more security. usd

ConCardis

Kreditkartensicherheit für Hotels

Wie PCI DSS die Geschäftstätigkeit nachhaltig sichert

ConCardis GmbH
Helfmann-Park 7
65760 Eschborn

www.concardis.com

more security. usd

Inhaltsverzeichnis

1. Angriffsziel: Kreditkarteninformationen

1.1. Wozu PCI DSS?

Kreditkartendaten sind ein sehr begehrtes Ziel für Kriminelle. Sie lassen sich besonders in kleineren Unternehmen leicht erbeuten und relativ unkompliziert in Geld umsetzen. Insbesondere wird häufig die Hotellerie Opfer von Kreditkartendiebstahl. Ob nun professionelle Hacker oder böswillige Insider am Werk sind, die Kriminellen sind meist bestens organisiert und das Geschäft mit gestohlenen Kreditkarteninformationen floriert.

Wird ein Diebstahl von Kreditkarteninformationen aufgedeckt, so zieht dies zunächst einmal kostspielige Untersuchungen nach sich. Dem folgen Schadensersatzansprüche und Strafzahlungen. Zu guter Letzt sorgt die Veröffentlichung des Vorfalls durch die Presse für eine Rufschädigung, die kaum noch zu beheben ist. Das Vertrauen der Kunden schwindet und die Geschäftstätigkeit trägt einen nachhaltigen Schaden davon.

Um dem entgegenzuwirken, haben sich die großen Kreditkartengesellschaften zusammengeschlossen und das Payment Card Industry Security Standards Council (PCI SSC) gegründet. Durch die Vereinheitlichung der Sicherheitsleitlinien der einzelnen Gesellschaften entstand der PCI Data Security Standard (PCI DSS). Er stellt die Basis für eine einheitliche Vorgehensweise zum Schutz von Kreditkartendaten dar und umfasst dabei sowohl technische als auch organisatorische Maßnahmen. Werden die Maßnahmen umgesetzt, so sorgt deren Zusammenspiel für ein Mindestmaß an Sicherheit von Kreditkarteninformationen.

Der Nachweis der eigenen PCI DSS-Konformität kann bei Bekanntwerden von Kreditkartendiebstahl die Haftungsfrage erheblich beeinflussen. Dazu muss allerdings bewiesen werden, dass zum Zeitpunkt des Zwischenfalls alle notwendigen Maßnahmen des PCI-Standards umgesetzt und befolgt wurden.

Allerdings nicht zuletzt sollte man als Hotelier nicht aus den Augen verlieren, dass man mit der Sicherheit der Kreditkartendaten seiner Kunden für die Sicherheit seiner Einnahmequelle sorgt und das Image seines Hauses bewahrt.

1.2. Worauf haben es die Kriminellen abgesehen?

Kreditkartendaten befinden sich zunächst einmal auf der Karte in Form von Beschriftung, auf dem Chip und auf dem Magnetstreifen. Die folgende Abbildung zeigt den Aufbau einer typischen Kreditkarte.

1. Chip
2. Kartennummer (Primary Account Number, PAN)
3. Gültigkeitsdatum
4. Name des Karteninhabers
5. Magnetstreifen
6. Kartenvalidierungscode, Prüfziffer

Die von Kriminellen begehrten Bestandteile von Kreditkarten sind vor allem die Kreditkartennummer (PAN) und die Prüfziffer (CVC2/CVV2/…) sowie der komplette Magnetstreifen, um eine illegale Kartenkopie anfertigen zu können. Auf dem blühenden Schwarzmarkt für gestohlene Kreditkarten können diese Informationen relativ einfach zu Geld gemacht werden. Das Risiko für die Kriminellen ist dabei vergleichsweise gering. Sie sind meist bestens organisiert und agieren international. Eine Rückverfolgbarkeit ist so gut wie unmöglich.

Aber was bringen die gestohlenen Informationen? Mit erbeuteten Kreditkartennummern lassen sich problemlos Bezahl-Transaktionen durchführen, für welche die Karte nicht physisch vorhanden sein muss, beispielsweise bei Onlineeinkäufen im Internet. Über ausgeklügelte Wege wird die Ware über Mittelsmänner ausgeliefert oder weiterverkauft.

Werden Bezahlterminals eingesetzt, so besteht die Gefahr, dass diese manipuliert werden und so der Magnetstreifen „kopiert“ wird. Die Daten des Magnetstreifens werden beim Zahlungsvorgang ausgelesen und an den Angreifer übermittelt. Dieser kann die erbeuteten Daten auf eine „Blanko“-Kreditkarte kopieren und diese dann physisch zum Bezahlen verwenden.

Die Maßnahmen des PCI DSS gehen gezielt auf mögliche Angriffswege ein und bieten dadurch ein Mindestmaß an Schutz für Kreditkarteninformationen.

2. Der Weg zur PCI DSS-Konformität

2.1. Wie starten?

Zu Beginn empfiehlt es sich, eine Liste anzufertigen, wo und wie im Hotel Kreditkarteninformationen verarbeitet werden. Dabei sollte berücksichtigt werden, an welcher Stelle und auf welchem Wege die Kreditkarteninformationen in das Hotel kommen, welchen Weg sie innerhalb des Hotels nehmen und wie sie das Hotel gegebenenfalls wieder verlassen.

Geschäftsprozess	Bereich	Medium, das die Kreditkartendaten enthält	Weiterverarbeitung der Kreditkartendaten
Kunde bezahlt mit Kreditkarte den Aufenthalt und übergibt dafür die Kreditkarte dem Mitarbeiter an der Rezeption	Rezeption	Papier	Rezeption zieht die Karte durch das Terminal, gibt sie anschließend dem Kunden zurück und behält einen Papierbeleg, welcher in einem/r verschließbaren Schrank/Schublade aufbewahrt wird
Die über einen Tag gesammelten Papierbelege der Rezeption werden an die Buchhaltung weitergegeben	Rezeption/ Buchhaltung	Papier	Buchhaltung nimmt die Papierbelege entgegen und prüft den Zahlungseingang; anschließend werden die Belege für die Dauer der gesetzlichen Aufbewahrungsfrist archiviert (in verschließbarem Archiv)
Dienstleister holt nach Ablauf der gesetzlichen Aufbewahrungsfrist die Papierbelege zur Entsorgung ab	Buchhaltung/ Archiv	Papier	Dienstleister entsorgt die Papierbelege ordnungsgemäß
Ein Kunde schickt (obwohl das eigentlich nicht gewollt ist) eine Reservierungsanfrage per E-Mail mit seinen Kreditkarteninformationen	Rezeption/ Reservierung	Digital	Die E-Mail wird ausgedruckt und direkt aus dem Postfach gelöscht

Der Vorteil einer solchen Liste ist, dass sie einen Überblick über potentielle Gefahrenbereiche bietet und dadurch gleichzeitig als Ansatzpunkt für die umzusetzenden Maßnahmen genutzt werden kann. Die abgebildete Liste erhebt keineswegs Anspruch auf Vollständigkeit, sondern stellt lediglich eine beispielhafte Auflistung dar.

Ein besonderes Augenmerk sollte auf diejenigen Stellen in der Liste gelegt werden, wo Kreditkartendaten in elektronischer (digitaler) Form vorhanden sind. Auf Rechnern gespeicherte Informationen stellen für Hacker eine leichte Beute dar. Wenn sie sich Zugang zum hotelinternen Netzwerk verschafft haben, können Kreditkartendaten in großen Mengen entwendet werden. Da sie dabei nicht physisch vor Ort sein müssen, ist das Risiko, entdeckt zu werden, für sie relativ gering.

Aufgrund des hohen Risikos, dem Kreditkartendaten in digitaler Form ausgesetzt sind, schreibt der PCI-Sicherheitsstandard sehr umfangreiche Maßnahmen vor, um diese angemessen zu schützen. Die Menge der umzusetzenden Maßnahmen zum Schutz von Kreditkarteninformationen und damit der Aufwand zur Erreichung der PCI DSS-Konformität kann erheblich reduziert werden, wenn auf jegliche elektronische Speicherung verzichtet wird!

Deshalb sollte in diesem Zusammenhang die Frage geklärt werden, ob Kreditkarteninformationen wirklich in elektronischer Form gespeichert werden müssen oder ob darauf verzichtet werden kann.

