel?

Eine zentrale PCI DSS-Bestimmung ist das Verbot der unverschlüsselten Speicherung von Kreditkartendaten im Hotel. Um in den protel-Produkten keine Kreditkartendaten speichern zu müssen, wird ein "Tokenisation" genanntes Verfahren eingesetzt. Hierbei werden Kreditkartendaten in einem besonders geschützten und PCI-zertifizierten Bereich des protel Cloud Centers verschlüsselt gespeichert, zusammen mit einem zufälligen Ersatzwert - dem Token. Im protel PMS wird anstelle der Kreditkartennummer *nur das Token* abgebildet.

Wie sicher sind Kreditkartendaten im protel Cloud Center (pCC)?

Der besonders geschützte Bereich des pCC ist gemäß PCI-DSS-Standard zertifiziert und somit gegen kriminelle Angriffe bestmöglich geschützt. Die jährlich stattfindende erneute Prüfung stellt sicher, dass auch die neuesten Erweiterungen des Standards erfüllt werden.

Was passiert bei der Umstellung auf Tokenisation?

Bei der Umstellung des protel PMS auf den Betrieb mit Tokenisation werden Kreditkartendaten vollständig aus dem protel PMS entfernt und durch ein Token ersetzt, d.h. es werden *keine Kreditkartendaten im protel PMS gespeichert*. Die erfolgreich gegen ein Token ersetzte Kreditkartennummer ist verschlüsselt im geschützten und zertifizierten Bereich des protel Cloud Centers (pCC) gespeichert. Im protel PMS wird die Kreditkartennummer bis auf einige Ziffern unkenntlich gemacht.

Was passiert mit Kreditkartendaten, die bereits im PMS sind?

Für vorhandene Kreditkartendaten hat protel ein spezielles Validierungs- und Cleanup-Tool entwickelt. Alle validen Kreditkartendaten im Datenbestand des protel PMS werden im Rahmen der PCI-Umstellung verschlüsselt, in ein Token umgewandelt und aus der protel Datenbank gelöscht. Nicht valide Kreditkartendaten können in Zusammenarbeit mit dem Hotelier korrigiert und bereinigt werden. Kreditkartendaten, die sich in nicht dafür vorgesehenen Freitextfeldern (z. B. Adressfelder, Gastwünsche, Notizfelder etc.) "verstecken", werden bis auf einige Ziffern unkenntlich gemacht (maskiert), sodass keine lesbaren Kreditkartennummern in protel verbleiben. Derart maskierte Daten können nicht mehr genutzt oder wiederhergestellt werden.

Wie werden Kreditkarteninformationen gespeichert?

Token können in protel mit Bezug zur Reservierung oder auch mit Bezug zur Gästekartei gespeichert werden. Bei lediglich reservierungsbezogener Speicherung wird das Token nach einer konfigurierbaren Anzahl von Tagen nach Check-out aus dem protel PMS gelöscht. Die Speicherung mit Bezug zu einer Gästekartei ist für Betriebe mit vielen Stammgästen die bevorzugte Methode, um bei neuen Reservierungen die Details zum hinterlegten Zahlungsmittel nicht noch einmal erfassen zu müssen.

Wer darf die Tokens entschlüsseln?

Nur protel-Benutzer mit den nötigen Zugriffsrechten dürfen die für ein Token gespeicherte Kreditkartennummer entschlüsseln und anzeigen lassen. Welche protel-Benutzer das sind, bestimmen Sie. Hierzu werden die protel-Benutzer als Cloud-User im protel Cloud Center angelegt. Für die Anlage der Cloud-User werden die individuellen E-Mail-Adressen der Benutzer benötigt, es dürfen keine gemeinsamen E-Mail-Konten benutzt werden.

Wie kann ich nach der PCI-Umstellung von protel auf Kreditkartendaten zugreifen?

Um auf Kreditkartendaten manuell zuzugreifen, kann sich der Hotelmitarbeiter in einer gesicherten Verbindung über seinen Web-Browser im protel Cloud Center einloggen. Dort ermöglicht der Detokenizer den sicheren Zugriff auf die Kreditkartendaten. Restriktive Zugriffsrechte kontrollieren den Zugriff, d.h. nur diejenigen, die tatsächlich mit den Kreditkartendaten arbeiten und über die nötigen Rechte verfügen, sind autorisiert darauf zuzugreifen.

Muss ich besondere Einstellungen in den protel Stammdaten vornehmen?

Alle im Hotel akzeptierten Kreditkarten (Mastercard, Visa, etc.) müssen in protel als CC-Zahlart aufgesetzt und online verfügbar sein. Alle anderen Einstellungen übernimmt protel für Sie.