Beispielsweise erhalten Hotels häufig E-Mails von Kunden, die Kreditkartendaten enthalten. Werden diese nicht umgehend gelöscht, so gilt dies als elektronische Speicherung von Kreditkartendaten. Die Problematik kann umgangen werden, indem die fraglichen E-Mails ausgedruckt werden und die Kreditkartendaten nur auf dem Papier weiterverarbeitet werden. Dann kann die E-Mail sofort nach dem Ausdrucken vollständig vom Rechner gelöscht werden. Dies beinhaltet auch das Entleeren des Papierkorbs bzw. „Gelöschte Objekte“-Ordners!

Generell gilt: Wenn eine elektronische Speicherung von Kreditkartendaten nicht notwendig ist, sollte auf jeden Fall darauf verzichtet werden!

2.2. Warum ist der Nachweis der eigenen PCI DSS-Konformität wichtig?

In vielen Fällen von Kreditkartendiebstahl wird in anschließenden Untersuchungen immer wieder festgestellt, dass eine oder mehrere der geforderten PCI DSS-Maßnahmen nicht umgesetzt wurden. Die Konsequenzen solcher Vorfälle bestehen u.a. aus Schadensersatzansprüchen, Strafzahlungen, Reputationsschädigung und damit Kundenverlust.

Ein solcher Vorfall kann also erheblichen Schaden verursachen und zu einer nachhaltigen Beeinträchtigung der Geschäftstätigkeit führen.

2.3. Nachweis der PCI DSS-Konformität anhand von Selbstbeurteilungsfragebögen

Die Selbstbeurteilungsfragebögen (engl. Self-Assessment Questionnaire, SAQ) stellen für kleine Unternehmen eine praktikable und effiziente Form zum Nachweis der PCI DSS-Konformität dar. Je nach Geschäftsmodell sind die SAQ auf die jeweiligen Bedürfnisse angepasst. Der SAQ ist einmal pro Jahr auszufüllen und einzureichen. Dies gibt die Möglichkeit, die eingeführten Maßnahmen zu überprüfen und/oder auf möglicherweise stattgefundene Veränderungen in den Geschäftsabläufen zu reagieren und gegebenenfalls die Kategorie des SAQ anzupassen.

2.4. Die Auswahl des richtigen SAQ

Welcher SAQ für Sie der richtige ist, hängt von Ihren Geschäftsprozessen ab. Es wurden sieben Kategorien gebildet, um eine adäquate Selbsteinschätzung hinsichtlich der PCI DSS-Konformität der eigenen Geschäftsumgebung vorzunehmen. Die Kriterien, nach denen unterschieden wird, sind in der folgenden Tabelle in der rechten Spalte angegeben. Ein maßgeblicher Einflussfaktor ist, ob Kreditkartendaten in elektronischer Form gespeichert werden. Ist dies der Fall, so ist immer SAQ der Kategorie D anzuwenden.

Den von Ihnen auszufüllenden SAQ erhalten Sie auf der ConCardis PCI DSS-Plattform, die Sie auf Ihrem Weg zur PCI DSS-Konformität unterstützt. Nach einer Registrierung auf der Plattform hilft Ihnen der SAQ-Auswahlassistent bei der Auswahl des anzuwendenden SAQ.

Eine Registrierung auf der ConCardis PCI DSS-Plattform können Sie unter folgendem Link vornehmen: https://www.pciplatform.ConCardis.com/

Bitte beachten Sie, dass ConCardis Ihnen zuvor die initialen Zugangsdaten zugesandt haben muss.

Alternativ dazu erhalten Sie den für Sie anwendbaren SAQ von ConCardis oder als Download von den Webseiten des PCI SSC unter: https://de.pcisecuritystandards.org/minisite/en/saq-v3.0-documentation.php

Beispiel: In meinem Hotel werden zur Zahlung mit Kreditkarte zwei Wähl-Terminals eingesetzt. Eines befindet sich an der Rezeption, das andere im Bereich des Speisesaals. Die Geräte speichern keine Kreditkartendaten, sie generieren nach erfolgter Zahlung lediglich einen Papierbeleg. Im Anschluss daran wird ausschließlich mit dem Papierbeleg weitergearbeitet (in Buchhaltung etc.). E-Mails, die Kreditkarteninformationen enthalten, werden sofort nach Erhalt aus dem Posteingang und dem Papierkorb bzw. „Gelöschte Objekte"-Ordner gelöscht. Daraus resultiert, dass SAQ der Kategorie B auszufüllen ist.

SAQ-Kategorie	Umfang	Zielpublikum/Merkmale
A	14 Fragen	▪ Alle Kreditkartenfunktionen ausgelagert ▪ Keine physische Präsenz von Kreditkarten (d.h. nur E-Commerce oder Versandhandel)
A-EP	105 Fragen	▪ E-Commerce-Händler, die alle Bezahlprozesse zu einem PCI DSS-validierten Dienstanbieter ausgelagert haben ▪ Eine Webseite betreiben, die nicht direkt Kartendaten empfängt, aber die Sicherheit des Bezahlprozesses beeinflussen kann ▪ Keinerlei elektronische Speicherung von Kreditkartendaten
B	38 Fragen	▪ Es werden ausschließlich Terminals mit Wählverbindung (ISDN oder analog) zur Kreditkartenzahlung eingesetzt ▪ Keine elektronische Speicherung von Kreditkartendaten (auch nicht vom Terminal!)
B-IP	62 Fragen	▪ Händler benutzen ausschließlich standalone, PTS-zertifizierte Bezahlterminals mit einer IP-Verbindung zum Bezahl-Prozessor ▪ Keine elektronische Speicherung von Kreditkartendaten
C-VT	58 Fragen	▪ Zahlungsabwicklung erfolgt ausschließlich mit webbasierten virtuellen Terminals ▪ Der Computer, auf dem das virtuelle Terminal verwendet wird, darf mit keinem anderen System des Händlers verbunden sein ▪ Keine elektronische Speicherung von Kreditkartendaten
C	96 Fragen	▪ Einsatz von Kreditkartenterminals und/oder Zahlungsanwendungssystemen, die mit dem Internet verbunden sind ▪ Die Kreditkartenterminals und/oder Zahlungsanwendungssysteme dürfen **nur** mit dem Internet und mit **keinem** anderen System des Händlers verbunden sein ▪ Keine elektronische Speicherung von Kreditkartendaten
D	241 Fragen	▪ Alle, die nicht in den Beschreibungen für SAQ A bis C oben enthalten sind ▪ Alle Dienstanbieter

2.5. Wichtige ergänzende Hinweise für die Auswahl des korrekten SAQ

Immer wieder kommt es vor, dass aufgrund von fehlendem Detailwissen über die Anforderungen des PCI DSS-Sicherheitsstandards die Auswahl des anzuwendenden SAQ nicht optimal ausfällt. So wird häufig als anzuwendender SAQ derjenige der Kategorie D festgestellt, obwohl durch geringfügige Änderungen durchaus eine Einstufung in eine andere Kategorie möglich wäre. Dies ist im Wesentlichen auf das Fehlverhalten von Mitarbeitern und der gegenwärtig vorhandenen Infrastruktur zurückzuführen, die sich allerdings auf relativ einfache Weise so anpassen lassen, dass ein SAQ der niedrigeren Kategorien anzuwenden ist. Der Vorteil liegt in dem erheblich niedrigeren Umfang von Sicherheitsmaßnahmen, die dann zu treffen sind, um den PCI DSS-Sicherheitsstandards zu genügen.

Im Folgenden werden einige häufig beobachtete Szenarien beschrieben, die eine Anwendbarkeit des SAQ der Kategorie D bewirken. Eine kurze Handlungsempfehlung zu jedem dieser Szenarien kann aus der Anwendbarkeit des SAQ D herausführen und damit die Erreichung der eigenen PCI DSS-Konformität erheblich vereinfachen.

Kreditkarteninformationen liegen in elektronischer Form vor

Es kommt häufig vor, dass Kreditkartendaten an unterschiedlichen Stellen elektronisch gespeichert werden, beispielsweise in Dateien aus Programmen zur Textverarbeitung oder Tabellenkalkulation, ohne dass die daraus resultierenden Risiken wahrgenommen werden. Zudem werden E-Mails, die Kreditkarteninformationen enthalten, in elektronischen Postfächern häufig nicht gelöscht. E-Mails können ausgedruckt und auf Papier weiterbearbeitet werden. Wird eine E-Mail sofort nach dem Ausdruck gelöscht, auch aus dem Papierkorb und dem „Gelöschte Objekte“-Ordner, dann liegt eine elektronische Speicherung im Sinne des PCI DSS nicht mehr vor. Wenn Sie sich nicht sicher sind, ob auf Ihren Systemen Kreditkartendaten in elektronischer Form vorhanden sind, so kann spezielle Software dabei helfen diese aufzuspüren. Eine initiale Überprüfung der vorhandenen Systeme ist zu empfehlen. Ihr IT-Dienstleister sollte Sie dabei unterstützen können.

Sollten in Ihrem Hotel Kreditkarteninformationen in elektronischer Form gespeichert werden, greift sofort SAQ D! Deshalb sei an dieser Stelle nochmals darauf hingewiesen, dass auf jegliche elektronische Speicherung von Kreditkartendaten Ihrerseits verzichtet werden sollte, sofern diese nicht unbedingt notwendig ist!

Fehlende Netzwerksegmentierung

Der PCI DSS-Sicherheitsstandard verlangt eine Trennung von Systemen, die Kreditkartendaten verarbeiten, und denen, die keinen Zugriff auf diese Informationen benötigen. Insbesondere für die Anwendbarkeit des SAQ B-IP ist die Isolierung kreditkartendatenverarbeitender Systeme zwingende Voraussetzung. Die Kreditkartenterminals und/oder Zahlungsanwendungssysteme dürfen nur mit dem Internet und mit keinem anderen System des Händlers verbunden sein. Damit soll das Risiko eines Diebstahls von Kreditkarteninformationen gesenkt werden.

Der Einsatz und die geeignete Konfiguration von Firewalls und Routern kann die Kommunikation zwischen denjenigen Systemen, welche Kreditkartendaten verarbeiten, und den anderen sich im Hotel befindlichen Systemen unterbinden, so dass die gewünschte Segmentierung erreicht wird. Ziel ist es, den nicht kreditkartendatenverarbeitenden Systemen den direkten Zugriff auf Systeme, die mit Kreditkartendaten arbeiten, zu verbieten. Ihr IT-Dienstleister sollte Sie bei der Umsetzung unterstützen können.

Bei fehlender Isolierung der kreditkartendatenverarbeitenden Systeme sind für das gesamte Netzwerk umfangreiche Maßnahmen zu dessen Schutz zu treffen. Daraus folgt die Anwendung des SAQ D!

Sicherer Zugriff bei Fernwartung

Häufig bieten Softwareanbieter ihren Kunden die Möglichkeit zur Fernwartung, um so auf effiziente Weise Probleme zu beheben. Ein unzureichend gesicherter Fernzugriff birgt ein erhebliches Risikopotential und kann dazu führen, dass ein Hacker sicherheitskritische Informationen erbeutet.

Sollten Sie Ihrem IT-Dienstleister oder einem Hersteller im Rahmen von Wartung und Support Fernzugriff auf Ihre Systeme gewähren, so ist dieser in entsprechender Weise zu sichern. Die Kommunikation muss unter Anwendung von Verschlüsselungstechnologien wie eine 2-Faktor-Authentifizierung erfolgen (z.B. über ein VPN mit Zertifikat und Benutzername bzw. Passwort). Des Weiteren darf der Zugang nur über einen speziell für diesen Zugriff eingerichteten Account erfolgen, der nur dann aktiv sein darf, wenn er benötigt wird. Er darf keine permanente Zugriffsmöglichkeit darstellen. Die Zugänge sind während ihrer Dauer zu überwachen. Ihr IT-Dienstleister oder der jeweilige Softwareanbieter sollte Ihnen bei der Umsetzung die nötige Hilfestellung bieten können.

In den häufigsten Fällen lässt sich durch die Berücksichtigung dieser Empfehlungen eine Anwendbarkeit des SAQ D vermeiden und dadurch die eigene PCI DSS-Konformität auf effizientere Weise erreichen.

3. Maßnahmen zur PCI DSS Compliance für Hotels (SAQ B)

- Kreditkartendaten werden nur von Wähl-Terminals und auf Papierbelegen verarbeitet.
- Keine elektronische Speicherung von Kreditkarteninformationen.

3.1. Anwendungsbereich

Die im Folgenden behandelten Inhalte entsprechen denen des SAQ der Kategorie B. Sie beziehen sich also auf eine Geschäftsumgebung, in der Kreditkartendaten ausschließlich auf Papier und mit Bezahlterminals über ISDN-Leitungen verarbeitet werden, ohne dass diese Daten elektronisch gespeichert werden. Sind diese Merkmale für Ihre Geschäftsabläufe in Ihrem Hotel nicht zutreffend, sollten Sie noch einmal unter dem vorangegangenen Abschnitt „Die Auswahl des richtigen SAQ“ nachsehen, welche Kategorie den für Sie passenden SAQ enthält, oder bei Ihrer Händlerbank nachfragen. Es ist wichtig, dass Sie im ersten Schritt die für Ihr Hotel richtige Kategorie ermitteln, da die im Folgenden beschriebenen Maßnahmen nur für Geschäftsumgebungen der Kategorie B vollständig sind.

Den für Ihre Geschäftsprozesse adäquaten SAQ erhalten Sie bei Ihrer Händlerbank (Acquirer) oder als Download von den Webseiten des PCI SSC unter https://de.pcisecuritystandards.org/minisite/en/saq-v3.0-documentation.php

3.2. Zugriff auf Kreditkarteninformationen

Potentielles Risiko

Der Zugriff auf Kreditkartendaten sollte nur denjenigen Mitarbeitern möglich sein, die den Zugriff für ihre Tätigkeit auch benötigen. Mit steigender Anzahl von Personen, die Zugriff auf sensible Daten haben, vergrößert sich natürlich auch das Risiko, dass diese abhandenkommen. Dies muss nicht zwangsläufig durch einen böswilligen Insider geschehen, sondern kann schlichtweg auf Unwissenheit zurückzuführen sein, wie mit sensiblen Informationen umzugehen ist.

Maßnahmen

Zugriffsrechte sollten demnach so vergeben werden, dass jeder Mitarbeiter ausschließlich die zur Ausführung seiner Tätigkeit notwendigen Rechte hat. Dies schließt sowohl den Zugang zu Rechnern als auch physische Zugangsmöglichkeiten zu Schränken, Schubladen oder Räumlichkeiten ein. Ein Passwort sollte nur demjenigen Mitarbeiter bekannt sein, der den Rechnerzugang auch benötigt. Genauso sollten nur diejenigen Mitarbeiter einen Schlüssel für die Aufbewahrungsorte von Kreditkarteninformationen erhalten, die diese für ihre Tätigkeit brauchen. Dabei sollte man sämtliche Aufbewahrungsorte berücksichtigen, also beispielsweise den Schrank in dem Back-Office oder der Buchhaltung genauso wie die Schublade an der Rezeption. Verlässt ein Mitarbeiter das Hotel, dann muss überprüft werden, ob dieser mit speziellen Zugriffsrechten ausgestattet war. Hatte er Zugang zu einem Rechner, so ist das Passwort zu ändern. Ausgehändigte Schlüssel sind selbstverständlich ebenfalls einzufordern.

Aufgaben aus diesem Abschnitt

Festlegen, welche Mitarbeiter Zugang zu den Behältnissen mit kritischen Kreditkarteninformationen auf Papier haben	☐

3.3. Umgang mit E-Mails

Potentielles Risiko

Häufig versenden Kunden eine E-Mail an das Hotel, die ihre Kreditkartendaten enthält, beispielsweise für eine Reservierung. Die E-Mail ist dadurch zunächst einmal für alle einsehbar, die Zugang zum jeweiligen Rechner haben.

Hinweis: An dieser Stelle beschreiben wir nur den Fall, dass Ihnen immer mal wieder Kunden ungewollt ihre Kreditkarteninformationen in einer Reservierungs-E-Mail schicken. Wenn dieser Fall jedoch ein von Ihnen gewollter, regulärer Geschäftsprozess ist, können Sie an dieser Stelle die Bearbeitung dieser Maßnahmenliste beenden. Sie fallen in den Selbstauskunftsfragebogen D und müssen damit deutlich umfassendere Sicherheitsmaßnahmen erfüllen. Für diesen Fall sollten Sie bei Ihrer Händlerbank (Acquirer) professionelle Sicherheitsunterstützung anfragen.

Maßnahmen

Unmittelbar nach Eingang der E-Mail sollte diese gelöscht werden. Dabei ist darauf zu achten, dass sie auch aus dem Papierkorb bzw. dem „Gelöschte Objekte“-Ordner entfernt wird und auch keine Kopie der E-Mail auf einem zentralen E-Mail-Server zu Archivierungszwecken gespeichert wird. Werden die Informationen benötigt, so empfiehlt es sich, diese E-Mail auszudrucken und nur auf Papier weiterzuverarbeiten. Wie mit Ausdrucken umzugehen ist, die Kreditkarteninformationen enthalten, erfahren Sie im nächsten Abschnitt.