Wie kann ich nach der PCI-Umstellung Kreditkartendaten erfassen?

Grundsätzlich gilt: Kreditkartendaten können nicht mehr direkt im protel Front Office erfasst werden!

Um Kreditkartendaten manuell zu erfassen, kann sich der Hotelmitarbeiter in einer gesicherten Verbindung über seinen Web-Browser im protel Cloud Center anmelden. Unter Angabe der Reservierungs- bzw. Gästekarteinummer können Kreditkartendaten dort im Tokenizer erfasst werden, welcher die Daten verschlüsselt im geschützten und zertifizierten Bereich des protel Cloud Centers speichert, zusammen mit einem erzeugten Ersatzwert - dem Token. Natürlich kann der Zugriff auf diese Funktion auf bestimmte Mitarbeiter beschränkt werden.

Alternativ zur manuellen Erfassung ermöglicht das protel Interface zu Cloud-Bezahlsystemen die PCI-konforme Erfassung von Kreditkartendaten über ein Kreditkartenterminal (siehe unten: „Interfaces zu elektronischen Bezahlsystemen“).

Was ändert sich nach der PCI-Umstellung in der Ansicht von protel?

Grundsätzlich gilt: Es gibt keine unverschlüsselten oder lesbaren Kreditkartendaten mehr im Front Office! Die verschlüsselten Kreditkartendaten werden im Navigator angezeigt. Die Kreditkartennummern werden bis auf einige Ziffern durch ein „x“ ersetzt gemacht (Beispiel: xxxxxxxxx7203 0120).

Die Funktion zur Erfassung von Kreditkartendaten im Reservierungsdialog wird deaktiviert. Im gesamten System werden keine lesbaren Kreditkartendaten mehr hinterlegt sein!

Bleibt mein protel PMS nach der PCI-Umstellung auf Dauer PCI compliant?

Das hängt davon ab, ob Sie und Ihre Mitarbeiter PCI-konform in protel arbeiten. Wenn vereinzelte Mitarbeiter zum Beispiel Kreditkartendaten an nicht bestimmungsgemäßen Stellen in protel eintragen (Notizfeld, Gastwünsche, etc.), stellt dies einen klaren Verstoß gegen die PCI-Bestimmungen dar. Es bedarf also entsprechender Arbeitsanweisungen und Richtlinien, damit sich jeder Mitarbeiter des sicheren Umgangs mit Kreditkartendaten in protel bewusst ist. Sofern Kreditkartendaten von Hand erfasst werden müssen, sorgen Sie dafür, dass die Daten ausschließlich über den protel Tokenizer im protel Cloud Center eingegeben werden!

Wie lang kann ich während der PCI Umstellung nicht mit protel arbeiten?

In der Zeit, in der die Konvertierung der Kreditkartendaten läuft, kann in protel weitergearbeitet werden, sofern keine Operationen ausgeführt werden, bei denen Kreditkartendaten eingesehen, verändert oder gespeichert werden. Die Zeit für die Konvertierung fällt je nach Größe des Datenbestands unterschiedlich aus. Rechnen Sie mit etwa 4 bis 6 Stunden für protel SPE und etwa 8 bis 12 Stunden bei protel MPE (Hotelketten).

protel Interfaces zu elektronischen Bezahlsystemen

Welche protel Interfaces zu Bezahlsystemen unterstützen einen Betrieb konform zu PCI-DSS?

protel bietet Interfaces zu Bezahlsystemen vor Ort oder zu Cloud-Bezahlsystemen an.

Bezahlsysteme vor Ort. Ob ein protel Interface zu einem Bezahlsystem vor Ort PCI-konform betrieben werden kann, hängt von der jeweiligen Betriebsart ab:

1. Wenn das Bezahlsystem **eine maskierte Kartennummer** an protel übergibt, werden keine lesbaren Kreditkartendaten in protel gespeichert. **Diese Betriebsart kann nach PCI-DSS zertifiziert** werden.
   Nachteil: Für jede erneute Transaktion mit derselben Kreditkartennummer (z. B. Korrekturen nach Check-out, No-Show-Belastungen, Einlösen von Zahlungsgarantien) muss die Kreditkarte des Gastes erneut in ein Bezahlterminal gesteckt werden (d.h. der Gast muss anwesend sein).
2. Wenn das Bezahlsystem **eine vollständige Kartennummer** an protel übergibt, verschlüsselt das Interface die Kartennummer und speichert sie in protel. Da nicht alle Vorgaben an die Verschlüsselung erfüllt werden, **kann diese Betriebsart nicht nach PCI-DSS zertifiziert werden**.