Aufgaben aus diesem Abschnitt

Mitarbeiter mit Rechnerzugriff anweisen, wie mit E-Mails zu verfahren ist	☐

3.4. Umgang mit Ausdrucken und Papierbelegen

Potentielles Risiko

Im Hotel finden sich Kreditkarteninformationen typischerweise auf einer Vielzahl von Papieren wieder. Dazu zählen vor allem Ausdrucke, Faxe und Belege der Bezahlterminals. Wird unachtsam mit diesen umgegangen, stellen darauf enthaltene Kreditkarteninformationen eine leichte Beute für einen böswilligen Mitarbeiter dar.

Maßnahmen

Überall, wo Kreditkarteninformationen auf Papier verarbeitet werden, müssen diese in verschließbaren Schränken oder Schubladen aufbewahrt werden. Ausdrucke und Belege sollten beispielsweise niemals sichtbar an der Rezeption gestapelt werden. Solche Dokumente sollten generell als vertraulich eingestuft werden und die Mitarbeiter, die mit ihnen in Berührung kommen, sollten hinsichtlich der Sensibilität der Informationen, die sie enthalten, geschult sein.

PCI DSS verbietet jegliche Speicherung von sogenannten sensiblen Authentisierungsdaten, was bei Kreditkarten unter anderem die Prüfziffer und die PIN sind. Auf die PIN hat allerdings in der Regel der Hotelier nie Zugriff. Enthält aber die E-Mail eines Kunden beispielsweise auch seine Prüfziffer, so muss diese auch auf dem Ausdruck unkenntlich gemacht (geschwärzt) werden. Ferner sollte der Zugriff auf die Belege nur durch Mitarbeiter möglich sein, die zur Ausführung ihrer Tätigkeit darauf zugreifen müssen. Deshalb sollte streng kontrolliert und schriftlich festgehalten werden, wer einen Schlüssel zu den Aufbewahrungsorten hat.

Bei der Entsorgung von Ausdrucken, Belegen und sonstigen Dokumenten auf Papier, die Kreditkartendaten enthalten, muss darauf geachtet werden, dass diese auch wirklich vernichtet werden und nicht wieder herstellbar sind. Sie gehören in den Aktenvernichter und nicht einfach nur in den Papierkorb. Durch einen Kreuzschnitt/Partikelschnitt (cross-cut) werden Dokumente in einer Weise zerkleinert, so dass eine Verwertbarkeit der Informationen auf den Einzelteilen nicht mehr möglich ist. Daher sollte, wenn Sie die Aktenvernichtung selbst vornehmen, bei der Anschaffung eines Aktenvernichters darauf geachtet werden, dass diese Form der Zerkleinerung unterstützt wird. In der Norm DIN 32757-1 sind fünf Sicherheitsstufen definiert. Für die sichere Vernichtung von sensiblen Informationen wird hierzu mindestens ein Aktenvernichter der Sicherheitsstufe 3 empfohlen.

Wird ein Dienstleister mit der Entsorgung beauftragt, so muss sichergestellt werden, dass dieser die Verantwortung für die ordnungsgemäße Vernichtung der Dokumente übernimmt. Dieser Aspekt sollte Bestandteil des schriftlichen Vertrags mit dem jeweiligen Dienstleister sein. Häufig werden in solch einer Situation die Dokumente nicht sofort vernichtet, sondern erst gesammelt. Dann muss der Container, in dem diese aufbewahrt werden, vor Zugriff durch Unbefugte geschützt werden. Wenn diese beispielsweise in einem Schrank aufbewahrt werden, sollte dieser mindestens mit einem Schloss gesichert werden.

Aufgaben aus diesem Abschnitt

Ausdrucke, Faxe und Belege mit Kreditkarteninformationen unter Verschluss aufbewahren	☐
Hochgradig sensible Informationen auf Ausdrucken müssen sicher geschwärzt werden	☐
Mitarbeiter informieren, wie mit Ausdrucken und Papierbelegen zu verfahren ist	☐
Kreditkartendaten werden bei Entsorgung unwiederbringlich vernichtet	☐
Der beauftragte Dienstleister nimmt eine ordnungsgemäße Entsorgung vor und trägt die Verantwortung dafür	☐

3.5. Das Bezahlterminal

Potentielles Risiko

Ist eine elektronische Speicherung von Kreditkarteninformationen nicht unbedingt notwendig, so sollte generell immer davon abgesehen werden. Die hier beschriebenen Maßnahmen (SAQ Kategorie B) gehen davon aus, dass keine Kreditkartendaten in digitaler Form gespeichert werden. Bei älteren Geräten besteht die Möglichkeit, dass Kreditkartendaten gespeichert werden. Dies sollte bei moderneren Kartenterminals nicht mehr der Fall sein. Zudem sollten die Geräte heutzutage manipulationssicher sein. Häufig wird hierzu auf dem Bezahlterminal ein Sicherheitssiegel aufgeklebt. Hintergrund ist, dass es in der Vergangenheit Diebstähle von Kreditkarteninformationen gegeben hat, die von manipulierten Kartenterminals abgegriffen wurden.

Maßnahmen

Wenn Sie sich nicht sicher sind, ob das von Ihnen eingesetzte Bezahlterminal manipulationssicher ist oder Kartendaten speichert, sollten Sie den Dienstleister, der Ihnen das Terminal zur Verfügung gestellt hat, fragen, ob das Bezahlterminal die Kreditkartensicherheitsstandards erfüllt.

Aufgaben aus diesem Abschnitt

Es muss sichergestellt sein, dass die Bezahlterminals gegen Austausch, Manipulation oder Beschädigung gesichert sind	☐
Klären, ob alle Mitarbeiter geschult wurden bzw. werden, solche Änderungen zu entdecken	☐
Alle Terminals werden in einer Liste geführt, die Aufstellungsort, Seriennummer und Hersteller beinhaltet. Mitarbeiter werden geschult, um offensichtliche Beschädigungen oder Änderungen an den Terminals zu entdecken	☐
Eine periodische Inspektion aller Geräte wird durchgeführt, um deren Sicherheit zu überprüfen und zu gewährleisten	☐
Dienstleister oder Hersteller des eingesetzten Kartenterminals kontaktieren (oder auf den Webseiten des PCI Councils die Zertifizierung des Gerätes verifizieren)	☐ ☐
Klären, ob das eigene Kartenterminal die Kreditkartensicherheitsstandards einhält	☐
Klären, ob das eigene Kartenterminal gegen Manipulationen besonders geschützt ist	☐
Klären, ob das eigene Kartenterminal Kreditkartendaten speichert	☐
Wenn ja: Klären, ob diese sicher gelöscht werden können	☐

3.6. Sicherheitsdokumente

Der PCI-Standard verlangt die Anfertigung und Pflege von bestimmten Dokumenten, die helfen sollen, den Überblick über die Einhaltung der verschiedenen Maßnahmen zu behalten. Zudem ist schriftliche Dokumentation der beste Weg, um im Nachhinein gegenüber Dritten die PCI-Konformität nachweisen zu können. Es empfiehlt sich daher für die folgenden Bereiche eine knappe und pragmatische Dokumentation zu pflegen.

Informationssicherheitsrichtlinie

Eine Informationssicherheitsrichtlinie sollte den Umgang mit allen sicherheitskritischen Aspekten im Hotel beschreiben. PCI DSS verlangt an dieser Stelle nicht die Anfertigung eines komplexen Nachschlagewerks, es sollten aber alle sicherheitsrelevanten Themen kurz abgebildet werden. Dies betrifft in erster Linie den sicheren Umgang mit Kreditkarteninformationen, aber auch den Umgang mit Computern und der auf ihnen installierten Software. Insbesondere sollten Mitarbeiter darauf hingewiesen werden, dass Kreditkarteninformationen niemals ungeschützt per E-Mail versendet werden dürfen.

Zur Kommunikation werden häufig sogenannte Messaging-Technologien für Endanwender verwendet, die allerdings keine Möglichkeit bieten, die zu übertragenden Daten angemessen zu schützen. Deshalb dürfen diese keinesfalls zum Versand von Kreditkartendaten verwendet werden. Unter dem Begriff der Endbenutzer-Technologien fallen generell unverschlüsselte E-Mails, Instant Messenger und Chat-Programme, wie beispielsweise ICQ oder Skype, aber auch Dropbox, Cloud etc. Durch im Internet frei verfügbare Software können die Nachrichten leicht abgefangen und ausgelesen werden, da die meisten dieser Programme keinerlei Möglichkeiten zur Verschlüsselung der Nachrichten bieten. Aufgrund des verstärkten Risikos bei der Kommunikation über Software, die Nachrichten unverschlüsselt überträgt, sollte gänzlich auf deren Nutzung verzichtet werden. Am besten ist dies in einer Arbeitsanweisung festzuhalten, die die Nutzung von riskanten Technologien verbietet. Damit Mitarbeiter verstehen, warum sie darauf verzichten sollen, weist man sie am besten auf die damit verbundenen Gefahren hin.

Mitarbeiter müssen dafür sensibilisiert werden, dass die Sicherheit der Kreditkartendaten Ihrer Kunden langfristig maßgeblich zum Geschäftserfolg beiträgt und damit in ihrem eigenen Interesse ist. Wenn möglich, sollte den Mitarbeitern ein Sicherheitstraining angeboten werden. Eine Sensibilisierung kann aber auch schon erreicht werden, indem beispielsweise Poster oder Bildschirmschoner am Arbeitsplatz darauf hinweisen.

Daher sollte die Informationssicherheitsleitlinie jedem Mitarbeiter ausgehändigt werden.

Einmal pro Jahr sollte die Richtlinie hinsichtlich ihrer Aktualität geprüft und gegebenenfalls angepasst werden, sofern Veränderungen stattgefunden haben.

Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten

Die Arbeitsanweisung für Mitarbeiter, die Umgang mit Kreditkartendaten haben, sollte diese darauf hinweisen, dass sie es mit sensiblen Informationen zu tun haben und wie mit diesen korrekt umzugehen ist. Dies umfasst die Inhalte aus den Abschnitten Umgang mit E-Mails sowie Umgang mit Ausdrucken und Papierbelegen.

Liste mit Zugriffs- und Zugangsberechtigungen

Eine Liste mit Zugriffs- und Zugangsberechtigungen sollte diejenigen Mitarbeiter enthalten, die den Rechner mit elektronischem Postfach benutzen und/oder einen Schlüssel für die Aufbewahrungsorte von Ausdrucken und Papierbelegen haben. Im Zusammenhang mit dem Dienstplan kann so nachverfolgt werden, wer zu welchem Zeitpunkt Zugriff auf Kreditkarteninformationen hatte.

Liste externer Dienstleister

Dem Umgang mit Dienstleistern kommt im SAQ B eine besondere Bedeutung zu, da wesentliche Bezahlprozesse an diesen ausgelagert sind. Bestehen Verträge mit externen Dienstleistern, die mit Kreditkartendaten in Berührung kommen, so sollten diese hinsichtlich der Sensibilität der Daten aufgeklärt werden. Es sollte vertraglich berücksichtigt werden, dass diese für die Sicherheit von Kreditkartendaten mitverantwortlich sind, sobald sie mit diesen zu tun haben. Beispielsweise muss einem Dienstleister, der mit der Vernichtung von Kreditkartendaten beauftragt wird, klar sein, dass er für eine ordnungsgemäße Entsorgung verantwortlich ist. Eine Liste, die alle externen Dienstleister aufführt, die direkt oder indirekt in den Bezahlprozess involviert sind, hilft dabei, den Überblick zu behalten. Diese Liste ist ständig aktuell zu halten. Bei den vertraglichen Bindungen an die Dienstleister ist deutlich zu unterscheiden, welche Aufgaben dem Dienstleister zufallen und von diesem zu verantworten sind. Mindestens 1x jährlich ist die PCI Compliance der Dienstleister zu prüfen. Wenn Sie den PCI DSS-Konformitätsstatus Ihres Serviceanbieters kennen, können Sie sich sicher sein, dass er denselben Anforderungen wie auch Ihr Unternehmen unterliegt.

Die großen Kreditkartengesellschaften führen eigene Listen, in denen die PCI DSS-Konformität von Dienstleistern und Herstellern rund um das Kreditkartengeschäft nachvollziehbar ist. Diese werden auf den jeweiligen Webseiten zur Verfügung gestellt und können von jedem eingesehen werden.

Die Liste von MasterCard finden Sie unter folgendem Link:
http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

Unter folgendem Link gelangen Sie zur Liste der von Visa Europe zertifizierten Dienstleister:
http://www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

Insbesondere wenn Sie Kreditkartendaten mit Zahlungsanwendungen verarbeiten und damit in den Anwendungsbereich des SAQ C fallen, können Sie auf den Webseiten des PCI Councils nachverfolgen, ob die von Ihnen eingesetzte Software dem PCI Payment Application Data Security Standard (PCI PA-DSS) genügt. Die Verwendung von zertifizierter Software erleichtert die Umsetzung der Maßnahmen zur eigenen PCI DSS-Konformität. Ob eine und welche Version einer Zahlungsanwendung nach PCI PA-DSS zertifiziert ist, können Sie unter folgendem Link auf die Webseiten des PCI Councils überprüfen:
https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Ob das von Ihnen eingesetzte Kartenterminal zertifiziert ist, können Sie ebenfalls auf den Webseiten des PCI Councils unter folgendem Link herausfinden:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Der Status der PCI DSS-Konformität von Dienstleistern ist einmal jährlich zu überprüfen.

Aufgaben aus diesem Abschnitt

Anfertigen einer Informationssicherheitsrichtlinie	☐
Anfertigen einer Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten	☐
Anfertigen einer Liste mit Zugriffs- und Zugangsberechtigungen	☐
Anfertigen einer Liste externer Dienstleister	☐
Überprüfung des Status zur PCI DSS-Konformität der Dienstleister	☐
Anfertigung einer Liste, welche PCI-Anforderungen vom Dienstleister wahrgenommen werden	☐

3.7. Kreditkartendaten dauerhaft erfolgreich sichern

Für Geschäftsmodelle mit ausschließlicher Kreditkartenverarbeitung über Terminals mit Wählverbindung und Papierbelegen stellen die hier beschriebenen Maßnahmen ein Mindestmaß an Sicherheit für Kreditkartendaten bereit. Bei Verzicht auf die elektronische Speicherung von Kreditkarteninformationen wird bei der Umsetzung aller Maßnahmen auf effiziente und praktikable Weise ein Basisschutz erreicht.

Um die PCI-Konformität aufrechtzuerhalten, ist der SAQ einmal pro Jahr auszufüllen und gegebenenfalls bei der Händlerbank einzureichen. Dadurch entsteht die Möglichkeit, die eingeführten Maßnahmen zu überprüfen und/oder auf möglicherweise stattgefundene Veränderungen in den Geschäftsabläufen zu reagieren und gegebenenfalls die Kategorie des SAQ anzupassen.

Die Erreichung bzw. der Nachweis der PCI-Konformität allein reicht aber nicht aus, um Kreditkartendaten nachhaltig zu schützen. Echter, dauerhafter Schutz wird nur erreicht, wenn die Maßnahmen auch gelebt werden. Dazu müssen alle Beteiligten gemeinsam an einem Strang ziehen.

Schließlich sollte der Schutz von Kundendaten nicht nur vor dem Hintergrund möglicher Haftungsansprüche geschehen, sondern auch aus der Motivation heraus entstehen, die eigene zukünftige Geschäftstätigkeit und Wettbewerbsfähigkeit langfristig zu sichern.