Cloud-Bezahlsysteme. Das protel Interface zu Cloud-Bezahlsystemen kann ohne Funktionseinschränkung PCI-konform mit dem protel PMS betrieben werden. Weil das Interfacing zwischen zwei sicheren Rechenzentren - dem protel pCC auf der einen und dem Rechenzentrum des Bezahlsystems auf der anderen Seite - betrieben wird, kann sich ein Hotel mit einem solchen Bezahlsystem und Interfacing sogar **selbst nach PCI-DSS zertifizieren**, wenn es sich bei dem angebundenen Bezahlsystem um eine P2PE (point-to-point encryption) Lösung handelt. In diesem Fall muss lediglich ein Selbstbeurteilungsbogen (SAQ) der niedrigeren Kategorie ausgefüllt werden, um PCI compliant zu werden.

Darüber hinaus können Sie bei einem Interfacing zu einem *Cloud-Bezahlsystem* sämtliche Transaktionen ausführen ohne das Token entschlüsseln zu müssen, d. h., es können im Bedarfsfall Kreditkarten-Transaktionen ausgeführt werden, ohne dass der Gast für jede Transaktion dessen Karte in ein Kartenterminal stecken muss (z.B. No-Show). Aktuell ist ein PCI-konformes Interfacing zu einem *Cloud-Bezahlsystem* mit dem Anbieter *3C Payments* möglich. protel steht in Kontakt mit weiteren Bezahldienstleistern, dazu gehören im deutschsprachigen Raum hauptsächlich die Firmen CCV und BS-PayOne. CCV ist ein Dienstleister, der eng mit der Firma Concardis zusammenarbeitet, mit der viele protel Kunden eine Geschäftsbeziehung pflegen.

Fragen und Antworten zu angeschlossenen Buchungsportalen

Was muss ich beim Einsatz einer IDS-Schnittstelle beachten?

Grundsätzlich kann jedes IDS-Interfacing konform zu PCI-DSS betrieben werden. protel bietet dazu einen Dienst im pCC an, der für die Kommunikation mit Buchungsportalen die Kreditkartennummern aus den vermittelten Reservierungen gegen ein Token ersetzt und die Kreditkartennummern im pCC verschlüsselt ablegt. Auch hier werden dann im protel PMS lediglich die Tokens gespeichert. Die Tokens können dann im Bedarfsfall – z.B. No-Show – verwendet werden. Fragen Sie unser Sales-Team, ob ein Betreiber eines Buchungsportals Kreditkartennummern liefert oder nicht.

Fragen und Antworten in Verbindung mit der protel WBE

Mit welcher WBE-Version kann ich PCI-compliant arbeiten?

Für den PCI-konformen Betrieb mit protel sind die WBE5 oder die WBE4 erforderlich.

Sind Kreditkartendaten, die über die WBE einlaufen, sicher?

Ja. Alle Kreditkartendaten, die über die protel Web Booking Engine einlaufen, gegen ein Token ersetzt und die Kreditkartennummern im pCC verschlüsselt ablegt.

Was ist bei Einbindung eines Bezahldienstleisters zu beachten?

Wenn der durch den Gast zu bezahlende Betrag bereits zum Buchungszeitpunkt zu entrichten ist, wird im Buchungsprozess - wie bei anderen Online-Shops auch - zwecks Bezahlung auf die Seite des Bezahldienstleisters gewechselt. Von dort aus gelangt man nach erfolgreicher Bezahlung wieder zurück zur protel WBE. Für eine so durchgeführte Zahlung werden keine Informationen über das verwendete Zahlungsmittel an protel übergeben. Die in protel dargestellte Zahlung enthält daher keine schützenswerten Informationen.

Wie werden Kreditkartendaten über die protel WBE behandelt?

Ob eine Erfassung von Kreditkartendaten als Sicherungsinformation erfolgt, wird mit Einstellungen in der WBE bestimmt und ist davon abhängig, welcher Preistyp für die Buchung zur Anwendung kommt. Vor Abschluss der Buchung wird der Gast im Browser auf eine sichere Seite im protel Cloud Center geleitet, gibt dort seine Kreditkarteninformationen ein und gelangt anschließend wieder zurück zur protel WBE. Aus den erfassten Kreditkarteninformationen wird die Kartennummer verschlüsselt, gespeichert und gegen ein Token ersetzt. Die im protel PMS angelegte Karteninformation enthält lediglich das Token.

Fragen und Antworten in Verbindung mit POS-Systemen

Was ist bei Einbindung eines POS-Systems zu beachten?

Bei einem Interfacing zwischen POS und protel werden keine Kreditkartennummern an das protel PMS übermittelt.