3.8. Anhang A: Checkliste SAQ B

Der Kreditkartenfluss im Hotel ist bekannt?	☐
Kreditkarten werden nur durch ein Terminal mit Wählverbindung und ansonsten nur auf Papier verarbeitet?	☐
Haben nur die Mitarbeiter Zugriff auf Kreditkartendaten, die diese zur Ausführung ihrer Tätigkeit auch brauchen?	☐
Haben nur diejenigen Mitarbeiter Zugang zu einem Rechner, die ihn benötigen?	☐
Haben nur diejenigen Mitarbeiter Schlüssel zu den Aufbewahrungsorten von Kreditkartendaten, die sie benötigen?	☐
Sind die Mitarbeiter hinsichtlich des sicheren Umgangs mit E-Mails, die Kreditkartendaten enthalten, geschult?	☐
Sind die Mitarbeiter hinsichtlich des sicheren Umgangs mit Ausdrucken und Papierbelegen, die Kreditkartendaten enthalten, geschult?	☐
Ist den Mitarbeitern die Sensibilität von Kreditkarteninformationen klar?	☐
Werden Ausdrucke, Faxe und Belege mit Kreditkarteninformationen unter Verschluss aufbewahrt?	☐
Werden hochgradig sensible Informationen auf Ausdrucken geschwärzt bzw. unkenntlich gemacht?	☐

Ist sichergestellt, dass Kreditkartendaten bei ihrer Entsorgung unwiederbringlich vernichtet werden?	☐
Ist vertraglich gesichert, dass der beauftragte Dienstleister eine ordnungsgemäße Entsorgung vornimmt und die Verantwortung dafür trägt?	☐
Mit dem Dienstleister klären: Hält sich das eingesetzte Kartenterminal an Kreditkartensicherheits-standards (oder auf den Webseiten des PCI Councils die Zertifizierung des Gerätes verifizieren)?	☐
Speichert das Kartenterminal Kreditkartendaten?	☐
Wenn ja: Können diese sicher gelöscht werden?	☐
Ist das Kartenterminal manipulationssicher?	☐
Existiert eine Informationssicherheitsrichtlinie?	☐
Sind die Inhalte allen Mitarbeitern klar?	☐
Existiert eine Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten?	☐
Existiert eine Liste mit Zugriffs- und Zugangsberechtigungen?	☐
Besteht ein Vertragsverhältnis mit Dienstleistern, die mit Kreditkartendaten in Berührung kommen?	☐
Existiert eine Liste dieser Dienstleister mit der Trennung der Aufgaben von Dienstleister und eige-nem Unternehmen?	☐
Überprüfung des Status zur PCI DSS-Konformität der Dienstleister	☐
Sind die Dienstleister für den Umgang mit Kreditkartendaten sensibilisiert?	☐
Werden die Maßnahmen und Dokumente einmal pro Jahr auf ihre Aktualität geprüft?	☐
Existiert eine Liste aller Bezahlterminals inkl. deren Seriennummer?	☐
Werden die Kartenterminals periodisch auf Vollständigkeit und Manipulation überprüft?	☐

3.9. Anhang B: Checkliste – Bereiche der Kreditkartenverarbeitung

Geschäftsprozess	Bereich	Medium, das die Kreditkartendaten enthält	Weiterverarbeitung der Kreditkartendaten

4. Maßnahmen zur PCI DSS Compliance für Hotels (SAQ B-IP)

- Ihr Hotel benutzt ausschließlich eigenständige und PTS-zertifizierte Geräte (POI), die über das Übertragungsprotokoll IP mit dem entsprechenden Bezahlprozessor verbunden sind, welcher die Bezahldaten übernimmt.
- Diese eigenständigen Geräte sind durch das PTS POI-Programm validiert. Validierte Geräte kann Ihnen ConCardis nennen.
- Die eigenständigen durch IP verbundenen POI-Geräte dürfen mit keinem anderen Netz Ihrer Umgebung verbunden sein (dies lässt sich z.B. durch eine Netzwerksegmentierung und eine Firewall erreichen).
- Die einzige Möglichkeit, Kartendaten zu transportieren, ist die Verbindung vom PTS-zertifizierten Gerät zum Bezahlprozessor.
- Das POI-Gerät benötigt keinerlei andere Geräte (z.B. Computer, Mobilgeräte, Kassen etc.) zur Verbindung zum Bezahlprozessor.
- Ihr Hotel behält ausschließlich Papierberichte oder Papierkopien der Rechnungen mit Kartendaten zurück und diese Papierunterlagen werden nicht elektronisch empfangen.
- Ihr Hotel speichert keine Kartendaten in einem elektronischen Format.
- Dieser SAQ gilt nicht für „SCR“ (Secure Card Reader).

4.1. Anwendungsbereich

Die im Folgenden behandelten Inhalte entsprechen denen des SAQ der Kategorie B-IP und sind in vielen Bereichen mit denen des SAQ B identisch. Der Unterschied ergibt sich in erster Linie durch IP-basierte Geräte, welche strikt von den anderen IT-Systemen des Hotels getrennt gehalten werden müssen. Hinzu kommt gegebenenfalls die Pflicht Ihr Netzwerk von außen vierteljährlich durch einen zertifizierten ASV auf Verwundbarkeiten überprüfen zu lassen. Siehe hierzu insbesondere die Ausnahme unter 4.3. „ASV Scans“. Einen zertifizierten ASV finden Sie unter www.usd.de oder unter https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Der SAQ B-IP bezieht sich auf eine Geschäftsumgebung, die Kreditkartendaten ausschließlich mit PTS-zertifizierten Bezahlterminals direkt an den Bezahlprozessor weiterleitet, ohne dass diese Daten elektronisch gespeichert werden, und in der Kreditkartendaten ausschließlich auf Papier vorhanden sind. Sind diese Merkmale für Ihre Geschäftsabläufe in Ihrem Hotel nicht zutreffend, sollten Sie noch einmal unter dem vorangegangenen Abschnitt „Die Auswahl des richtigen SAQ“ nachsehen, welche Kategorie den für Sie passenden SAQ enthält, oder bei Ihrer Händlerbank nachfragen. Es ist wichtig, dass Sie im ersten Schritt die für Ihr Hotel richtige Kategorie ermitteln, da die im Folgenden beschriebenen Maßnahmen nur für Geschäftsumgebungen der Kategorie B-IP vollständig sind.

Den für Ihre Geschäftsprozesse adäquaten SAQ erhalten Sie bei ConCardis oder als Download von den Webseiten des PCI SSC unter
https://de.pcisecuritystandards.org/minisite/en/saq-v3.0-documentation.php

Netzwerksegmentierung: Der SAQ B-IP bedingt eine strikte Trennung der Bezahlsysteme von jeglichen anderen Orten und Systemen des Hotels. Bei unzureichender Netzwerksegmentierung können Daten aus den PTS-Terminals in das Hotelnetz gelangen und Angreifern die Möglichkeit eröffnen, diese Daten zu entwenden oder weiterzuleiten (siehe auch Seite 10). Voraussetzung für eine erfolgreiche Segmentierung ist eine vollständige Übersicht Ihres Netzwerks mit allen Komponenten und insbesondere Ein- und Ausgängen zu ungesicherten Netzwerken (Internet). Bei jeder Änderung der Infrastruktur ist die wirksame Segmentierung erneut zu prüfen. Ein IT-Dienstleister leistet hier oftmals wertvolle Arbeit.

Aufgaben aus diesem Abschnitt

Existiert ein aktueller Netzwerkplan?	☐
Besteht eine effektive Netzwerksegmentierung zwischen Bezahlsystemen und dem restlichen Hotel-Netzwerk?	☐
Wird eine Firewall eingesetzt?	☐

4.2. Zugriff auf Kreditkarteninformationen

Potentielles Risiko

Der Zugriff auf Kreditkartendaten sollte nur denjenigen Mitarbeitern möglich sein, die den Zugriff für ihre Tätigkeit auch benötigen. Mit steigender Anzahl von Personen, die Zugriff auf sensible Daten haben, vergrößert sich natürlich auch das Risiko, dass diese abhandenkommen. Dies muss nicht zwangsläufig durch einen böswilligen Insider geschehen, sondern kann schlichtweg auf Unwissenheit zurückzuführen sein, wie mit sensiblen Informationen umzugehen ist.

Maßnahmen

Zugriffsrechte sollten demnach so vergeben werden, dass jeder Mitarbeiter ausschließlich die zur Ausführung seiner Tätigkeit notwendigen Rechte hat. Dies schließt den physischen Zugang zu Schränken, Schubladen oder Räumlichkeiten ein. Nur diejenigen Mitarbeiter sollten einen Schlüssel für die Aufbewahrungsorte von Kreditkarteninformationen erhalten, die diese für ihre Tätigkeit brauchen. Dabei sollte man sämtliche Aufbewahrungsorte berücksichtigen, also beispielsweise den Schrank in dem Back-Office oder der Buchhaltung genauso wie die Schublade an der Rezeption. Verlässt ein Mitarbeiter das Hotel, sind ausgehändigte Schlüssel selbstverständlich einzufordern.

Aufgaben aus diesem Abschnitt

Überprüfen, ob alle Bezahlterminals PTS-zertifiziert sind	☐
Festlegen, welche Mitarbeiter Zugang zu den Behältnissen mit kritischen Kreditkarteninformationen auf Papier haben	☐

4.3. ASV Scans

Die Erfüllung der Compliance durch den SAQ B-IP kann die vierteljährliche Durchführung von sog. ASV Scans (ASV = Applied Security Vendor) gegen öffentlich erreichbare Schnittstellen des Hotels beinhalten.
Weitere Informationen hierzu erhalten Sie unter
https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v2.pdf
Diese ASV Scans stellen fest, ob Ihre Absicherung nach außen wirkungsvoll ist.

AUSNAHME: Wenn Ihre Firewall aus dem Internet nicht erreichbar ist und von den PTS-Bezahlterminals nur ausgehender Verkehr zugelassen ist, entfällt Ihre Scan-Pflicht. Sicherheit verschafft Ihnen ein einmaliger ASV Scan auf Ihre Umgebung.

4.4. Umgang mit E-Mails

Potentielles Risiko

Häufig versenden Kunden eine E-Mail an das Hotel, die ihre Kreditkartendaten enthält, beispielsweise für eine Reservierung. Die E-Mail ist dadurch zunächst einmal für alle einsehbar, die Zugang zum jeweiligen Rechner haben.

Hinweis: An dieser Stelle beschreiben wir nur den Fall, dass Ihnen immer mal wieder Kunden ungewollt ihre Kreditkarteninformationen in einer Reservierungs-E-Mail schicken. Wenn dieser Fall jedoch ein von Ihnen gewollter, regulärer Geschäftsprozess ist, können Sie an dieser Stelle die Bearbeitung dieser Maßnahmenliste beenden. Sie fallen in den Selbstauskunftsfragebogen D und müssen damit deutlich umfassendere Sicherheitsmaßnahmen erfüllen. Für diesen Fall sollten Sie bei Ihrer Händlerbank (Acquirer) professionelle Sicherheitsunterstützung anfragen.

Maßnahmen

Unmittelbar nach Eingang der E-Mail sollte diese gelöscht werden. Dabei ist darauf zu achten, dass sie auch aus dem Papierkorb bzw. dem „Gelöschte Objekte“-Ordner entfernt wird und auch keine Kopie der E-Mail auf einem zentralen E-Mail-Server zu Archivierungszwecken gespeichert wird. Werden die Informationen benötigt, so empfiehlt es sich, diese E-Mail auszudrucken und nur auf Papier weiterzuverarbeiten. Wie mit Ausdrucken umzugehen ist, die Kreditkarteninformationen enthalten, erfahren Sie im nächsten Abschnitt.

Aufgaben aus diesem Abschnitt

Mitarbeiter mit Rechnerzugriff anweisen, wie mit E-Mails zu verfahren ist	☐

4.5. Umgang mit Ausdrucken und Papierbelegen

Potentielles Risiko

Im Hotel finden sich Kreditkarteninformationen typischerweise auf einer Vielzahl von Papieren wieder. Dazu zählen vor allem Ausdrucke, Faxe und Belege der Bezahlterminals. Wird unachtsam mit diesen umgegangen, stellen darauf enthaltene Kreditkarteninformationen eine leichte Beute für einen böswilligen Mitarbeiter dar.

Maßnahmen

Überall, wo Kreditkarteninformationen auf Papier verarbeitet werden, müssen diese in verschließbaren Schränken oder Schubladen aufbewahrt werden. Ausdrucke und Belege sollten beispielsweise niemals sichtbar an der Rezeption gestapelt werden. Solche Dokumente sollten generell als vertraulich eingestuft werden und die Mitarbeiter, die mit ihnen in Berührung kommen, sollten hinsichtlich der Sensibilität der Informationen, die sie enthalten, geschult sein.

PCI DSS verbietet jegliche Speicherung von sogenannten sensiblen Authentisierungsdaten, was bei Kreditkarten unter anderem die Prüfziffer und die PIN sind. Auf die PIN hat allerdings in der Regel der Hotelier nie Zugriff. Enthält aber die E-Mail eines Kunden beispielsweise auch seine Prüfziffer, so muss diese auch auf dem Ausdruck unkenntlich gemacht (geschwärzt) werden. Ferner sollte der Zugriff auf die Belege nur durch Mitarbeiter möglich sein, die zur Ausführung ihrer Tätigkeit darauf zugreifen müssen. Deshalb sollte streng kontrolliert und schriftlich festgehalten werden, wer einen Schlüssel zu den Aufbewahrungsorten hat.

Bei der Entsorgung von Ausdrucken, Belegen und sonstigen Dokumenten auf Papier, die Kreditkartendaten enthalten, muss darauf geachtet werden, dass diese auch wirklich vernichtet werden und nicht wieder herstellbar sind. Sie gehören in den Aktenvernichter und nicht einfach nur in den Papierkorb. Durch einen Kreuzschnitt/Partikelschnitt (cross-cut) werden Dokumente in einer Weise zerkleinert, so dass eine Verwertbarkeit der Informationen auf den Einzelteilen nicht mehr möglich ist. Daher sollte, wenn Sie die Aktenvernichtung selbst vornehmen, bei der Anschaffung eines Aktenvernichters darauf geachtet werden, dass diese Form der Zerkleinerung unterstützt wird. In der Norm DIN 32757-1 sind fünf Sicherheitsstufen definiert. Für die sichere Vernichtung von sensiblen Informationen wird hierzu mindestens ein Aktenvernichter der Sicherheitsstufe 3 empfohlen.

Wird ein Dienstleister mit der Entsorgung beauftragt, so muss sichergestellt werden, dass dieser die Verantwortung für die ordnungsgemäße Vernichtung der Dokumente übernimmt. Dieser Aspekt sollte Bestandteil des schriftlichen Vertrags mit dem jeweiligen Dienstleister sein. Häufig werden in solch einer Situation die Dokumente nicht sofort vernichtet, sondern erst gesammelt. Dann muss der Container, in dem diese aufbewahrt werden, vor Zugriff durch Unbefugte geschützt werden. Wenn diese beispielsweise in einem Schrank aufbewahrt werden, sollte dieser auch abschließbar sein.

4.6. Sicherheitsdokumente

Der PCI-Standard verlangt die Anfertigung und Pflege von bestimmten Dokumenten, die helfen sollen, den Überblick über die Einhaltung der verschiedenen Maßnahmen zu behalten. Zudem ist schriftliche Dokumentation der beste Weg, um im Nachhinein gegenüber Dritten die PCI-Konformität nachweisen zu können. Es empfiehlt sich daher für die folgenden Bereiche eine knappe und pragmatische Dokumentation zu pflegen.

Informationssicherheitsrichtlinie

Eine Informationssicherheitsrichtlinie sollte den Umgang mit allen sicherheitskritischen Aspekten im Hotel beschreiben. PCI DSS verlangt an dieser Stelle nicht die Anfertigung eines komplexen Nachschlagewerks, es sollten aber alle sicherheitsrelevanten Themen kurz abgebildet werden. Dies betrifft in erster Linie den sicheren Umgang mit Kreditkarteninformationen, aber auch den Umgang mit Computern und der auf ihnen

installierten Software. Insbesondere sollten Mitarbeiter darauf hingewiesen werden, dass Kreditkarteninformationen niemals ungeschützt per E-Mail versendet werden dürfen.

Zur Kommunikation werden häufig sogenannte Messaging-Technologien für Endanwender verwendet, die allerdings keine Möglichkeit bieten, die zu übertragenden Daten angemessen zu schützen. Deshalb dürfen diese keinesfalls zum Versand von Kreditkartendaten verwendet werden. Unter dem Begriff der Endbenutzer-Technologien fallen generell unverschlüsselte E-Mails, Instant Messenger und Chat-Programme, wie beispielsweise ICQ oder Skype, aber auch Dropbox, iCloud etc. Durch im Internet frei verfügbare Software können die Nachrichten leicht abgefangen und ausgelesen werden, da die meisten dieser Programme keinerlei Möglichkeiten zur Verschlüsselung der Nachrichten bieten. Aufgrund des verstärkten Risikos bei der Kommunikation über Software, die Nachrichten unverschlüsselt überträgt, sollte gänzlich auf deren Nutzung verzichtet werden. Am besten ist dies in einer Arbeitsanweisung festzuhalten, die die Nutzung von riskanten Technologien verbietet. Damit Mitarbeiter verstehen, warum sie darauf verzichten sollen, weist man sie am besten auf die damit verbundenen Gefahren hin.

Mitarbeiter müssen dafür sensibilisiert werden, dass die Sicherheit der Kreditkartendaten Ihrer Kunden langfristig maßgeblich zum Geschäftserfolg beiträgt und damit in ihrem eigenen Interesse ist. Eine Sensibilisierung kann aber auch schon erreicht werden, indem beispielsweise Poster oder Bildschirmschoner am Arbeitsplatz darauf hinweisen. Darüber hinaus sollte jedem Mitarbeiter ein periodisch stattfindendes Sicherheitstraining angeboten werden. Die Informationssicherheitsrichtlinie muss jedem Mitarbeiter ausgehändigt werden.

Einmal pro Jahr sollte die Richtlinie hinsichtlich ihrer Aktualität geprüft und gegebenenfalls angepasst werden, sofern Veränderungen stattgefunden haben.

Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten

Die Arbeitsanweisung für Mitarbeiter, die Umgang mit Kreditkartendaten haben, sollte diese darauf hinweisen, dass sie es mit sensiblen Informationen zu tun haben und wie mit diesen korrekt umzugehen ist. Dies umfasst die Inhalte aus den Abschnitten Umgang mit E-Mails sowie Umgang mit Ausdrucken und Papierbelegen.

Liste mit Zugriffs- und Zugangsberechtigungen

Eine Liste mit Zugriffs- und Zugangsberechtigungen sollte diejenigen Mitarbeiter enthalten, die den Rechner mit elektronischem Postfach benutzen und/oder einen Schlüssel für die Aufbewahrungsorte von Ausdrucken und Papierbelegen haben. Im Zusammenhang mit dem Dienstplan kann so nachverfolgt werden, wer zu welchem Zeitpunkt Zugriff auf Kreditkarteninformationen hatte.

Liste externer Dienstleister

Dem Umgang mit Dienstleistern kommt im SAQ B-IP eine besondere Bedeutung zu, da wesentliche Bezahlprozesse an diesen ausgelagert sind. Bestehen Verträge mit externen Dienstleistern, die mit Kreditkartendaten in Berührung kommen, so sollten diese hinsichtlich der Sensibilität der Daten aufgeklärt werden. Es sollte vertraglich berücksichtigt werden, dass diese für die Sicherheit von Kreditkartendaten mitverantwortlich sind, sobald sie mit diesen zu tun haben. Beispielsweise muss einem Dienstleister, der mit der Vernichtung von Kreditkartendaten beauftragt wird, klar sein, dass er für eine ordnungsgemäße Entsorgung verantwortlich ist. Eine Liste, die alle externen Dienstleister aufführt, die direkt oder indirekt in den Bezahlprozess involviert sind, hilft dabei, den Überblick zu behalten. Diese Liste ist ständig aktuell zu halten. Bei den vertraglichen Bindungen an die Dienstleister ist deutlich zu unterscheiden, welche Aufgaben dem Dienstleister zufallen und von diesem zu verantworten sind. Mindestens 1x jährlich ist die PCI Compliance dieser Dienstleister zu prüfen. Wenn Sie den PCI DSS-Konformitätsstatus Ihres Serviceanbieters kennen, können Sie sich sicher sein, dass er denselben Anforderungen wie auch Ihr Unternehmen unterliegt.

Die großen Kreditkartengesellschaften führen eigene Listen, in denen die PCI DSS-Konformität von Dienstleistern und Herstellern rund um das Kreditkartengeschäft nachvollziehbar ist. Diese werden auf den jeweiligen Webseiten zur Verfügung gestellt und können von jedem eingesehen werden.

Die Liste von MasterCard finden Sie unter folgendem Link:
http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

Unter folgendem Link gelangen Sie zur Liste der von Visa Europe zertifizierten Dienstleister:
http://www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

Ob das von Ihnen eingesetzte Kartenterminal zertifiziert ist, können Sie auf den Webseiten des PCI Councils unter folgendem Link herausfinden:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Der Status der PCI DSS-Konformität von Dienstleistern ist einmal jährlich zu überprüfen.

Aufgaben aus diesem Abschnitt

Anfertigen einer Informationssicherheitsrichtlinie	☐
Anfertigen einer Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten	☐
Anfertigen einer Liste mit Zugriffs- und Zugangsberechtigungen	☐
Anfertigen einer Liste externer Dienstleister	☐
Überprüfung des Status zur PCI DSS-Konformität der Dienstleister	☐
Anfertigung einer Liste, welche PCI-Anforderungen vom Dienstleister wahrgenommen werden du welche das Hotel selbst wahrnimmt	☐

4.7. Anhang C: Checkliste SAQ B-IP

Der Kreditkartenfluss im Hotel ist bekannt?	☐
Existiert ein aktuelles Netzwerkdiagramm und eine Firewall und Konfigurationsstandards gemäß Requirement 1 des SAQ B-IP?	☐
Kreditkarten werden nur durch PTS-zertifizierte Terminals über IP und ansonsten nur auf Papier verarbeitet?	☐
Ist sichergestellt, dass die Bezahlterminals ihre Daten nur verschlüsselt übertragen? (Bitmap oder SSL?)	☐
Ist sichergestellt, dass die Bezahlterminals und die betroffenen Netzwerkkomponenten gemäß Requirement 2 des SAQ gehärtet sind?	☐

Ist sichergestellt, dass keine Kreditkartendaten mehr in den Hotel-Systemen vorhanden sind?	☐
Kassen dürfen nicht mehr über IP angesprochen werden (ggfs. Anbindung der Kasse an das Bezahlterminal per USB).	☐
Ein Remote Access von Dienstleistern darf nur über eine 2-Faktor-Authentifizierung erfolgen (z.B. VPN mit Zertifikat und Benutzername/Passwort).	☐
Haben nur diejenigen Mitarbeiter Zugang zu einem Rechner, die ihn benötigen? Insbesondere dürfen Berechtigungen auf Bezahlterminals nur nach Bedarf und geschäftlicher Anforderung vergeben werden.	☐
Beschränken die Firewall- und Router-Konfiguration die Kommunikation zwischen kreditkartenverarbeitenden Systemen und dem Internet? Sind alle Bezahlterminals in einem eigenen Netzwerksegment? (Subnetz oder VLAN?)	☐
Erfolgt eine regelmäßige Softwareaktualisierung auf den betroffenen Netzwerkkomponenten (z.B. Security Patches)?	☐
Werden nur eindeutige Kennungen auf den betroffenen Netzwerkkomponenten vergeben (dazu gehört auch: keine generischen, Gruppen- oder gemeinsam genutzte Passwörter und Zugänge)?	☐
Ist sichergestellt, dass WLANs nicht direkt mit dem POS-Terminal verbunden sind?	☐
Sind die Mitarbeiter hinsichtlich des sicheren Umgangs mit E-Mails, die sensitive Kreditkartendaten enthalten, geschult?	☐
Existiert eine Liste aller PTS-Bezahlterminals inkl. deren Modell, Hersteller, Aufstellungsort und Seriennummer?	☐
Werden die Kartenterminals periodisch auf Vollständigkeit und Manipulation überprüft?	☐
Existiert eine Liste mit der Trennung der Aufgaben von Dienstleister und eigenem Unternehmen?	☐
Werden vierteljährlich externe Schwachstellenscans auf alle Netzwerkkomponenten von einem ASV durchgeführt?	☐
Werden externe Scans wiederholt, bis keine Schwachstellen mehr mit einer CVSS-Klassifizierung größer als 4.0 gefunden werden?	☐
Existiert eine Informationssicherheitsrichtlinie mit Arbeitsanweisungen und Prozessbeschreibungen gemäß insb. Requirement 12 und allen anderen Requirements?	☐
Wird diese an alle Mitarbeiter, die mit Kreditkartendaten in Berührung kommen, verteilt?	☐
Sind die Inhalte meinen Mitarbeitern klar?	☐

Existiert eine Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten?	☐
Existiert eine Liste mit Zugriffs- und Zugangsberechtigungen?	☐
Sind die Mitarbeiter im Umgang mit den eingesetzten Technologien vertraut?	☐
Ist den Mitarbeitern, die mit Kreditkartendaten arbeiten, die Sensibilität dieser Daten bewusst?	☐
Wird der Status zur PCI DSS-Konformität der Dienstleister mind. jährlich überprüft?	☐
Sind die Dienstleister für den Umgang mit Kreditkartendaten sensibilisiert?	☐
Werden die Maßnahmen und Dokumente einmal pro Jahr auf ihre Aktualität geprüft?	☐
Wurde für Sicherheitsvorfälle ein Incidence Response Plan erstellt?	☐
Existiert ein Prozess, um Sicherheitslücken zu identifizieren?	☐

4.8. Anhang D: Checkliste – Bereiche der Kreditkartenverarbeitung

Geschäftsprozess	Bereich	Medium, das die Kreditkartendaten enthält	Weiterverarbeitung der Kreditkartendaten